Motorola RFS Series Wireless LAN Switches

WiNG System Reference Guide

© 2009 Motorola, Inc. All rights reserved.

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Symbol is a registered trademark of Symbol Technologies, Inc. All other product or service names are the property of their respective owners.

About This Guide

Introduction

This guide provides information about using the following Motorola switches and version numbers:

- **RFS6000 4.0**
- **RFS7000 4.0**

NOTE: Screens and windows pictured in this guide are samples and can differ from actual screens.

Documentation Set

The documentation set for the Motorola RF Series Switches is partitioned into the following guides to provide information for specific user needs.

- ***Installation Guides*** - Each switch has a unique Installation Guide which describes the basic hardware setup and configuration required to transition to more advanced configuration of the switches.
- ***Motorola RFS Series Wireless LAN Switches WiNG System Reference*** - Describes configuration of the Motorola RF Switches using the Web UI.
- ***Motorola RFS Series Wireless LAN Switches WiNG CLI Reference*** - Describes the *Command Line Interface* (CLI) and *Management Information Base* (MIB) commands used to configure the Motorola RF Switches.
- ***RF Management Software Users Guide*** - Describes how to use Motorola RFMS to set up and monitor your switch in respect to areas of good RF throughput and defined physical barriers.

Document Conventions

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

NOTE: Indicate tips or special requirements.

SWITCH NOTE: Indicates caveats unique to a RFS6000 or RFS7000 model switch.

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.

Notational Conventions

The following additional notational conventions are used in this document:

- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen.
- **GUI** text is used to highlight the following:
  - Screen names
  - Menu items
  - Button names on a screen.
- bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Contents

Chapter 1.Overview

1.1 Hardware Overview . . . 1-2
1.1.1 Physical Specifications . . . 1-2
1.2 Software Overview . . . 1-3
1.2.1 Infrastructure Features . . . 1-3
1.2.2 Wireless Switching . . . 1-6
1.2.3 Wired Switching . . . 1-16
1.2.4 Management Features . . . 1-17
1.2.5 Security Features . . . 1-18
1.2.6 Supported Access Ports/Points . . . 1-24

Chapter 2. Switch Web UI Access and Image Upgrades

2.1 Accessing the Switch Web UI . . . 2-1
2.1.1 Web UI Requirements . . . 2-1
2.1.2 Connecting to the Switch Web UI . . . 2-1
2.2 Switch Password Recovery . . . 2-3
2.3 Upgrading the Switch Image . . . 2-4
2.4 Auto Installation . . . 2-4
2.5 AP-4131 Access Point to Access Port Conversion . . . 2-6

Chapter 3. Switch Information

3.1 Viewing the Switch Interface . . . 3-1
3.1.1 Setting the Switch Country Code . . . 3-2
3.1.2 Viewing the Switch Configuration . . . 3-2
3.1.3 Switch Dashboard Details . . . 3-4
3.1.4 Viewing Switch Statistics . . . 3-9
3.2 Viewing Switch Port Information . . . 3-11
3.2.1 Viewing the Port Configuration . . . 3-11
3.2.2 Viewing the Ports Runtime Status . . . 3-14
3.2.3 Reviewing Port Statistics . . . 3-15
3.2.4 Power over Ethernet (PoE) . . . 3-19
3.2.5 Editing Port PoE Settings . . . 3-21
3.3 Viewing Switch Configurations . . . 3-22
3.3.1 Viewing the Detailed Contents of a Config File . . . 3-23
3.3.2 Transferring a Config File . . . 3-24
3.4 Viewing Switch Firmware Information . . . 3-25
3.4.1 Editing the Switch Firmware . . . 3-27
3.4.2 Enabling Global Settings for the Image Failover . . . 3-27

3.4.3 Updating the Switch Firmware . . . 3-28
3.5 Switch File Management . . . 3-29
3.5.1 Transferring Files . . . 3-29
3.5.2 Viewing Files . . . 3-33
3.6 Configuring Automatic Updates . . . 3-35
3.7 Viewing the Switch Alarm Log . . . 3-37
3.7.1 Viewing Alarm Log Details . . . 3-38
3.8 Viewing Switch Licenses . . . 3-39
3.9 How to use the Filter Option . . . 3-41

Chapter 4. Network Setup

4.1 Displaying the Network Interface . . . 4-2
4.2 Viewing Network IP Information . . . 4-4
4.2.1 Configuring DNS . . . 4-4
4.2.2 Configuring IP Forwarding . . . 4-6
4.2.3 Viewing Address Resolution . . . 4-8
4.3 Viewing and Configuring Layer 2 Virtual LANs . . . 4-10
4.3.1 Viewing and Configuring VLANs by Port . . . 4-10
4.3.2 Editing the Details of an Existing VLAN by Port . . . 4-11
4.3.3 Viewing and Configuring Ports by VLAN . . . 4-12
4.4 Configuring Switch Virtual Interfaces . . . 4-14
4.4.1 Configuring the Virtual Interface . . . 4-14
4.4.2 Viewing Virtual Interface Statistics . . . 4-18
4.5 Viewing and Configuring Switch WLANs . . . 4-22
4.5.1 Configuring WLANs . . . 4-22
4.5.2 Viewing WLAN Statistics . . . 4-61
4.5.3 Configuring WMM . . . 4-67
4.5.4 Configuring the NAC Inclusion List . . . 4-71
4.5.5 Configuring the NAC Exclusion List . . . 4-75
4.5.6 NAC Configuration Examples Using the Switch CLI . . . 4-78
4.6 Viewing Associated MU Details . . . 4-81
4.6.1 Viewing MU Status . . . 4-81
4.6.2 Configuring Mobile Units . . . 4-84
4.6.3 Viewing MU Statistics . . . 4-86
4.6.4 Viewing Voice Statistics . . . 4-89
4.7 Viewing Access Port Information . . . 4-90
4.7.1 Configuring Access Port Radios . . . 4-91
4.7.2 Viewing AP Statistics . . . 4-104
4.7.3 Configuring WLAN Assignment . . . 4-108
4.7.4 Configuring WMM . . . 4-110
4.7.5 Configuring Access Point Radio Bandwidth . . . 4-113
4.7.6 Configuring Radio Groups for MU Load Balancing . . . 4-114
4.7.7 Viewing Active Calls (VCAC) Statistics . . . 4-115
4.7.8 Viewing Mesh Statistics . . . 4-116
4.7.9 Smart RF . . . 4-118
4.7.10 Voice Statistics . . . 4-127
4.8 Viewing Access Port Adoption Defaults . . . 4-128
4.8.1 Configuring AP Adoption Defaults . . . 4-129

4.8.2 Configuring Layer 3 Access Port Adoption . . . 4-136
4.8.3 Configuring WLAN Assignment. . . . 4-136
4.8.4 Configuring WMM. . . . 4-138
4.9 Configuring Access Ports . . . 4-140
4.9.1 Viewing Adopted Access Ports . . . 4-140
4.9.2 Viewing Unadopted Access Ports . . . 4-142
4.9.3 Viewing Sensor Information . . . 4-143
4.9.4 Configuring Secure WiSPe . . . 4-144
4.9.5 Configuring Adaptive AP Firmware . . . 4-146
4.10 Multiple Spanning Tree. . . . 4-148
4.10.1 Configuring a Bridge . . . 4-149
4.10.2 Viewing and Configuring Bridge Instance Details. . . . 4-151
4.10.3 Configuring a Port . . . 4-153
4.10.4 Viewing and Configuring Port Instance Details. . . . 4-157
4.11 Configuring IGMP Snooping . . . 4-159
4.11.1 IGMP Snooping Configuration . . . 4-160
4.11.2 IGMP Snoop Querier Configuration . . . 4-161

Chapter 5.Switch Services

5.1 Displaying the Services Interface . . . 5-2
5.2 DHCP Server Settings . . . 5-3
5.2.1 Configuring the Switch DHCP Server . . . 5-4
5.2.2 Viewing the Attributes of Existing Host Pools . . . 5-10
5.2.3 Configuring Excluded IP Address Information . . . 5-12
5.2.4 Configuring the DHCP Server Relay. . . . 5-13
5.2.5 Viewing DDNS Bindings . . . 5-15
5.2.6 Viewing DHCP Bindings. . . . 5-16
5.2.7 Reviewing DHCP Dynamic Bindings . . . 5-17
5.2.8 Configuring the DHCP User Class . . . 5-19
5.2.9 Configuring DHCP Pool Class. . . . 5-21
5.3 Configuring Secure NTP . . . 5-24
5.3.1 Defining the SNTP Configuration . . . 5-24
5.3.2 Configuring Symmetric Keys . . . 5-26
5.3.3 Defining a NTP Neighbor Configuration . . . 5-27
5.3.4 Adding an NTP Neighbor . . . 5-29
5.3.5 Viewing NTP Associations. . . . 5-31
5.3.6 Viewing NTP Status. . . . 5-33
5.4 Configuring Switch Redundancy and Clustering. . . . 5-34
5.4.1 Configuring Redundancy Settings . . . 5-36
5.4.2 Reviewing Redundancy Status . . . 5-39
5.4.3 Configuring Redundancy Group Membership . . . 5-42
5.4.4 Redundancy Group License Aggregation Rules. . . . 5-46
5.4.5 Managing Clustering Using the Web UI . . . 5-46
5.5 Layer 3 Mobility. . . . 5-48
5.5.1 Configuring Layer 3 Mobility . . . 5-48
5.5.2 Defining the Layer 3 Peer List . . . 5-50
5.5.3 Reviewing Layer 3 Peer List Statistics . . . 5-51
5.5.4 Reviewing Layer 3 MU Status . . . 5-53
5.6 Configuring Self Healing . . . 5-53

5.6.1 Configuring Self Healing Neighbor Details . . . 5-55
5.7 Configuring Switch Discovery . . . 5-57
5.7.1 Configuring Discovery Profiles . . . 5-57
5.7.2 Viewing Discovered Switches . . . 5-60
5.8 Locationing . . . 5-63
5.8.1 RTLS Overview . . . 5-63
5.8.2 SOLE - Smart Opportunistic Location Engine . . . 5-63
5.8.3 Defining Site Parameters . . . 5-64
5.8.4 Configuring SOLE Parameters . . . 5-66
5.8.5 Configuring Aeroscout Parameters . . . 5-67
5.8.6 Configuring Ekahau Parameters . . . 5-69

Chapter 6. Switch Security

6.1 Displaying the Main Security Interface . . . 6-1
6.2 AP Intrusion Detection . . . 6-3
6.2.1 Enabling and Configuring AP Detection . . . 6-3
6.2.2 Approved APs . . . 6-6
6.2.3 Unapproved APs (AP Reported) . . . 6-7
6.2.4 Unapproved APs (MU Reported) . . . 6-9
6.2.5 AP Containment . . . 6-10
6.3 MU Intrusion Detection . . . 6-11
6.3.1 Configuring MU Intrusion Detection . . . 6-11
6.3.2 Viewing Filtered MUs . . . 6-12
6.4 Configuring Firewalls and Access Control Lists . . . 6-14
6.4.1 ACL Overview . . . 6-15
6.4.2 Configuring the Firewall . . . 6-19
6.4.3 Attaching an ACL on a WLAN Interface/Port . . . 6-23
6.4.4 Attaching an ACL Layer 2/Layer 3 Configuration . . . 6-25
6.4.5 Configuring the Role Based Firewall . . . 6-26
6.4.6 Configuring a Role . . . 6-28
6.4.7 Configuring Wireless Filters . . . 6-31
6.4.8 Editing an Existing Wireless Filter . . . 6-33
6.4.9 Adding a new Wireless Filter . . . 6-34
6.4.10 Associating an ACL with a WLAN . . . 6-35
6.4.11 L2 Level Attack Detection and Mitigation . . . 6-36
6.4.12 Configuring WLAN Firewall Rules . . . 6-39
6.4.13 Configuring Denial of Service (DoS) Attack Firewall Rules . . . 6-42
6.4.14 Configuring Firewall Logging Options . . . 6-44
6.4.15 Reviewing Firewall and ACL Statistics . . . 6-46
6.5 Configuring NAT Information . . . 6-49
6.5.1 Defining Dynamic NAT Translations . . . 6-49
6.5.2 Defining Static NAT Translations . . . 6-52
6.5.3 Configuring NAT Interfaces . . . 6-55
6.5.4 Viewing NAT Status . . . 6-56
6.6 Configuring IKE Settings . . . 6-58
6.6.1 Defining the IKE Configuration . . . 6-58
6.6.2 Setting IKE Policies . . . 6-60
6.6.3 Viewing SA Statistics . . . 6-64
6.7 Configuring IPSec VPN . . . 6-65

6.7.1 Defining the IPSec Configuration . . . 6-66
6.7.2 Defining the IPSec VPN Remote Configuration . . . 6-71
6.7.3 Configuring IPSEC VPN Authentication . . . 6-72
6.7.4 Configuring Crypto Maps . . . 6-74
6.7.5 Viewing IPSec Security Associations . . . 6-82
6.8 Configuring the Radius Server . . . 6-84
6.8.1 Radius Overview . . . 6-84
6.8.2 Using the Switch's Radius Server Versus an External Radius . . . 6-86
6.8.3 Defining the Radius Configuration . . . 6-87
6.8.4 Configuring Radius Authentication and Accounting . . . 6-89
6.8.5 Configuring Radius Users . . . 6-92
6.8.6 Configuring Radius User Groups . . . 6-94
6.8.7 Viewing Radius Accounting Logs . . . 6-98
6.9 Creating Server Certificates . . . 6-98
6.9.1 Using Trustpoints to Configure Certificates . . . 6-99
6.9.2 Configuring Trustpoint Associated Keys . . . 6-107
6.10 Configuring Enhanced Beacons and Probes . . . 6-110
6.10.1 Configuring the Beacon Table . . . 6-110
6.10.2 Configuring the Probe Table . . . 6-113
6.10.3 Reviewing Found Beacons . . . 6-114
6.10.4 Reviewing Found Probes . . . 6-115

Chapter 7.Switch Management

7.1 Displaying the Management Access Interface . . . 7-1
7.2 Configuring Access Control . . . 7-2
7.3 Configuring SNMP Access . . . 7-4
7.3.1 Configuring SNMP v1/v2 Access . . . 7-5
7.3.2 Configuring SNMP v3 Access . . . 7-7
7.3.3 Setting SNMP Access Message Parameters . . . 7-9
7.3.4 Accessing SNMP v2/v3 Statistics . . . 7-9
7.4 Configuring SNMP Traps . . . 7-10
7.4.1 Enabling Trap Configuration . . . 7-11
7.4.2 Configuring Trap Thresholds . . . 7-14
7.5 Configuring SNMP Trap Receivers . . . 7-18
7.5.1 Editing SNMP Trap Receivers . . . 7-19
7.5.2 Adding SNMP Trap Receivers . . . 7-19
7.6 Configuring Management Users . . . 7-20
7.6.1 Configuring Local Users . . . 7-20
7.6.2 Configuring Switch Authentication . . . 7-26

Chapter 8.Diagnostics

8.1 Displaying the Main Diagnostic Interface . . . 8-1
8.1.1 Switch Environment . . . 8-2
8.1.2 CPU Performance . . . 8-3
8.1.3 Switch Memory Allocation . . . 8-4
8.1.4 Switch Disk Allocation . . . 8-5
8.1.5 Switch Memory Processes . . . 8-5
8.1.6 Other Switch Resources . . . 8-6

8.2 Configuring System Logging 8-7
8.2.1 Log Options 8-7
8.2.2 File Management 8-9
8.3 Reviewing Core Snapshots 8-13
8.3.1 Transferring Core Snapshots 8-14
8.4 Reviewing Panic Snapshots 8-15
8.4.1 Viewing Panic Details 8-16
8.4.2 Transferring Panic Files 8-16
8.5 Debugging the Applet 8-17
8.6 Configuring a Ping 8-18
8.6.1 Modifying the Configuration of an Existing Ping Test 8-19
8.6.2 Adding a New Ping Test 8-20
8.6.3 Viewing Ping Statistics 8-22

Appendix A Customer Support

Appendix B Adaptive AP

B.1 Adaptive AP Overview B-1
B.1.1 Where to Go From Here B-1
B.1.2 Adaptive AP Management B-2
B.1.3 Types of Adaptive APs B-2
B.1.4 Licensing B-3
B.1.5 Switch Discovery B-3
B.1.6 Securing a Configuration Channel Between Switch and AP B-4
B.1.7 Adaptive AP WLAN Topology B-4
B.1.8 Configuration Updates B-5
B.1.9 Securing Data Tunnels between the Switch and AAP B-5
B.1.10 Adaptive AP Switch Failure B-5
B.1.11 Remote Site Survivability (RSS) B-5
B.1.12 Adaptive Mesh Support B-6
B.1.13 AAP Radius Proxy Support B-7
B.2 Supported Adaptive AP Topologies B-8
B.2.1 Topology Deployment Considerations B-8
B.2.2 Extended WLANs Only B-9
B.2.3 Independent WLANs Only B-9
B.2.4 Extended WLANs with Independent WLANs B-9
B.2.5 Extended VLAN with Mesh Networking B-9
B.3 How the AP Receives its Adaptive Configuration B-9
B.3.1 Adaptive AP Pre-requisites B-10
B.3.2 Configuring the Adaptive AP for Adoption by the Switch B-10
B.3.3 Configuring the Switch for Adaptive AP Adoption B-10
B.4 Establishing Basic Adaptive AP Connectivity B-11
B.4.1 Adaptive AP Configuration B-11
B.4.2 Switch Configuration B-13
B.4.3 Adaptive AP Deployment Considerations B-15
B.4.4 Sample Switch Configuration File for IPSec and Independent WLAN B-16

Appendix C Troubleshooting

C.1 General Troubleshooting . . . C-1
C.1.1 Wireless Switch Issues . . . C-1
C.1.2 Access Port Issues . . . C-4
C.1.3 Mobile Unit Issues . . . C-5
C.1.4 Miscellaneous Issues . . . C-6
C.1.5 System Logging Mechanism . . . C-7
C.2 Troubleshooting SNMP Issues . . . C-7
C.2.1 MIB Browser not able to contact the agent . . . C-7
C.2.2 Not able to SNMP WALK for a GET . . . C-8
C.2.3 MIB not visible in the MIB browser . . . C-8
C.2.4 SNMP SETs not working . . . C-8
C.2.5 Not receiving SNMP traps . . . C-8
C.2.6 Additional Configuration . . . C-8
C.3 Security Issues . . . C-8
C.3.1 Switch Password Recovery . . . C-8
C.3.2 RADIUS Troubleshooting . . . C-9
C.3.3 Troubleshooting RADIUS Accounting Issues . . . C-11
C.4 Rogue AP Detection Troubleshooting . . . C-11
C.5 Troubleshooting Firewall Configuration Issues . . . C-12

Appendix D “How To” Tutorials

D.1 Adopted AP300 Sensor Conversion . . . D-1
D.1.1 About the Motorola AirDefense System . . . D-2
D.1.2 Defining an AP300 Sensor Conversion Configuration . . . D-2
D.1.3 RF Switch Running Configuration . . . D-8
D.2 Integrated WLAN RTLS . . . D-13
D.2.1 Wi-Fi Location Determination . . . D-14
D.2.2 Location Presentation . . . D-14
D.2.3 Network Topology . . . D-15
D.2.4 Defining an Integrated WLAN RTLS Configuration . . . D-16
D.2.5 Baseline Configurations . . . D-27
D.3 MU to MU Disallow . . . D-37
D.3.1 Defining an MU to MU Disallow Configuration . . . D-38
D.3.2 RF Switch Running Configuration . . . D-40
D.4 Secure Beacons . . . D-46
D.4.1 Configuring a Secure Beacon Deployment . . . D-47
D.4.2 RF Switch Running Configuration . . . D-49
D.5 Secure Device Management . . . D-55
D.5.1 Configuring a Secure Device Deployment . . . D-56
D.5.2 RF Switch Running Configuration . . . D-68
D.6 Secure WISPe . . . D-74
D.6.1 Shared Secrets . . . D-75
D.6.2 Pre Staging Mode . . . D-75
D.6.3 Applications . . . D-76
D.6.4 Restrictions . . . D-76
D.6.5 Secure WISPe Configuration . . . D-76
D.6.6 RF Switch Running Configuration . . . D-86
D.7 Wireless IDS . . . D-92

D.7.1 Unauthorized Access Point Detection D-93
D.7.2 Unauthorized Access Point Containment D-94
D.7.3 Wireless Intrusion Detection D-94
D.7.4 Applications D-95
D.7.5 Restrictions D-95
D.7.6 Configuring a Wireless IDS Deployment D-96
D.8 Wireless Filters D-114
D.8.1 Configuring a Wireless Filter D-114
D.9 802.11i Support D-126
D.9.1 Applications D-127
D.9.2 Restrictions D-127
D.9.3 Configuring 802.11i Support D-127
D.9.4 RF Switch Running Configuration D-135

1

Overview

A Motorola RF Switch is a centralized management solution for wireless networking. It connects to non-legacy Access Ports through Layer 2 or Layer 3 (Layer 2 is preferable, if the situation allows it).

Access ports function as radio antennas for data traffic management and routing. System configuration and intelligence for the wireless network resides with the switch. The switch uses Access Ports to bridge data to and from wireless devices. The wireless switch applies appropriate policies to data packets before forwarding them to their destination.

All data packets to and from wireless devices are processed by the switch, where appropriate policies are applied before they are decapsulated and sent to their destination.

Access port configuration is managed by the switch through a Web UI *Graphical User Interface* (GUI), SNMP or the switch *Command Line Interface* (CLI).

SWITCH NOTE: The discussion of the switch Web UI within this guide is presented generically, making it equally relevant to both the RFS6000 and RFS7000 switch platforms. However, some subtle differences do exist between these baselines. These differences are noted within the specific GUI elements impacted. When these differences are noted, the options available to each switch baseline are described in detail.

1.1 Hardware Overview

The RFS6000 and RFS7000 are rack-mountable devices that manage all inbound and outbound traffic on the wireless network. They provide security, network service and system management applications.

Unlike traditional wireless infrastructure devices that reside at the edge of a network, the switch uses centralized, policy-based management to apply sets of rules or actions to all devices on the wireless network. The switch collects management "intelligence" from individual Access Ports/Points and moves the collected information to the centralized switch.

Access ports (APs) are 48V Power-over-Ethernet devices connected to the switch by an Ethernet cable. An Access Port receives 802.11x data from MUs and forwards the data to the switch which applies the appropriate policies and routes the packets to their destinations.

Access ports do not have software or firmware upon initial receipt from the factory. When the Access Port is first powered on and cleared for the network, the switch initializes the Access Port and installs a small firmware file automatically. Therefore, installation and firmware upgrades are automatic and transparent.

1.1.1 Physical Specifications

The physical dimensions and operating parameters of the RFS6000 include:

Width	440mm (17.32 in)
Height	44.45mm (1.75 in)
Depth	390.8mm (15.38 in)
Weight	6.35 Kg (14 lbs)
Operating Temperature	0°C - 40°C (32°F - 104°F)
Operating Humidity	5% - 85% RH, non-condensing

The physical dimensions and operating parameters of the RFS7000 include:

Width	440mm (17.32 in)
Height	44.45mm (1.75 in)
Depth	390.8mm (15.38 in)
Weight	6.12 Kg (13.5 lbs)
Operating Temperature	0°C - 40°C (32°F - 104°F)
Operating Humidity	5% - 85% RH, non-condensing

A power cord is not supplied with a RFS6000 or RFS7000 model switch. Use only a correctly rated power cord certified for the country of operation.

1.1.1.1 Power Protection

To best protect the switch from unexpected power surges or other power-related problems, ensure the switch installation meets the following guidelines:

- *If possible, use a dedicated circuit to protect data processing equipment*. Commercial electrical contractors are familiar with wiring for data processing equipment and can help with the load balancing of dedicated circuits.
- *Install surge protection*. Use a surge protection device between the electricity source and the switch.
- *Install an Uninterruptible Power Supply (UPS)*. A UPS provides continuous power during a power outage. Some UPS devices have integral surge protection. UPS equipment requires periodic maintenance to ensure reliability.

1.1.1.2 Cabling Requirements

A minimum of one category 6 Ethernet cables (not supplied) are required to connect the switch to the LAN and WLAN. The cable(s) are used with the Ethernet ports on the front panel of the switch.

SWITCH NOTE: Motorola recommends connecting via the *Management Ethernet* (ME) interface to better ensure secure and easy switch management. The ME interface is connected to the management VLAN, and is therefore separate from production VLANs.

SWITCH NOTE: On the RFS6000, the *Uplink* (UP) port is the preferred method of connecting the switch to the network. The Uplink port has its own dedicated 1Gbps connection which is unaffected by internal traffic across the GE ports.

The console cable included with the switch connects the switch to a computer running a serial terminal emulator program to access the switch's *Command Line Interface* (CLI) for initial configuration. An initial configuration is described within the *Installation Guide* shipped with each switch.

1.2 Software Overview

The switch includes a robust set of features. The features are listed and described in the following sections:

- *Infrastructure Features*
- *Wireless Switching*
- *Wired Switching*
- *Management Features*
- *Security Features*
- *Supported Access Ports/Points*

NOTE: The Motorola RF Management Software is a recommended utility to plan the deployment of the switch and view its configuration once operational in the field. Motorola RFMS can help optimize the positioning and configuration of a switch in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Motorola Web site.

1.2.1 Infrastructure Features

The switch includes the following Infrastructure features:

- *Installation Feature*

- *Licensing Support*
- *Configuration Management*
- *Diagnostics*
- *Serviceability*
- *Tracing / Logging*
- *Process Monitor*
- *Hardware Abstraction Layer and Drivers*
- *Redundancy*
- *Secure Network Time Protocol (SNTP)*
- *Password Recovery*

1.2.1.1 Installation Feature

The upgrade/downgrade of the switch can be performed at boot time using one of the following methods:

- *Web UI*
- *DHCP*
- *CLI*
- *SNMP*
- *Patches*

The switch has sufficient non-volatile memory to store two firmware images. Having a second firmware image provides a backup in case of failure of the primary image. It also allows for testing of new firmware on a switch with the ability to easily revert to a previous image.

1.2.1.2 Licensing Support

The following licensing information is utilized when upgrading the switch

- The maximum numbers of AP licenses a switch can adopt is dependant on the number purchased

1.2.1.3 Configuration Management

The switch supports the redundant storage of configuration files to protect against corruption during a write operation and ensure (at any given time) a valid configuration file exists. If writing the configuration file fails, it is rolled back and a pre-write file is used.

Text Based Configuration

The configuration is stored a in human readable format (as a set of CLI commands).

1.2.1.4 Diagnostics

The following diagnostics are available:

1. *In-service Diagnostics* – In-service diagnostics provide a range of automatic health monitoring features ensuring both the system hardware and software are in working order. In-service-diagnostics continuously monitor available physical characteristics (as detailed below) and issue log messages when warning or error thresholds are reached. There are three types of in-service diagnostics:
    - *Hardware* – Ethernet ports, chip failures, system temperature via the temperature sensors provided by the hardware, etc.

- *Software* – CPU load, memory usage, etc.
- *Environmental* – CPU and air temperature, fans speed, etc.

2. *Out-of-service Diagnostics* – Out-of-service diagnostics are a set of intrusive tests run from the user interface. Out-of-service diagnostics cannot be run while the switch is in operation. Intrusive tests include:
   - *Ethernet loopback tests*
   - *RAM tests, Real Time Clock tests, etc.*
3. *Manufacturing Diagnostics* – Manufacturing diagnostics are a set of diagnostics used by manufacturing to inspect quality of hardware.

1.2.1.5 Serviceability

A special set of Service CLI commands are available to provide additional troubleshooting capabilities for service personnel (access to Linux services, panic logs, etc.). Only authorized users or service personnel are provided access to the Service CLI.

A built-in Packet Sniffer enables service personnel and users to capture incoming and outgoing packets in a buffer.

The switch also collects statistics for RF activity, Ethernet port activity etc. RF statistics include roaming stats, packet counters, octets tx/rx, signal, noise SNR, retry, and information for each MU.

1.2.1.6 Tracing / Logging

Log messages are well-defined and documented system messages with various destinations. They are numbered and referenced by ID. Each severity level group, can be configured separately to go to either the serial console, telnet interface, log file or remote syslog server.

Trace messages are more free-form and are used mainly by support personnel for tracking problems. They are enabled or disabled via CLI commands. Trace messages can go to a log file, the serial console, or the current tty.

Log and trace messages are interleaved in the same log file, so chronological order is preserved. Log and trace messages from different processes are similarly interleaved in the same file for the same reason.

Log message format is similar to the format used by syslog messages (RFC 3164). Log messages include message severity, source (facility), the time the message was generated and a textual message describing the situation triggering the event. For more information on using the switch logging functionality, see *Configuring System Logging on page 8-7*.

1.2.1.7 Process Monitor

The switch Process Monitor checks to ensure processes under its control are up and running. Each monitored process sends periodic heartbeat messages. A process that is down (due to a software crash or stuck in an endless loop) is detected when its heartbeat is not received. Such a process is terminated (if still running) and restarted (if configured) by the Process Monitor.

1.2.1.8 Hardware Abstraction Layer and Drivers

The *Hardware Abstraction Layer* (HAL) provides an abstraction library with an interface hiding hardware/ platform specific data. Drivers include platform specific components such as Ethernet, Flash Memory storage and thermal sensors.

1.2.1.9 Redundancy

Using the switch redundancy, up to 12 switches can be configured in a redundancy group (and provide group monitoring). In the event of a switch failure, an existing cluster member assumes control. Therefore, the switch supported network is always up and running even if a switch fails or is removed for maintenance or a software upgrade.

The following redundancy features are supported:

- Up to 12 switch redundancy members are supported in a single group. Each member is capable of tracking statistics for the entire group in addition to their own.
- Each redundancy group is capable of supporting an Active/Active configuration responsible for group load sharing.
- Members within the same redundancy group can be deployed across different subnets.
- APs are load balanced across members of the group.
- Licenses are aggregated across the group. When a new member joins the group, the new member can leverage the Access Port adoption license(s) of existing members.
- Each member of the redundancy group (including the reporting switch) is capable of displaying cluster performance statistics for all members in addition to their own.
- Centralized redundancy group management using the switch CLI.

For more information on configuring the switch for redundancy support, see *Configuring Switch Redundancy and Clustering on page 5-34*.

1.2.1.10 Secure Network Time Protocol (SNTP)

Secure Network Time Protocol (SNTP) manages time and/or network clock synchronization within the switch managed network. SNTP is a client/server implementation. The switch (a SNTP client) periodically synchronizes its clock with a master clock (an NTP server). For example, the switch resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server. Time synchronization is recommended for the switch's network operations. The following holds true:

- The switch can be configured to provide NTP services to NTP clients.
- The switch can provide NTP support for user authentication.
- *Secure Network Time Protocol* (SNTP) clients can be configured to synchronize switch time with an external NTP server.

For information on configuring the switch to support SNTP, see *Configuring Secure NTP on page 5-24*.

1.2.1.11 Password Recovery

The switch has a provision allowing it to restore its factory default configuration if your password is lost. In doing so however the current configuration is erased, but can be restored assuming if has been exported to an external location. For information on password recovery, see *Switch Password Recovery on page 2-2*.

1.2.2 Wireless Switching

The switch includes the following wireless switching features:

- *Adaptive AP*
- *Physical Layer Features*

- *Rate Limiting*
- *Proxy-ARP*
- *HotSpot / IP Redirect*
- *IDM (Identity Driven Management)*
- *Voice Prioritization*
- *Self Healing*
- *Wireless Capacity*
- *AP and MU Load Balancing*
- *Wireless Roaming*
- *Power Save Polling*
- *QoS*
- *Wireless Layer 2 Switching*
- *Automatic Channel Selection*
- *WMM-Unscheduled APSD*
- *Multiple VLANs per WLAN*

1.2.2.1 Adaptive AP

An adaptive AP (AAP) is an AP-5131 or AP-7131 Access Point adopted by a wireless switch. The management of an AAP is conducted by the switch, once the Access Point connects to the switch and receives its AAP configuration.

An AAP provides:

- *local 802.11 traffic termination*
- *local encryption/decryption*
- *local traffic bridging*
- *tunneling of centralized traffic to the wireless switch*

The connection between the AAP and the switch can be secured using IPSec depending on whether a secure WAN link from a remote site to the central site already exists.

The switch can be discovered using one of the following mechanisms:

- *DHCP*
- *Switch fully qualified domain name (FQDN)*
- *Static IP addresses*

The benefits of an AAP deployment include:

- *Centralized Configuration Management & Compliance* - Wireless configurations across distributed sites can be centrally managed by the wireless switch or cluster.
- *WAN Survivability* - Local WLAN services at a remote sites are unaffected in the case of a WAN outage.
- *Securely extend corporate WLAN's to stores for corporate visitors* - Small home or office deployments can utilize the feature set of a corporate WLAN from their remote location.

- *Maintain local WLAN's for specific applications* - WLANs created and supported locally can be concurrently supported with your existing infrastructure.

For an overview of AAP and how it is configured and deployed using the switch and Access Point, see *Adaptive AP Overview*.

1.2.2.2 Physical Layer Features

802.11a

- *DFS Radar Avoidance – Dynamic Frequency Selection* (DFS) is mandatory for WLAN equipment intended to operate in the frequency bands 5150 MHz to 5350 MHz and 5470 MHz to 5725 MHz when in countries of the EU.

  The purpose of DFS is:

  - Detect interference from other systems and avoid co-channeling with those systems (most notably radar systems).
  - Provide uniform spectrum loading across all devices.

    This feature is enabled automatically when the country code indicates that DFS is required for at least one of the frequency bands that are allowed in the country.
- *TPC – Transmit Power Control* (TPC) meets the regulatory requirement for maximum power and mitigation for each channel. TPC functionality is enabled automatically for every AP that operates on the channel.

802.11bg

- *Dual mode b/g protection* – ERP builds on the payload data rates of 1 and 2 Mbit/s that use DSSS modulation and builds on the payload data rates of 1, 2, 5.5, and 11 Mbit/s, that use DSSS, CCK, and optional PBCC modulations. ERP provides additional payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s. The transmission and reception capability for 1, 2, 5.5, 11, 6, 12, and 24 Mbit/s data rates is mandatory.

  Two additional optional ERP-PBCC modulation modes with payload data rates of 22 and 33 Mbit/s are defined. An ERP-PBCC station may implement 22 Mbit/s alone or 22 and 33 Mbit/s. An optional modulation mode (known as DSSS-OFDM) is also incorporated with payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s.
- *Short slot protection* – The slot time is 20 µs, except an optional 9 µs slot time may be used when the BSS consists of only ERP STAs capable of supporting this option. The optional 9 µs slot time should not be used if the network has one or more non-ERP STAs associated. For IBSS, the Short Slot Time field is set to 0, corresponding to a 20 µs slot time.

1.2.2.3 Rate Limiting

Rate Limiting limits the maximum rate sent to or received from the wireless network per mobile unit. 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 the radius server using Motorola vendor specific attributes. The switch extracts the rate limits from radius server response. When such attributes are not present, the global settings on the switch are then applied.

1.2.2.4 Proxy-ARP

Proxy ARP is provided for MU's whose IP address is known. The WLAN generates an ARP reply on behalf of a MU (if the MU's IP address is known). The ARP reply contains the MAC address of the MU (not the MAC

address of switch). Thus, the MU does not awaken to send ARP replies (increasing MU battery life and conserving wireless bandwidth).

If an MU goes into PSP without transmitting at least one packet, its Proxy ARP will not work.

1.2.2.5 HotSpot / IP Redirect

A hotspot is a Web page users are forced to visit before they are granted access to the Internet. With the advent of Wi-Fi enabled client devices (such as laptops and PDAs) commercial hotspots are common and can be found at many airports, hotels and coffee shops. The hotspot re-directs the user's traffic on hotspot enabled WLANs to a web page that requires them to authenticate before granting access to the WLAN. The following is a typical sequence for hotspot access:

1. A visitor with a laptop requires hotspot access at a site.
2. A user ID/ Password and hotspot ESSID is issued by the site receptionist or IT staff.
3. The user connects their laptop to this ESSID.
4. The laptop receives its IP configuration via DHCP.
5. The user opens a Web browser and connects to their home page.
6. The switch re-directs them to the hotspot Web page for authentication.
7. The user enters their User ID/ Password.
8. A Radius server authenticates the user.
9. Upon successful authentication, the user is directed to a Welcome Page that lists (among other things) an Acceptable Use Policy.
10. The user agrees to the usage terms and is granted access to the Internet. (or other network services).

To setup a hotspot, create a WLAN ESSID and select Hotspot authentication from the Authentication menu. This is simply another way to authenticate a WLAN user, as it would be impractical to authenticate visitors using 802.1x. For information on configuring a hotspot, see *Configuring Hotspots on page 4-35*.

1.2.2.6 IDM (Identity Driven Management)

Radius authentication is performed for all protocols using a Radius-based authentication scheme (such as EAP). Identity driven management is provided using a Radius client. The following IDMs are supported:

- *User based SSID authentication* — Denies authentication to MUs if associated to a ESSID configured differently by their Radius server.
- U*ser based VLAN assignment* — Allows the switch to extract VLAN information from the Radius server.
- *User based QoS* — Enables QoS for the MU based on settings within the Radius Server.

1.2.2.7 Voice Prioritization

The switch has the capability of having its QoS policy configured to prioritize network traffic requirements for associated MUs. Use QoS to enable voice prioritization for devices using voice as its transmission priority.

Voice prioritization allows you to assign priority to voice traffic over data traffic, and (if necessary) assign legacy voice supported devices (non WMM supported voice devices) additional priority.

Currently voice support implies the following:

- *Spectralink voice prioritization* - Spectralink sends packets that allow the switch to identify these MU's as voice MU's. Thereafter, any UDP packet sent by these MU's is prioritized ahead of data.
- *Strict priority* - The prioritization is strict.
- *Multicast prioritization* - Multicast frames that match a configured multicast mask bypass the PSP queue. This features permits intercom mode operation without delay (even in the presence of PSP MU's).

For more information on configuring voice prioritization for a target WLAN, see *Configuring WMM on page 4-67*.

1.2.2.8 Self Healing

Self Healing is the ability to dynamically adjust the RF network by modifying transmit power and/or supported rates upon an AP failure.

In a typical RF network deployment, APs are configured for Transmit Power below their maximum level. This allows the Tx Power to be increased when there is a need to increase coverage when an AP fails.

When an AP fails, the Tx Power/Supported rates of APs neighboring the failed AP are adjusted. The Tx power is increased and/or Supported rates are decreased. When the failed AP becomes operational again, Neighbor AP's Tx Power/Supported rates are brought back to the levels before the self healing operation changed them.

The switch detects an AP failure when:

- *AP stops sending heartbeats.*
- *AP beacons are no longer being sent. This is determined when other detector APs are no longer hearing beacons from a particular AP.*

Configure 0 (Zero) or more APs to act as either:

- *Detector APs* — Detector APs scan all channels and send beacons to the switch which uses the information for self-healing.
- *Neighbor APs* — When an AP fails, neighbor APs assist in self healing.
- *Self Healing Actions* — When an AP fails, actions are taken on the neighbor APs to do self-healing.

Detector APs

Configure an AP in either – Data mode (the regular mode) or Detector mode.

In Detector mode, an AP scans all channels at a configurable rate and forwards received beacons the switch. The switch uses the information to establish a *receive signal strength baseline* over a period of time and initiates self-healing procedures (if necessary).

Neighbor Configuration

Neighbor detect is a mechanism allowing an AP to detect its neighbors as well as their signal strength. This enables you to verify your installation and configure it for self-healing when an AP fails.

Self Healing Actions

If AP1 detects AP2 and AP3 as its neighbors, you can assign failure actions to AP2 and AP3 whenever AP1 fails.

Assign up to four self healing actions:

1. No action
2. Decrease supported rates
3. Increase Tx power
4. Both 2 and 3.

You can specify the Detector AP (AP2 or AP3) to stop detecting and adopt the RF settings of the failed AP. For more information on configuring self healing, see *Configuring Self Healing on page 5-53*.

1.2.2.9 Wireless Capacity

Wireless capacity specifies the maximum numbers of MUs, Access Ports and wireless networks usable by a switch. Wireless capacity is largely independent of performance. Aggregate switch performance is divided among the switch clients (MUs and Access Ports) to find the performance experienced by a given user. Each switch platform is targeted at specific market segments, so the capacity of each platform is chosen appropriately. Wireless switch capacity is measured by:

- *The maximum number of WLANs per switch*
- *The maximum number of Access Ports adopted per switch*
- *The maximum number of MUs per switch*
- *The maximum number of MUs per Access Port*

The actual number of Access Ports adoptable by a switch is defined by the switch licenses or the total licenses in the cluster in which this switch is a member.

1.2.2.10 AP and MU Load Balancing

Fine tune a network to evenly distribute data and/or processing across available resources. Refer to the following:

- *MU Balancing Across Multiple APs*
- *AP Balancing Across Multiple Switches*

MU Balancing Across Multiple APs

Per the 802.11 standard, AP and MU association is a process conducted independently of the switch. 802.11 provides message elements used by the MU firmware to influence roaming decisions. The switch implements the following MU load balancing techniques:

- *802.11e admission control* — 1 byte: channel utilization % and 1 byte: MU count is sent in QBSS Load Element in beacons to MU.
- *Motorola load balancing element (proprietary)* — 2 byte: MU Count are sent in beacon to MU.

AP Balancing Across Multiple Switches

At adoption, the AP solicits and receives multiple adoption responses from the switches on the network. These adoption responses contain preference and loading information the AP uses to select the optimum switch to be adopted by. Use this mechanism to define which APs are adopted by which switches. By default, the adoption algorithm generally distributes AP adoption evenly among the switches available.

NOTE: Port adoption per switch is determined by the number of licenses acquired.

For more information on Access Port adoption in a layer 3 environment, see *Configuring Layer 3 Access Port Adoption on page 4-136*.

1.2.2.11 Wireless Roaming

The following types of wireless roaming are supported by the switch:

- *Interswitch Layer 2 Roaming*
- *Interswitch Layer 3 Roaming*
- *Fast Roaming*
- *International Roaming*
- *MU Move Command*
- *Power Save Polling*

Interswitch Layer 2 Roaming

An associated MU (connected to a switch) can roam to another Access Port connected to a different switch. Both switches must be on the same Layer 2 domain. Authentication information is not shared between the switches, nor are buffered packets on one switch transferred to the other. Pre-authentication between the switch and MU allows faster roaming.

Interswitch Layer 3 Roaming

Interswitch Layer 3 roaming allows MUs to roam between switches which are not on the same LAN or IP subnet without the MUs or the rest of the network noticing. This allows switches to be placed in different locations on the network without having to extend the MU VLANs to every switch.

Fast Roaming

Using 802.11i can speed up the roaming process from one AP to another. Instead of doing a complete 802.1x authentication each time a MU roams between APs, 802.11i allows a MU 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 APs, Opportunistic Key Caching allows multiple APs to share PMKs amongst themselves. This allows an MU to roam to an AP it has not previously visited and reuse a PMK from another AP to skip the 802.1x authentication.

International Roaming

The wireless switch supports international roaming per the 802.11d specification.

MU Move Command

As a value added proprietary feature between Motorola infrastructure products and Motorola MUs, a *move* command has been introduced. The move command permits an MU to roam between ports connected to the same switch without the need to perform the full association and authentication defined by the 802.11 standard. The move command is a simple packet up/packet back exchange with the Access Port. Verification of this feature is dependent on its implementation in one or more mobile units.

1.2.2.12 Power Save Polling

An MU uses *Power Save Polling* (PSP) to reduce power consumption. When an MU is in PSP mode, the switch buffers its packets and delivers them using the DTIM interval. The PSP-Poll packet polls the AP for buffered packets. The PSP null data frame is used by the MU to signal the current PSP state to the AP.

1.2.2.13 QoS

QoS provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic.

If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when the switch's bandwidth is shared by different users and applications.

QoS helps ensure each WLAN on the switch receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards MUs are classified into categories such as Management, Voice and Data. Packets within each category are processed based on the weights defined for each WLAN.

The switch supports the following QoS mechanisms:

802.11e QoS

802.11e enables real-time audio and video streams to be assigned a higher priority over data traffic. The switch supports the following 802.11e features:

- *Basic WMM*
- *WMM Linked to 802.1p Priorities*
- *WMM Linked to DSCP Priorities*
- *Fully Configurable WMM*
- *Admission Control*
- *Unscheduled-APSD*
- *TSPEC Negotiation*
- *Block ACKQBSS Beacon Element*

802.1p Support

802.1p is a standard for providing QoS in 802-based networks. 802.1p uses three bits to allow switches to re-order packets based on priority level.

Voice QoS

When switch resources are shared between a *Voice over IP* (VoIP) conversation and a file transfer, bandwidth is normally exploited by the file transfer, thus reducing the quality of the conversation or even causing it to

disconnect. With QoS, a VoIP conversation (a real-time session), receives priority, maintaining a high level of voice quality. Voice QoS ensures:

- *Strict Priority*
- *Spectralink Prioritization*
- *VOIP Prioritization (IP ToS Field)*
- *Multicast Prioritization*

Data QoS

The switch supports the following data QoS techniques:

- *Egress Prioritization by WLAN*
- *Egress Prioritization by ACL*

DCSCP to AC Mapping

The switch provides arbitrary mapping between *Differentiated Services Code Point* (DCSCP) values and WMM Access Categories. This mapping can be set manually.

1.2.2.14 Wireless Layer 2 Switching

The switch supports the following layer 2 wireless switching techniques:

- *WLAN to VLAN*
- *MU User to VLAN*
- *WLAN to GRE*

1.2.2.15 Automatic Channel Selection

Automatic channel selection works sequentially as follows:

1. When a new AP is adopted, it scans each channel. However, the switch does not forward traffic at this time.
2. The switch then selects the least crowded channel based on the noise and traffic detected on each channel.
3. The algorithm used is a simplified maximum entropy algorithm for each radio, where the signal strength from adjoining AP's/MU's associated to adjoining AP's is minimized.
4. The algorithm ensures adjoining AP's are as far away from each other as possible (in terms of channel assignment).

NOTE: Individual radios can be configured to perform automatic channel selection.

1.2.2.16 WMM-Unscheduled APSD

This feature is also known as WMM Power Save or WMM-UPSD (*Unscheduled Power Save Delivery*). WMM-UPSD defines an unscheduled service period, which are contiguous periods of time during which the switch is expected to be awake. If the switch establishes a downlink flow and specifies UPSD power management, it requests (and the AP delivers) buffered frames associated with that flow during an unscheduled service period. The switch initiates an unscheduled service period by transmitting a trigger frame. A trigger frame is defined as a data frame (e.g. an uplink voice frame) associated with an uplink flow

with UPSD enabled. After the AP acknowledges the trigger frame, it transmits the frames in its UPSD power save buffer addressed to the triggering switch.

UPSD is well suited to support bi-directional frame exchanges between a voice STA and its AP.

1.2.2.17 Multiple VLANs per WLAN

The switch permits the mapping of a WLAN to more than one VLAN. When a MU associates with a WLAN, the MU is assigned a VLAN by means of load balance distribution. The VLAN is picked from a pool assigned to the WLAN. The switch tracks the number of MUs per VLAN, and assigns the least used/loaded VLAN to the MU. This number is tracked on a per-WLAN basis.

A broadcast key, unique to the VLAN, encrypts packets coming from the VLAN. If two or more MUs are on two different VLANs, they both hear the broadcast packet, but only one can decrypt it. The switch provides each MU a unique VLAN broadcast key as part of the WPA2 handshake or group key update message of a WPA handshake.

Limiting Users Per VLAN

Not all VLANs within a single WLAN must have the same DHCP pool size. Assign a user limit to each VLAN to allow the mapping of different pool sizes.

Specify the VLAN user limit. This specifies the maximum number of MUs associated with a VLAN (for a particular WLAN). When the maximum MU limit is reached, no more MUs can be assigned to that VLAN.

Packet Flows

There are four packet flows supported when the switch is configured to operate with multiple VLAN per WLAN:

- *Unicast From Mobile Unit* – Frames are decrypted, converted from 802.11 to 802.3 and switched to the wired side of the VLAN dynamically assigned to the mobile device. If the destination is another mobile device on the wireless side, the frame is encrypted and switched over the air.
- *Unicast To Mobile Unit* – The frame is checked to ensure the VLAN is same as that assigned to the mobile device. It is then converted to an 802.11 frame, encrypted, and sent over the air.
- *Multicast/Broadcast From Mobile Unit* – The frame is treated as a unicast frame from the MU, with the exception that it is encrypted with the per-VLAN broadcast key and then transmitted over the air.
- *Multicast/Broadcast from Wired Side* – If the frame comes from a VLAN mapped to the WLAN, it's encrypted using a per-VLAN broadcast key and transmitted over the air. Only MUs on that VLAN have a broadcast key that can decrypt this frame. Other MUs receive it, but discard it.

  In general, when there are multiple VLANs mapped to the same WLAN, the broadcast buffer queue size scales linearly to accommodate a potential increase in the broadcast packet stream.

Roaming within the Switch

When a MU is assigned to a VLAN, the switch registers the VLAN assignment in its credential cache. If the MU roams, it is assigned back to its earlier assigned VLAN. The cache is flushed upon detected MU inactivity or if the MU associates over a different WLAN (on the same switch).

Roaming across a Cluster

MUs roam amongst switch cluster members. The switch must ensure a VLAN remains unchanged as an MU roams. This is accomplished by passing MU VLAN information across the cluster using the interface used by a hotspot. It automatically passes the username/password across the credential caches of the member

switches. This ensures a VLAN MU association is maintained even while the MU roams amongst cluster members.

Roaming across a Layer 3 Mobility Domain

When an MU roams amongst switches in different Layer 3 mobility domains, Layer 3 ensures traffic is tunneled back to the correct VLAN (on the home switch).

Interaction with Radius Assigned VLANs

Multiple VLANs per WLAN can co-exist with VLANs assigned by a Radius server. Upon association, an MU is assigned to a VLAN from a pool of available VLANs. When the Radius server assigns the user another VLAN, MU traffic is forwarded to that VLAN.

When 802.1x is used, traffic from the MU is dropped until authentication is completed. None of the MU data is switched onto the temporarily VLAN. A Radius assigned VLAN overrides the statically assigned VLAN.

If the Radius assigned VLAN is among the VLANs assigned to a WLAN, it is available for VLAN assignment in the future. If the Radius assigned VLAN is not one of the VLANs assigned to a WLAN, it is not available for future VLAN assignment. To configure Multiple VLANs for a single WLAN, see *Assigning Multiple VLANs per WLAN on page 4-31*.

1.2.3 Wired Switching

The switch includes the following wired switching features:

- *DHCP Servers*
- *DHCP User Class Options*
- *DDNS*
- *VLAN Enhancements*
- *Interface Management*

1.2.3.1 DHCP Servers

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 to which they are attached. Each subnet may 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 a DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an pre-determined interval. Before a lease expires, 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. For information on defining the switch DHCP configuration, see *DHCP Server Settings on page 5-3*.

1.2.3.2 DHCP User Class Options

A DHCP Server groups clients based on defined user-class option values. Clients with a defined set of user-class values are segregated by class. The 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. For more information, see *Configuring the DHCP User Class on page 5-19*.

1.2.3.3 DDNS

Dynamic DNS (DDNS) keeps a domain name linked to a changing IP address. Typically, when a user connects to a network, the user's ISP assigns it an unused IP address from a pool of IP addresses. This address is only valid for a short period. Dynamically assigning IP addresses increases the pool of assignable IP addresses. DNS maintains a database to map a given name to an IP address used for communication on the Internet. The dynamic assignment of IP addresses makes it necessary to update the DNS database to reflect the current IP address for a given name. Dynamic DNS updates the DNS database to reflect the correct mapping of a given name to an IP address.

1.2.3.4 VLAN Enhancements

The switch has incorporated the following VLAN enhancements:

- Network interfaces operate in either trunk or access modes.
- A network interface in access mode can only send and receive untagged packets.
- A trunk port can now receive both tagged and untagged packets. Each ethernet port is assigned a native VLAN.
- You can now configure a set of allowed VLANs on a trunk port. Packets received on this port that belong to other VLANs are discarded.

1.2.3.5 Interface Management

The switch's physical interfaces auto-negotiate speed and duplex. The switch also allows:

- Manual bandwidth configuration of a physical interface speed to 10/100/1000Mbps.
- Manual duplex configuration of a physical interface to Full Duplex or Half Duplex.
- Manual configuration of administrative shutdown of a physical interface.

1.2.4 Management Features

The switch supports the following management features:

- A secure, browser-based management console
- A *Command Line Interface* (CLI) accessible via the serial port or through Telnet or a *Secure Shell* (SSH) application
- A CLI Service mode enabling the capture of system status information that can be sent to Motorola personnel for use in problem resolution
- The support for *Simple Network Management Protocol* (SNMP) version 3 as well as SNMP version 2
- Upload and download of Access Port firmware and configuration files using TFTP, FTP, SFTP and HTTP.
- Transfer of firmware and configuration files using Compact Flash (RFS7000 only) or USB (RFS6000 and RFS7000 platforms only)
- The graphing of wireless statistics
- A GUI dashboard summary of system status
- Multi switch management via MSP application

- Heat map support for RF deployment
- Secure guest access with specific permission intervals
- Switch discovery enabling users to discover each Motorola switch on the specified network.

1.2.5 Security Features

Switch security can be classified into wireless security and wired security.

The switch includes the following wireless security features:

- *Encryption and Authentication*
- *MU Authentication*
- *Secure Beacon*
- *MU to MU Disallow*
- *802.1x Authentication*
- *WIPS*
- *Rogue AP Detection*

The switch includes the following wired security features:

- *ACLs*
- *Local Radius Server*
- *IPSec VPN*
- *NAT*
- *Certificate Management*
- *NAC*

1.2.5.1 Encryption and Authentication

The switch can implement the following encryption and authentication types:

- *WEP*
- *WPA*
- *WPA2*
- *Keyguard-WEP*

WEP

Wired Equivalent Privacy (WEP) is an encryption scheme used to secure wireless networks. WEP was intended to provide comparable confidentiality to a traditional wired network, hence the name. WEP had many serious weaknesses and hence was superseded by *Wi-Fi Protected Access* (WPA). Regardless, WEP still provides a level of security that can deter casual snooping. For more information on configuring WEP for a target WLAN, see *Configuring WEP 64 on page 4-56* or *Configuring WEP 128 / KeyGuard on page 4-57*.

WEP uses passwords entered manually at both ends (Pre Shared Keys). Using the RC4 encryption algorithm, WEP originally specified a 40-bit key, but was later boosted to 104 bits. Combined with a 24-bit initialization vector, WEP is often touted as having a 128-bit key.

WPA

WPA is designed for use with an 802.1X authentication server, which distributes different keys to each user. However, it can also be used in a less secure *pre-shared key* (PSK) mode, where every user is given the same passphrase.

WPA uses *Temporal Key Integrity Protocol* (TKIP), which dynamically changes keys as the system is used. When combined with the much larger Initialization Vector, it defeats well-known key recovery attacks on WEP. For information on configuring WPA for a WLAN, see *Configuring WPA/WPA2 using TKIP and CCMP on page 4-59*.

WPA2

WPA2 uses a sophisticated key hierarchy that generates new encryption keys each time a MU associates with an Access Point. Protocols including 802.1X, EAP and Radius are used for strong authentication. WPA2 also supports the TKIP and AES-CCMP encryption protocols. For information on configuring WPA for a WLAN, see *Configuring WPA/WPA2 using TKIP and CCMP on page 4-59*.

Keyguard-WEP

KeyGuard is Motorola's proprietary dynamic WEP solution. Motorola (upon hearing of the vulnerabilities of WEP) developed a non standard method of rotating keys to prevent compromises. Basically, KeyGuard is TKIP without the message integrity check. KeyGuard is proprietary to Motorola MUs only. For information on configuring KeyGuard for a WLAN, see *Configuring WEP 128 / KeyGuard on page 4-57*.

1.2.5.2 MU Authentication

The switch uses the following authentication schemes for MU association:

- *Kerberos*
- *802.1x EAP*
- *MAC ACL*

Refer to *Editing the WLAN Configuration on page 4-26* for additional information.

Kerberos

Kerberos allows for mutual authentication and end-to-end encryption. All traffic is encrypted and security keys are generated on a per-client basis. Keys are never shared or reused, and are automatically distributed in a secure manner. For information on configuring Kerberos for a WLAN, see *Configuring Kerberos on page 4-34*.

802.1x EAP

802.1x EAP is the most secure authentication mechanism for wireless networks and includes EAP-TLS, EAP-TTLS and PEAP. The switch is a proxy for Radius packets. An MU does a full 802.11 authentication and association and begins transferring data frames. The switch realizes the MU needs to authenticate with a Radius server and denies any traffic not Radius related. Once Radius completes its authentication process, the MU is allowed to send other data traffic. You can use either an onboard Radius server or internal Radius Server for authentication. For information on configuring 802.1x EAP for a WLAN, see *Configuring 802.1x EAP on page 4-33*.

MAC ACL

The MAC ACL feature is basically a dynamic MAC ACL where MUs are allowed/denied access to the network based on their configuration on the Radius server. The switch allows 802.11 authentication and association, then checks with the Radius server to see if the MAC address is allowed on the network. The Radius packet

uses the MAC address of the MU as both the username and password (this configuration is also expected on the Radius server). MAC-Auth supports all encryption types, and (in case of 802.11i) the handshake is completed before the Radius lookup begins. For information on configuring 802.1x EAP for a WLAN, see *Configuring MAC Authentication on page 4-48*.

1.2.5.3 Secure Beacon

Devices in a wireless network use *Service Set Identifiers* (SSIDs) to communicate. An SSID is a text string up to 32 bytes long. An AP in the network announces its status by using beacons. To avoid others from accessing the network, the most basic security measure adopted is to change the default SSID to one not easily recognizable, and disable the broadcast of the SSID.

The SSID is a code attached to all packets on a wireless network to identify each packet as part of that network. All wireless devices attempting to communicate with each other must share the same SSID. Apart from identifying each packet, the SSID also serves to uniquely identify a group of wireless network devices used in a given service set.

1.2.5.4 MU to MU Disallow

Use MU to MU Disalllow to restrict MU to MU communication within a WLAN. The default is 'no', which allows MUs to exchange packets with other MUs. It does not prevent MUs on other WLANs from sending packets to this WLAN. You would have to enable MU to MU Disallow on the other WLAN. To define how MU to MU traffic is permitted for a WLAN, see *Editing the WLAN Configuration on page 4-26*.

1.2.5.5 802.1x Authentication

802.1x Authentication cannot be disabled (its always enabled). A factory delivered out-of-the-box AP300 supports 802.1x authentication using a default username and password. EAP-MD5 is used for 802.1x.

When you initially switch packets on an out-of-the-box AP300 port, it immediately attempts to authenticate using 802.1x. Since 802.1x supports *supplicant initiated* authentication, the AP300 attempts to initiate the authentication process.

On reset (all resets including power-up), the AP300 sends an EAPOL start message every time it sends a Hello message (periodically every 1 second). The *EAPOL start* is the *supplicant initiated* attempt to become authenticated.

If an appropriate response is received in response to the *EAPOL start* message, the AP300 attempts to proceed with the authentication process to completion. Upon successful authentication, the AP300 transmits the Hello message and the download proceeds the way as it does today.

If no response is received from the *EAPOL start* message, or if the authentication attempt is not successful, the AP300 continues to transmit *Hello* messages followed by *LoadMe* messages. If a parent reply is received in response to the *Hello message,* then downloading continue normally - without authentication. In this case, you need not enable or disable the port authentication.

802.1x authentication is conducted:

- At power up
- On an AP300 operator initiated reset (such as pulling Ethernet cable)
- When the switch administrator initiates a reset of the AP300.
- When re-authentication is initiated by the Authenticator (say the switch in between)

Change Username/Password after AP Adoption

Once the AP300 is adopted using 802.1x authentication (say default username/password) OR using a non-secure access method (hub or switch without 802.1x enabled), use the CLI/SNMP/UI to reconfigure the username/password combination.

Reset Username/Password to Factory Defaults

To restore the AP300 username/password to factory defaults, adopt the AP300 using a non-secure access method (a hub or switch without 802.1x enabled), then reconfigure the username/password combination.

The Access Port does not make use of any parameters (such as MAC based authentication, VLAN based etc.) configured on Radius Server.

1.2.5.6 WIPS

The Motorola *Wireless Intrusion Protection Software* (WIPS) monitors for any presence of unauthorized rogue Access Points. Unauthorized attempts to access the WLAN is generally accompanied by anomalous behavior as intruding MUs try to find network vulnerabilities. Basic forms of this behavior can be monitored and reported without needing a dedicated WIPS. When the parameters exceed a configurable threshold, the switch generates an SNMP trap and reports the result via the management interfaces. Basic WIPS functionality does not require monitoring APs and does not perform off-channel scanning.

NOTE: When converting an AP300 to an Intrusion Detection Sensor, the conversion requires approximately 60 seconds.

NOTE: When using an AP-5131for use with WIPS and as a sensor you must first configure the WIPS server IP Addresses before converting the AP-5131 to a sensor.

1.2.5.7 Rogue AP Detection

The switch supports the following techniques for rogue AP detection:

- *RF scan by Access Port on all channels*
- *SNMP Trap on discovery*
- *Authorized AP Lists*
- *Rogue AP Report*
- *Motorola RFMS Support*

NOTE: The *Motorola RF Management Software* is recommended to plan the deployment of the switch. Motorola RFMS can help optimize the positioning and configuration of a switch in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Motorola Web site.

RF scan by Access Port on one channel

This process requires an Access Port to assist in Rogue AP detection. It functions as follows:

- The switch sends a new configuration message to the adopted AP informing it to detect Rogue APs.
- The Access Port listens for beacons on its present channel.
- It passes the beacons to the switch as it receives them without any modification.
- The switch processes these beacon messages to generate the list of APs

This process of detecting a Rogue AP is non-disruptive and none of the MUs are disassociated during this process. The Access Port will only scan on its present channel. An AP300 provides this support.

By choosing this option for detection, all capable Access Ports will be polled for getting the information.

RF scan by Access Port on all channels

The process used to scan for Rogue APs on all available channels functions as follows:

- The switch sends a configuration message (with the ACS bit set and channel dwell time) to the Access Port.
- An Access Port starts scanning each channel and passes the beacons it hears on each channel to the switch.
- An Access Port resets itself after scanning all channels.
- An switch then processes this information

SNMP Trap on discovery

An SNMP trap is sent for each detected and Rogue AP. Rogue APs are only detected, and notification is provided via a SNMP trap.

NOTE: Wired side scanning for Rogue APs using WNMP is not supported. Similarly, Radius lookup for approved AP is not provided.

Authorized AP Lists

Configure a list of authorized Access Ports based on their MAC addresses. The switch evaluates the APs against the configured authorized list after obtaining Rogue AP information from one of the 2 mechanisms as mentioned in *Rogue AP Detection on page 1-21*.

Rogue AP Report

After determining which are authorized APs and which are Rogue, the switch prepares a report.

Motorola RFMS Support

With this most recent switch firmware release, the switch can provide rogue device detection data to the Motorola RF Management software application (or Motorola RFMS). Motorola RFMS uses this data to refine the position and display the rogue on a site map representative of the physical dimensions of the actual radio coverage area of the switch. This is of great assistance in the quick identification and removal of unauthorized devices.

1.2.5.8 ACLs

ACLs control access to the network through a set of rules. Each rule specifies an action taken when a packet matches a set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is

allowed. If the action is to mark, the packet is tagged for priority. The switch supports the following types of ACLs:

- *IP Standard ACLs*
- *IP Extended ACLs*
- *MAC Extended ACLs*
- *Wireless LAN ACLs*

For information on creating an ACL, see *Configuring Firewalls and Access Control Lists on page 6-14*.

1.2.5.9 Local Radius Server

Radius is a common authentication protocol utilized by the 802.1x wireless security standard. Radius improves the WEP encryption key standard, in conjunction with other security methods such as EAP-PEAP. The switch has one onboard Radius server. For information on configuring the switch's resident Radius Server, see *Configuring the Radius Server on page 6-84*.

1.2.5.10 IPSec VPN

IP Sec is a security protocol providing authentication and encryption over the Internet. Unlike SSL (which provides services at layer 4 and secures two applications), IPsec works at Layer 3 and secures the network. Also unlike SSL (which is typically built into the Web browser), IPsec requires a client installation. IPsec can access both Web and non-Web applications, whereas SSL requires workarounds for non-Web access such as file sharing and backup.

A VPN is used to provide secure access between two subnets separated by an unsecured network. There are two types of VPNs:

- *Site-Site VPN* — For example, a company branching office traffic to another branch office traffic with an unsecured link between the two locations.
- *Remote VPN* — Provides remote user ability to access company resources from outside the company premises.

The switch supports:

- *IPSec termination for site to site*
- *IPSec termination for remote access*
- *IPSec traversal of firewall filtering*
- *IPSec traversal of NAT*
- *IPSec/L2TP (client to switch)*

1.2.5.11 NAT

Network Address Translation (NAT) is supported for packets routed by the switch. The following types of NAT are supported:

- *Port NAT*– Port NAT (also known as NAPT) entails multiple local addresses are mapped to single global address and a dynamic port number. The user is not required to configure any NAT IP address. Instead IP address of the public interface of the switch is used to NAT packets going out from private network and vice versa for packets entering private network.
- *Static NAT*– Static NAT is similar to Port NAT with the only difference being that it allows the user to configure a source NAT IP address and/or destination NAT IP address to which all the packets will be NATted to. The source NAT IP address is used when hosts on a private network are trying to access a host on a public network. A destination NAT IP address can be used for public hosts to talk to a host on a private network.

1.2.5.12 Certificate Management

Certificate Management is used to provide a standardized procedure to:

- Generate a Server certificate request and upload the server certificate signed by certificate authority (CA).
- Uploading of CA's root certificate
- Creating a self-signed certificate

Certificate management will be used by the applications HTTPS, VPN, HOTSPOT and Radius. For information on configuring switch certificate management, see *Creating Server Certificates on page 6-98*.

1.2.5.13 NAC

Using *Network Access Control* (NAC), the switch hardware and software grants access to specific network resources. NAC performs a user and MU authorization check for resources that do not have a NAC agent. NAC verifies a MU's compliance with the switch's security policy. The switch supports only the EAP/802.1x type of NAC. However, the switch also provides a mean to bypass NAC authentication for MU's that do not have NAC 802.1x support (printers, phones, PDAs etc.). For information on configuring NAC support, see *Configuring NAC Server Support on page 4-53*.

1.2.6 Supported Access Ports/Points

A RF switch supports the adoption of the following Motorola Enterprise Access Ports and Access Points:

- *AP100*
- *AP300*
- *AP-5131*
- *AP-7131*

2

Switch Web UI Access and Image Upgrades

The content of this chapter is segregated amongst the following:

- *Accessing the Switch Web UI*
- *Switch Password Recovery*
- *Upgrading the Switch Image*
- *Auto Installation*
- *AP-4131 Access Point to Access Port Conversion*

2.1 Accessing the Switch Web UI

2.1.1 Web UI Requirements

The switch Web UI is accessed using Internet Explorer version 5.5 (or later) and SUN JRE (Java Runtime Environment) 1.5 (or later). Refer to the Sun Microsystems Web site for information on downloading JRE.

NOTE: To successfully access the switch Web UI through a firewall, UDP port 161 must be open in order for the switch's SNMP backend to function.

To prepare Internet Explorer to run the Web UI:

1. Open IE's **Tools > Internet Options** panel and select the **Advanced** tab.
2. Uncheck the following checkboxes:
   - Use HTTP 1.1
   - Java console enabled (requires restart)
   - Java logging enabled
   - JIT compiler for virtual enabled (requires restart).

2.1.2 Connecting to the Switch Web UI

To display the Web UI, launch a Web browser on a computer with the capability of accessing the switch.

NOTE: Ensure you have HTTP connectivity to the switch, as HTTP is a required to launch the switch Web UI from a browser.

To display the switch Web UI:

1. Point the browser to the IP address assigned to the wired Ethernet port (port 2). Specify a secure connection using the https:// protocol.

   The switch login screen displays:

2. Enter the Username **admin**, and Password **superuser.** Both are case-sensitive. Click the **Login** button.

NOTE: If using HTTP to login into the switch, you may encounter a Warning screen if a self-signed certificate has not been created and implemented for the switch. This warning screen will continue to display on future login attempts until a self-signed certificate is implemented. Motorola recommends only using the default certificate for the first few login attempts until a self-signed certificate can be generated.

NOTE: If your password is lost, there is a means to access the switch, but you are forced to revert the switch back to its factory default settings and lose your existing configuration (unless saved to a secure location). Consequently, Motorola recommends keeping the password in a secure location so it can be retrieved. For information on password recovery, see *Switch Password Recovery on page 2-2*.

Once the Web UI is accessed, the Switch main menu item displays a configuration tab with high-level switch information. Click the **Show Dashboard** button to display an overall indicator of switch health. Once the switch is fully configured, the dashboard is the central display for the user to view the version of firmware running on the switch, quickly assess the last 5 alarms generated by the switch, view the status of the switch's Ethernet connections and view switch CPU and memory utilization statistics.

NOTE: The chapters within this *System Reference Guide* are arranged to be complimentary with the main menu items in the menu tree of the switch Web UI. Refer to this content to configure switch network addressing, security and diagnostics as required.

2.2 Switch Password Recovery

The switch has a means of restoring its password to its default value. Doing so also reverts the switch's security, radio and power management configuration to their default settings. Only an installation professional should reset the switch password and promptly define a new restrictive password.

To contact Motorola Support in the event of a password reset requirement, go to *http://www.symbol.com/contactsupport*.

CAUTION: Only a qualified installation professional should set or restore the switch's radio and power management configuration in the event of a password reset.

2.3 Upgrading the Switch Image

The switch ships with a factory installed firmware image with the full feature functionality described in this *System Reference Guide*. However, Motorola periodically releases switch firmware that includes enhancements or resolutions to known issues. Verify your current switch firmware version with the latest version available from the Motorola Web site before determining if your system requires an upgrade.

2.4 Auto Installation

The switch auto install function can be configured manually or using a DHCP server. When configuring auto installation using DHCP, the server requires the definition of a vendor class and four sub-options under option 43 namely:

- *Option 186* - defines the tftp/ftp server and ftp username, password information
- *Option 187* - defines the firmware path and file name
- *Option 188* - defines the config path and file name
- *Option 190* - defines the cluster config path and file name.

The individual features (config, cluster-config and image) can be enabled separately using the CLI, SNMP or Web UI. If a feature is disabled, it is skipped when auto install is triggered.

For manual configuration (where the URLs for the configuration and image files are not supplied by DHCP), the URLs can be specified using the CLI, SNMP or Applet. Use the CLI to define the expected firmware image version. If the image version is not specified, the switch will derive it from the header of the firmware image file.

Configuration files are tracked by their MD5 checksum. Configuration files are tracked by their contents. If a file is renamed its contents remain the same and the file will not be reloaded.

The requested image file version (if any) is checked against the current version before any attempt is made to load it. If the requested version is the same as the running version, no action is taken. If the image file version (embedded in the file header) does not match the expected version, no further action is taken. If the version has not been specified, the image file header is compared to the local version. If they are the same, no action is taken.

NOTE: Once the system has been operating for ten minutes, Auto Install is disabled, though it may still be reconfigured. This is to prevent the system from attempting to re-install each time a DHCP lease is renewed.

Configuring Auto Install via the CLI

There are three compulsory and four optional configuration parameters.

The compulsory parameters are:

- configuration upgrade enable
- cluster configuration upgrade enable
- image upgrade enable

Optional (only for the static case):

- configuration file URL
- cluster configuration file URL

- image file URL
- expected image version

To set default to no, and the URLs and the version default to "" (blank):

```
RF Switch(config)#show autoinstall
feature    enabled      URL
config       no         --not-set--
cluster cfg  no         --not-set--
image        no         --not-set--
expected image version  --not-set--
```

Enables are set using the **autoinstall <feature>** command:

```
RF Switch>en
RF Switch#conf t
RF Switch(config)#autoinstall image
RF Switch(config)#autoinstall config
RF Switch(config)#autoinstall cluster-config
```

After this configuration update, any switch reboot with DHCP enabled on the RON port will trigger an auto install, provided the DHCP Server is configured with appropriate options.

The "enables" are cleared using the **no autoinstall <feature>**

URLs and the version string are stored in the configuration file as text and can be cleared using an empty pair of double quotes to denote the blank string. In the following example, define the three URLs and the expected version of the image file, then enable all three features for the auto install.

```
RF Switch(config)#autoinstall config url ftp://ftp:ftp@192.9.200.1/RFSwitch/
config
RF Switch(config)#autoinstall cluster-config url ftp://ftp:ftp@192.9.200.1/
RFSwitch/cluster-config
RF Switch(config)#autoinstall image url ftp://ftp:ftp@147.11.1.11/RFSwitch/
images/RFS6000.img
RF Switch(config)#autoinstall image version 3.1.0.0-XXXXX
RF Switch(config)#autoinstall config
RF Switch(config)#autoinstall cluster-config
RF Switch(config)#autoinstall image
RF Switch(config)#show autoinstall
feature    enabled      URL
config       yes        ftp://ftp:ftp@192.9.200.1/RFSwitch/config
cluster cfg  yes        ftp://ftp:ftp@192.9.200.1/RFSwitch/cluster-config
image        yes       ftp://ftp:ftp@147.11.1.11/RFSwitch/images/RFS6000.img
expected image version  3.1.0.0-XXXXX
```

Once again, for DHCP option based auto install the URLs is ignored and those passed by DHCP are not stored.

Whenever a string is blank it is shown as **--not-set--**.

2.5 AP-4131 Access Point to Access Port Conversion

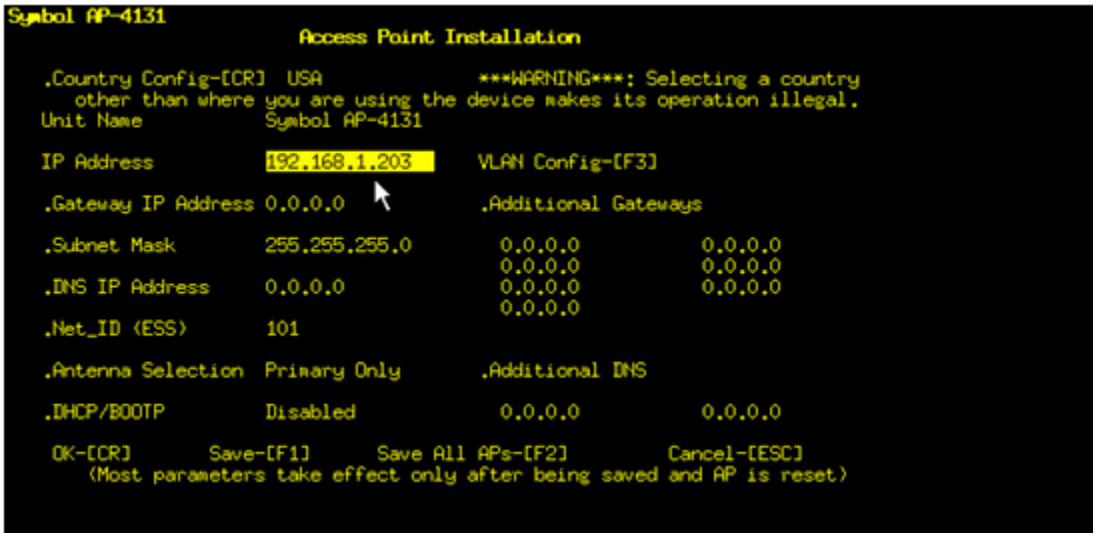
SWITCH NOTE: AP-4131 Access Point to Access Port Conversion is only available on the RFS6000 platform.

To convert an AP-4131 *fat* Access Point to a *thin* AP-4131 Access Port you need to load the port conversion version firmware. Refer to the files available with you Motorola Web site download package.

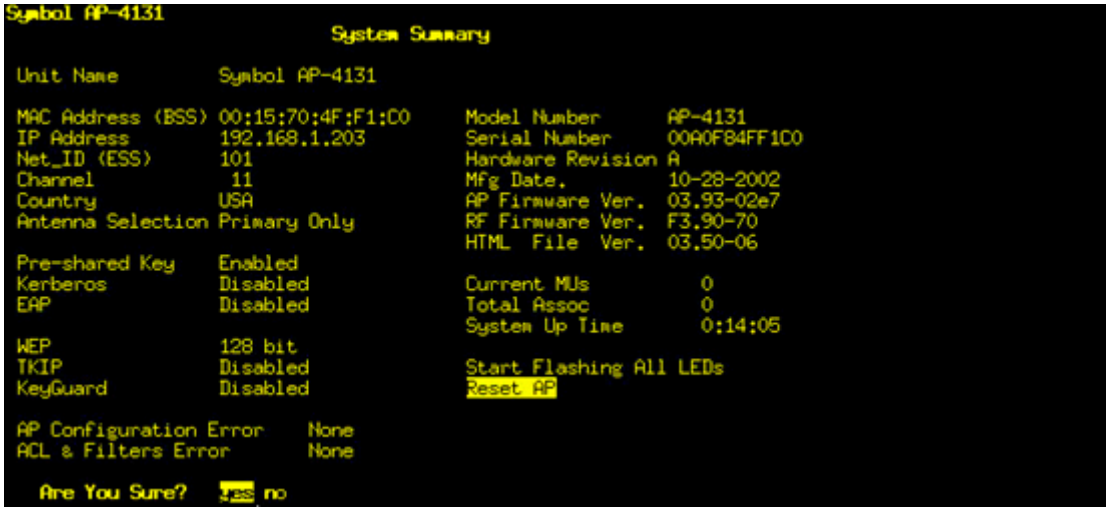
To convert an AP-4131 Access Point

1. Verify a TFTP server is up and running and the firmware you are going to install is in the root directory of the TFTP server.
2. Log in to the AP-4131 as **Admin**. The default password is **Symbol**.

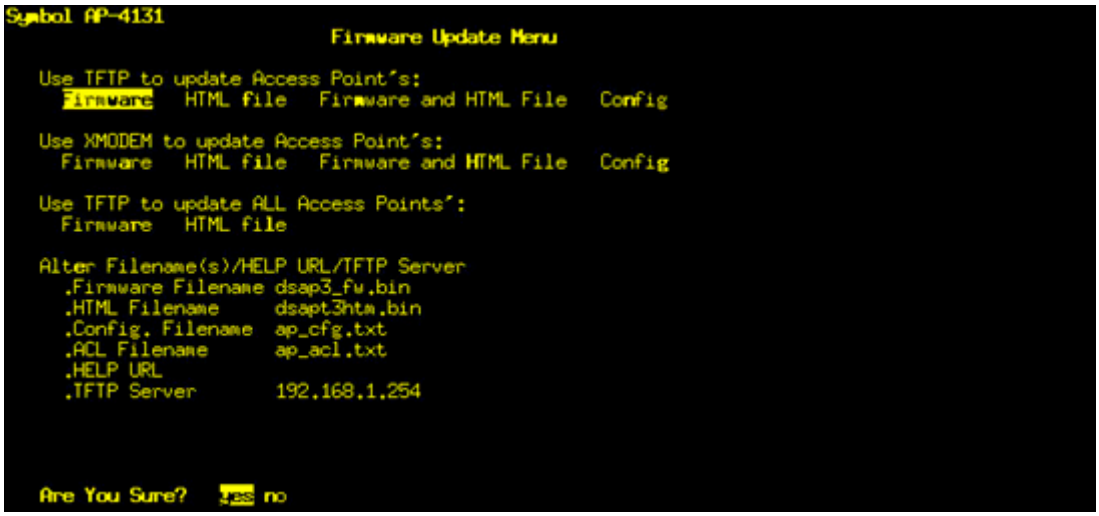
3. Select the **AP Installation** main menu item.
4. From the **IP Address** field, enter a new IP address (if required) and select **Save-[F1]** to save the change. If the IP address was changed, you will need to reset the AP for the change to be implemented.



5. Reset the AP if you changed the AP's IP address, buy displaying the **System Summary** and selecting the **Reset AP** option. If you reset the AP-4131 you will need to login as Admin again.



6. Select the **Special Functions** main menu item.
7. Select the **Firmware Update Menu-[F3]** menu item
8. Select the **Alter Filename(s)/HELP URL/TFTP Server** menu item.
    a. Confirm that the Firmware File Name is correct, make changes as needed.
    b. Enter the IP address of your TFTP server, select enter.
    c. Select F1 to save your changes.
9. Select **Firmware** under the **Use TFTP to update Access Point's** option.



10. Select **yes** when asked to confirm.
11. The AP-4131 will now reset, download and install the desired firmware.
12. Once the firmware download is complete, connect the AP-4131 to the PoE switch and the RF Switch The AP-4131 should adopt and operate as a "thin" Access Port.

3

Switch Information

This chapter describes the Switch main menu information used to configure the switch. This chapter consists of the following sections:

- *Viewing the Switch Interface*
- *Viewing Switch Port Information*
- *Viewing Switch Configurations*
- *Viewing Switch Firmware Information*
- *Switch File Management*
- *Configuring Automatic Updates*
- *Viewing the Switch Alarm Log*
- *Viewing Switch Licenses*
- *How to use the Filter Option*

3.1 Viewing the Switch Interface

The Switch **Configuration** tab provides high-level system, switch name and address information accessible from one location. Use this information to assess whether the current firmware version is the most recent and if the number of licenses available is correct to support the number of radio devices deployed. The values displayed within the screen can be defined in numerous additional locations throughout the switch applet.

NOTE: The *Motorola RF Management Software* is a recommended utility to plan the deployment of the switch and view its interface statistics once operational in the field. Motorola RFMS can help optimize the positioning and configuration of a switch (and its associated radios) in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Motorola Web site.

The switch screen displays two tabs supporting the following configuration activities:

- *Setting the Switch Country Code*
- *Setting the Switch Country Code*
- *Viewing Switch Statistics*

NOTE: When the switch's configuration is successfully updated (using the Web UI), the effected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the effected screen's Status field and the screen remains displayed. With file transfer operations, the transfer screen remains open during the transfer and remains open upon completion (with status displayed within the Status field).

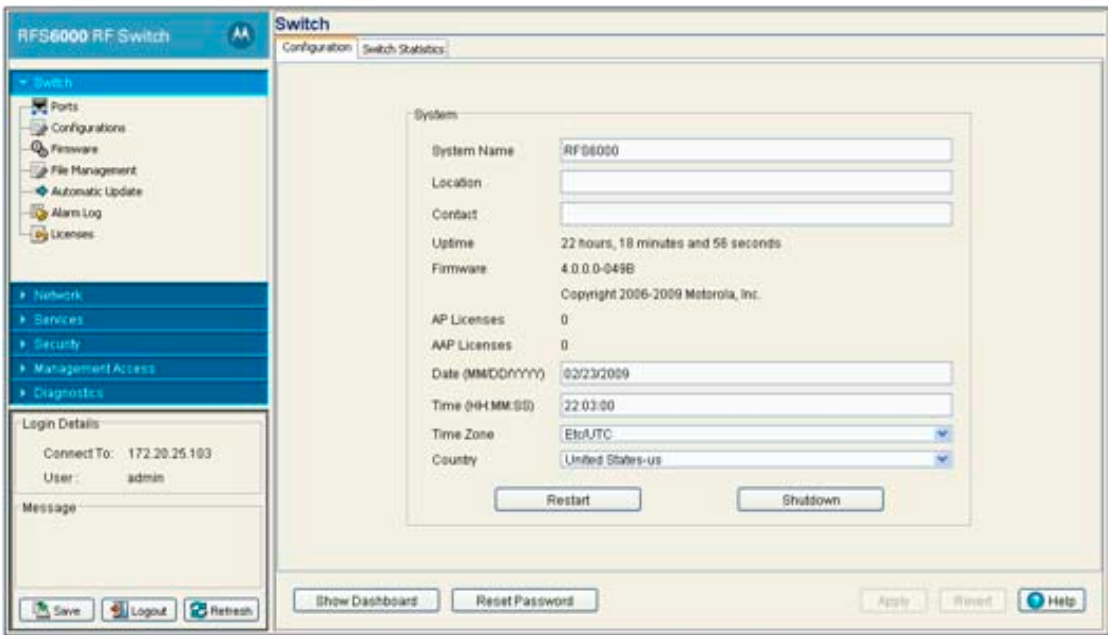
3.1.1 Setting the Switch Country Code

When initially logging into the system, the switch requests that you enter the correct country code for your region. If a country code is not configured, a warning message will display stating that an incorrect country setting will lead to the illegal use of the switch. Consequently, selecting the correct country is extremely important. Each country has its own regulatory restrictions concerning electromagnetic emissions (channel range) and the maximum RF signal strength transmitted. To ensure compliance with national and local laws, be sure to set the **Country** value correctly.

3.1.2 Viewing the Switch Configuration

To view a high-level display of the switch configuration:

1. Select **Switch** from the main menu tree.
2. Click the **Configuration** tab.



3. Refer the **System** field to view or define the following information:

System Name	Displays the designated system name. Provide a system name serving as a reminder of the user base the switch supports (engineering, retail, etc.).
Location	The Location parameter serves as a reminder of where the switch can be found. Define the System Name as a specific identifier of the switch's location. Use the System Name and Location parameters together to optionally define the switch name by the radio coverage type it supports and physical location. For example, "second floor engineering."
Contact	Displays a **Contact** value for system administration and troubleshooting. This name should be the network administrator responsible for switch operations.
Uptime	Displays the current operational time for the device name defined within the System Name field. Uptime is the cumulative time since the switch was last rebooted or lost power.
Firmware	Displays the current firmware version running on the switch. This version should be periodically compared to the most recent version available on the Motorola Web site, as versions with increased functionality are periodically released.
AP Licenses	Displays the number of Access Port licenses currently available for the switch. This value represents the maximum number of Access Ports the switch is licensed to adopt.
AAP Licenses	Displays the number of Adaptive AP licenses currently available for the switch. This value represents the maximum number of AAPs the switch is licensed to adopt.
Date (MM/DD/YYYY)	Displays the day, month and year currently used with the switch.
Time (HH:MM:SS)	Displays the time of day used by the switch.
Time Zone	Use the drop-down menu to specify the time zone used with the switch. Adjusting the time zone will in turn, cause an adjustment to the time displayed.
Country	Use the drop-down menu to specify the correct country of operation. Selecting the country incorrectly could render your switch as operating illegally.

4. Click the **Restart** button to reboot the switch. The switch itself does not include a hardware reset feature.

CAUTION: When rebooting the switch, the Radius Server will also be restarted regardless of its state before the reboot.

5. Click the **Shutdown** button to shutdown and power off the switch.

NOTE: On the RFS6000 and RFS7000 the shutdown command will shutdown the switch but the fans on the switch will remain on.

6. Click the **Show Dashboard** button to display a screen with important indicators of switch health and status. For more information, see *Switch Dashboard Details*. Referencing the Details screen is recommended before new configurations are employed that utilize increased switch bandwidth.
7. Click the **Reset Password** button to display a screen to reset the password.

Enter the new password within the **Password** and **Confirm Password** fields and click **OK**.

NOTE: When entering a new password for the switch, please note that the password must be a minimum of 8 characters long.

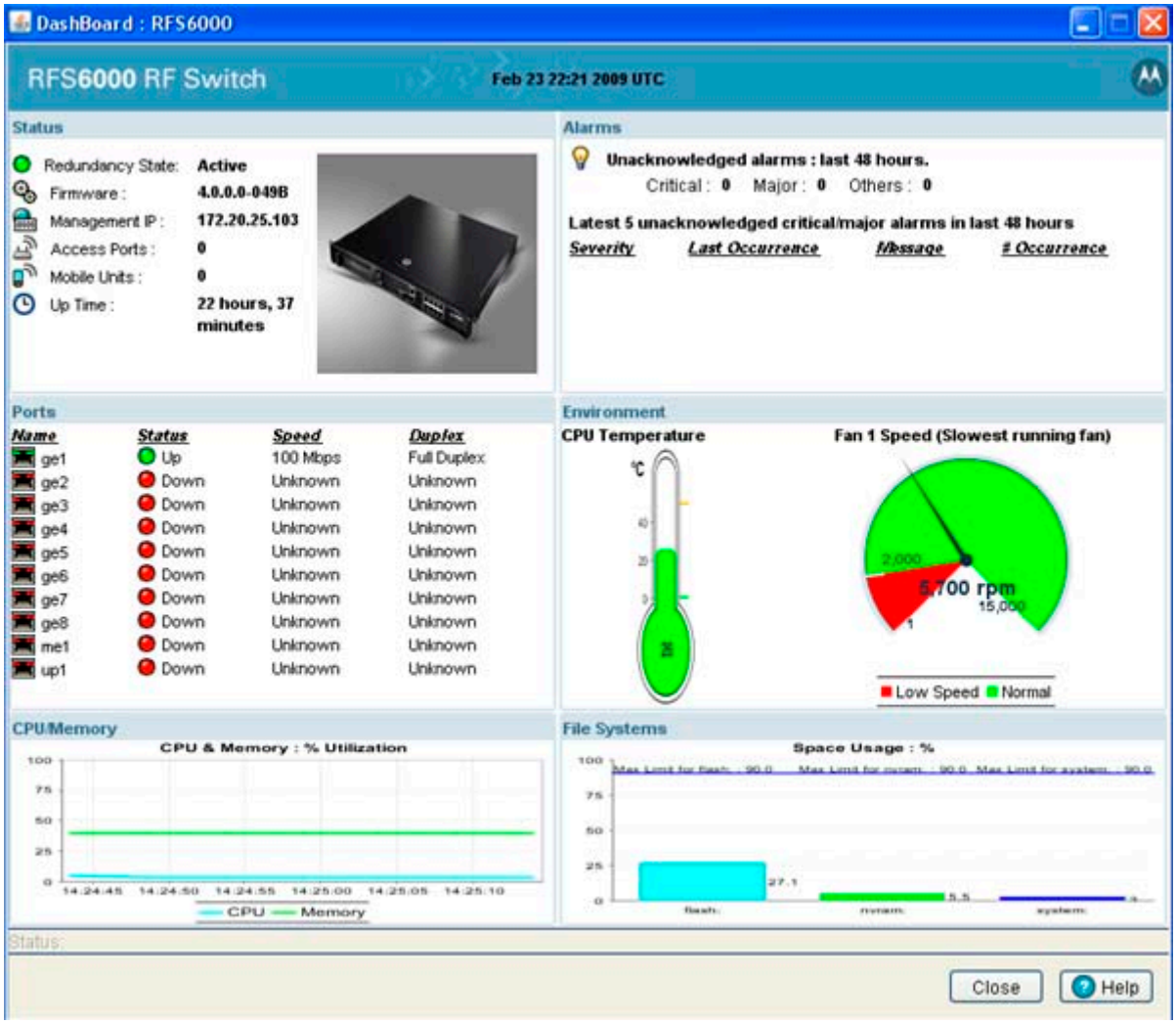
8. Click the **Revert** button to undo any changes. The **Revert** button must be clicked before hitting the **Apply** button for any changes to be reverted.
9. Click the **Apply** button to save the updates (to the Time Zone or Country parameters specifically).

3.1.3 Switch Dashboard Details

Each Motorola RF Switch platform contains a dashboard which represents a high-level graphical overview of central switch processes and hardware. When logging into the switch, the dashboard should be the first place you go to assess overall switch performance and any potential performance issues.

Click the **Show Dashboard** button (within the Switch screen's Configuration tab) to display the current health of the switch

3.1.3.1 RFS6000 Switch Dashboard



The **Dashboard** screen displays the current health of the switch and is divided into fields representing the following important diagnostics:

- *Alarms*
- *Ports*
- *Environment*
- *CPU/Memory*
- *File Systems*

Apart from the sections mentioned above, it also displays the following status:

Redundancy State	Displays the Redundancy State of the switch. The status can be either Enabled or Disabled. • *Enabled* - Defined a green state. • *Disabled* - Defined by a yellow state.
Firmware	Displays the Firmware version of the current software running on the wireless switch.
Management IP	Displays the Management IP address of the switch.
Access Ports	Displays the total number of Access Ports adopted by the switch.
Mobile Units	Displays the total number of MUs associated with the switch.
Up Time	Displays the actual switch uptime. The **Uptime** is the current operational time of the device defined within the System Name field. Uptime is the cumulative time since the switch was last rebooted or lost power.

1. Refer to the **Alarms** field for details of all the unacknowledged alarms generated during the past 48 hours. The alarms are classified as:
   - *Critical* — Denoted by a red indicator. These alarms warrant immediate attention.
   - *Major* — Denoted by a yellow indicator. These alarms warrant attention.
   - *Others* — Denoted by a blue indicator.

   The alarms field also displays details (in a tabular format) of the 5 most recent unacknowledged critical/major alarms raised during the past 48 hours. The table displays the following details:

Severity	Displays the severity of the alarm. It can be either Critical or Major.
Last Occurrence	Displays the time when the alarm was reported.
Message	Displays the message associated with the alarm.
# Occurrences	Displays the number of times during the past 48 hours such an alarm was generated.

2. Refer to the **Ports** field for link, speed and duplex status of each physical port on the switch's front panel. It displays the following details in a tabular format:

Name	Displays the name of the port (ge1-8, me1 or up1)
Status	Displays the status of the port, either— Up or Down

Speed	Displays the speed at which the port transmits or receives data.
Duplex	Displays the status of the port, either— Full Duplex or Unknown.

3. The **Environment** section displays the CPU temperature. It displays the valid threshold range set by the user.
4. The **CPU/Memory** section displays the free memory available with the RAM.
5. The **File Systems** section displays the free file system available for:
   - *flash*
   - *nvram*
   - system

3.1.3.2 RFS7000 Switch Dashboard

The **Dashboard** screen displays the current health of the switch and is divided into fields representing the following important diagnostics:

- *Alarms*
- *Ports*
- *Environment*
- *CPU/Memory*
- *File Systems*

Apart from the sections mentioned above, it also displays the following status:

Redundancy State	Displays the Redundancy State of the switch. The status can be either Enabled or Disabled.
	• *Enabled* - Defined a green state. • *Disabled* - Defined by a yellow state.
Firmware	Displays the Firmware version of the current software running on the wireless switch.
Management IP	Displays the Management IP address of the switch.
Access Ports	Displays the total number of Access Ports adopted by the switch.
Mobile Units	Displays the total number of MUs associated with the switch.
Up Time	Displays the actual switch uptime. The **Uptime** is the current operational time of the device defined within the System Name field. Uptime is the cumulative time since the switch was last rebooted or lost power.

1. Refer to the **Alarms** field for details of all the unacknowledged alarms generated during the past 48 hours. The alarms are classified as:
   - *Critical* — Denoted by a red indicator. These alarms warrant immediate attention.
   - *Major* — Denoted by a yellow indicator. These alarms warrant attention.
   - *Others* — Denoted by a blue indicator.

   The alarms field also displays details (in a tabular format) of the 5 most recent unacknowledged critical/major alarms raised during the past 48 hours. The table displays the following details:

Severity	Displays the severity of the alarm. It can be either Critical or Major.
Last Occurrence	Displays the time when the alarm was reported.
Message	Displays the message associated with the alarm.
# Occurrences	Displays the number of times during the past 48 hours such an alarm was generated.

2. Refer to the **Ports** field for link, speed and duplex status of each physical port on the switch's front panel. It displays the following details in a tabular format:

Name	Displays the name of the port (ge1, ge2, ge3, ge4 and me1).
Status	Displays the status of the port, either— Up or Down
Speed	Displays the speed at which the port transmits or receives data.
Duplex	Displays the status of the port, either— Full Duplex or Unknown.

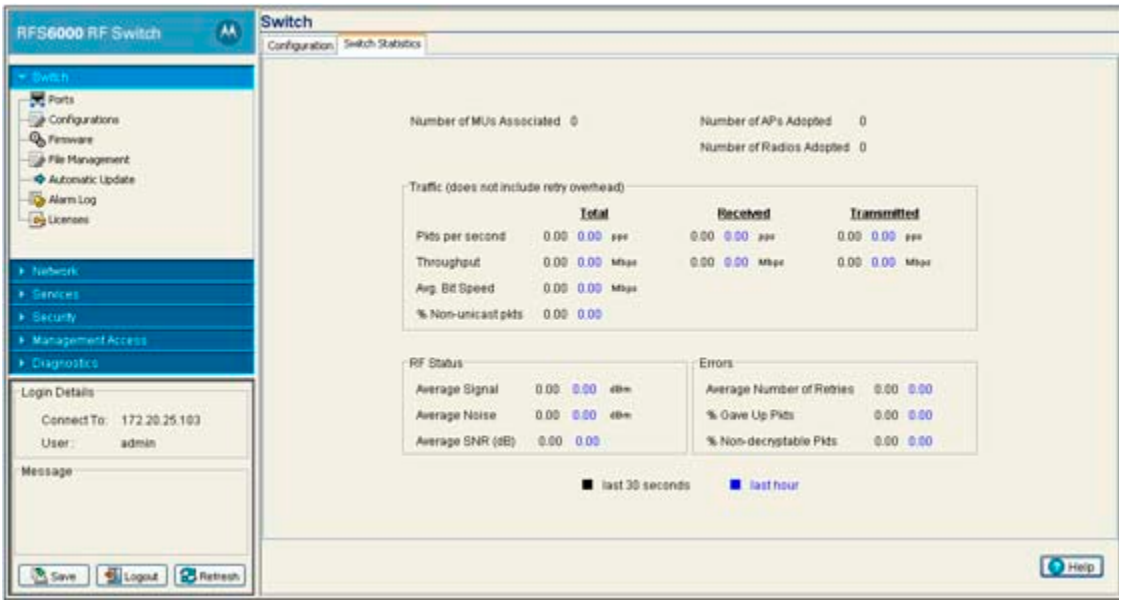
3. The **Environment** section displays the CPU temperature. It displays the valid threshold range set by the user.
4. The **CPU/Memory** section displays the free memory available with the RAM.
5. The **File Systems** section displays the free file system available for:
   - *flash*
   - *nvram*
   - system

3.1.4 Viewing Switch Statistics

The **Switch Statistics** tab displays an overview of the recent network traffic and RF status for the switch.

To display the Switch Statistics tab:

1. Select **Switch** from the main menu tree.
2. Click the **Switch Statistics** tab at the top of the Switch screen.



3. Refer to the following read-only information about associated MUs:

Number of MUs Associated	Displays the total number of MUs currently associated to the switch.
Number of APs Adopted	Displays the total number of Access Ports currently adopted by the switch.
Number of Radios Adopted	Displays the total number of radios currently adopted by the switch.

4. Refer to the **Traffic** field to assess network traffic for associated APs and radios:

Pkts per second	Displays the packet transmission rate for received and transmitted packets over last 30 seconds and 1 hour.
Throughput	Displays the traffic throughput for packets received, packets transmitted and total packets over last 30 seconds and 1 hour.

Avg. Bit Speed	Displays the average bit speed for the switch over last 30 seconds and 1 hour. Use the average bit speed value to help determine overall network speeds and troubleshoot network congestion.
% Non-unicast pkts	Displays the percentage of non-unicast packets seen (received & transmitted) by the switch over last 30 seconds and 1 hour. Non-unicast traffic includes both multicast and broadcast traffic. Broadcasted, multicasted, and flooded packets are sent over the air at the slowest rate on every radio in the WLAN and therefore have a much larger airtime utilization than unicast packets a greater chance of causing collisions.

5. The **RF Status** section displays the following read-only RF radio signal information for associated APs and radios:

Average Signal	Displays the average signal strength for MUs associated with the switch over the last 30 seconds and 1 hour. Typically, the higher the signal, the closer the MU.
Average Noise	Displays the average RF noise for all MUs associated with the selected WLAN. MU noise for the last 30 seconds is displayed in black and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the Access Port, or in area with less conflicting network traffic. Excessive noise may also be an indication of network interference.
Average SNR (dB)	Displays the average *Signal to Noise Ratio* (SNR) for all MUs associated with the switch. The SNR is an indication of overall RF performance on the wireless network.

6. Refer to the **Errors** field for read-only packet error and loss information for associated Access Ports and radios:

Average Number of Retries	Displays the average number of retries for all MUs associated with the switch. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour. If the Average Number of Retries starts increasing this indicates that MUs are not getting a good link back to the AP.
% Gave Up Pkts	Displays the percentage of packets which the switch gave up on for all MUs associated with the switch. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour. If this field displays a non-zero number it indicates bad links causing packets to the MUs
% Non-decryptable Pkts	Displays the percentage of undecryptable packets for all MUs associated with the switch. The number in black represents undecryptable pkts for the last 30 seconds and the number in blue represents undecryptable pkts for the last hour. If this field displays a non-zero number it can indicate outside intrusion into the network or an MU using incorrect cryptography such as a a misconfigured static key.

3.2 Viewing Switch Port Information

The **Port** screen displays configuration, runtime status and statistics of the ports on the switch.

SWITCH NOTE: The ports available vary by switch platform.
RFS6000: ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1
RFS7000: ge1, ge2, ge3, ge4, me1

The port types are defined as follows:

GE#	GE ports are available on the RFS6000 and RFS7000 platforms. GE ports on the RFS6000 are RJ-45 which support 10/100/1000Mbps. GE ports on the RFS7000 can be RJ-45 or fiber ports which support 10/100/1000Mbps.
ME#	ME ports are available on the RFS6000 and RFS7000 platforms. ME ports are out-of-band management ports which can be used to manage the switch via CLI or Web UI even when the other ports on the switch are unreachable.
UP#	An UP port is available on the RFS6000 platform only. This port is used to connect the RFS6000 to the backbone network. The UP port on the RFS6000 supports either RJ-45 or fiber. The UP port is the preferred way to connect to the backbone as it has a non-blocking 1gbps connection unlike the ge1-8 ports.

The Port screen contains three tabs supporting the following port assessment activities:

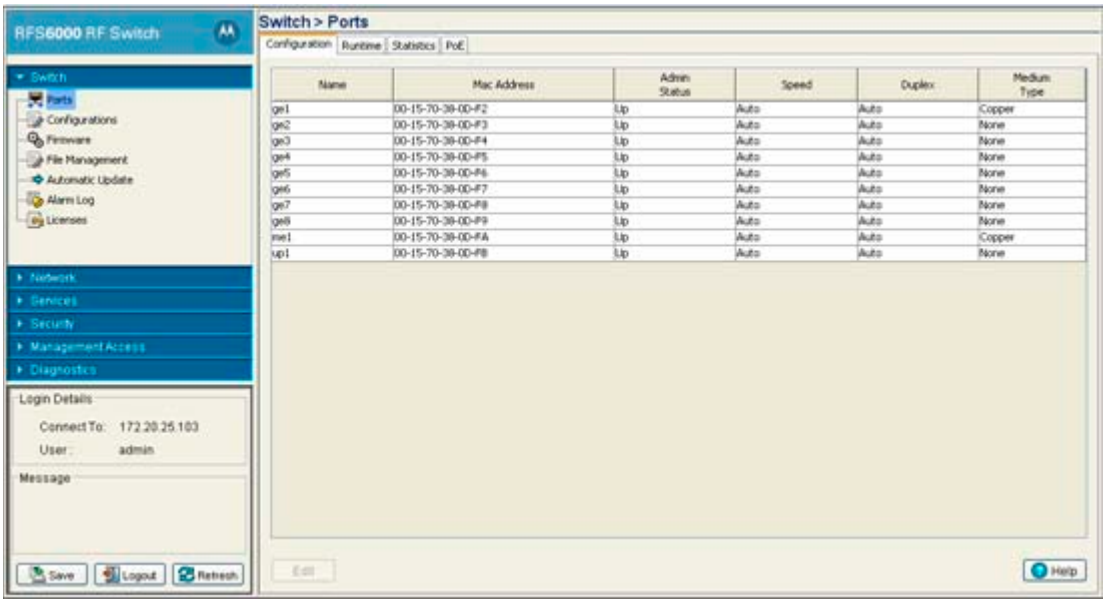
- *Viewing the Port Configuration*
- *Viewing the Ports Runtime Status*
- *Reviewing Port Statistics*

3.2.1 Viewing the Port Configuration

The **Configuration** tab displays the current configuration for the switch ports. Use the port configuration information to determine whether an existing port configuration can be used as is or requires modification for use within the switch managed network.

To view configuration details for the uplink and downlink ports:

1. Select **Switch** > **Port** from the main menu tree.
2. Select the **Configuration** tab to display the following read-only information:



Name	Displays the current port name. The port names available vary by switch. *RFS6000: ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1* *RFS7000: ge1, ge2, ge3, ge4, me1*
MAC Address	Displays the port's MAC Address. This value is read-only, set at the factory and cannot be modified.
Admin Status	Displays whether the port is currently Up or Down.
Speed	Displays the current speed of the data transmitted and received over the port.
Duplex	Displays the port as either half or full duplex.
Medium	Displays whether the connection medium is cooper or not.

SWITCH NOTE: On a RFS7000, the MAC address for the me1 port changes when the switch firmware is updated to the 1.3 version. This addresses an issue where the switch MAC address and ge1 interface shared the same MAC address in previous versions.

3. Select a port and click the **Edit** button to modify the port configuration. For additional information, see *Editing the Port Configuration*.

3.2.1.1 Editing the Port Configuration

To modify the port configuration:

1. Select a port from the table displayed within the Configuration screen.

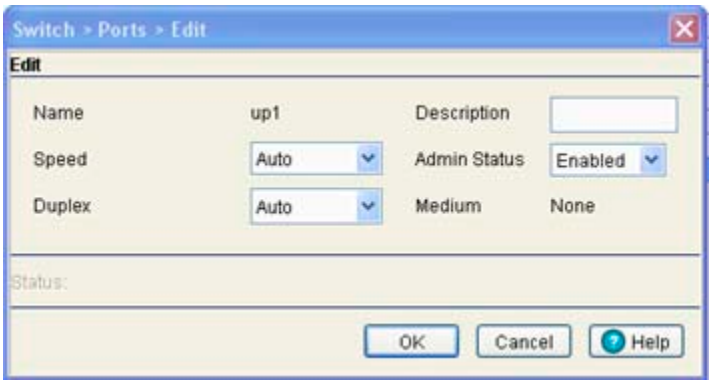
2. Click the **Edit** button.

   A **Port Change Warning** screen displays, stating any change to the port setting could disrupt access to the switch. Communication errors may occur even if modifications made are successful.

3. Click the **OK** button to continue.

   Optionally, select the **Don't show this message again for the rest of the session** checkbox to disable the pop-up.

4. Use the **Edit** screen to modify the following port configurations for the selected port.



Name	Displays the read-only name assigned to the port.
Speed	Select the speed at which the port can receive and transmit the data. Select from the following range: • *10 Mbps* • *100 Mbps* • *1000 Mbps* • *Auto*
Duplex	Modify the duplex status by selecting one of the following options: • *Half* • *Full* • *Auto*
Channel Group	Optionally, set the **Channel Group** defined for the port. The switch bundles individual Ethernet links (over the selected channel) into a single logical link that provides bandwidth between the switch and another switch or host. The port speed used is dependant on the Duplex value selected (full, half or auto). If a segment within a channel fails, traffic previously carried over the failed link is routed to the remaining segments within the channel. A trap is sent upon a failure identifying the switch, channel and failed link.
Description	Enter a brief description for the port. The description should reflect the port's intended function to differentiate it from others with similar configurations.
Admin Status	Either Enable (activate) or Disable (shutdown) the admin status of the port.
Medium	Displays the current (read-only) connection medium used by this port.

Read-only details about the port's cabling connection also display within the **Edit** screen. This information should be used to determine the configuration defined for this port.

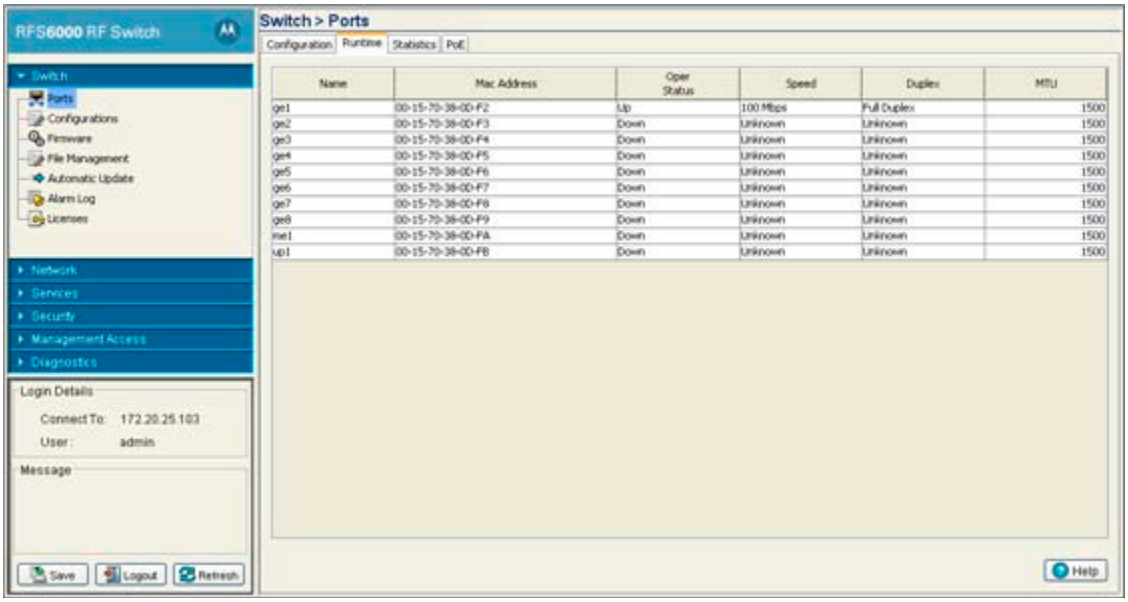
5. Click the **OK** button to commit the changes made to the port configurations.
6. Click **Cancel** to disregard any changes and revert back to the last saved configuration.

3.2.2 Viewing the Ports Runtime Status

The **Runtime** tab displays read-only runtime configuration for uplink and downlink ports.

To view the runtime configuration details of the uplink and downlink ports:

1. Select **Switch** > **Port** from the main menu tree.



2. Select the **Runtime** tab to display the following read-only information:

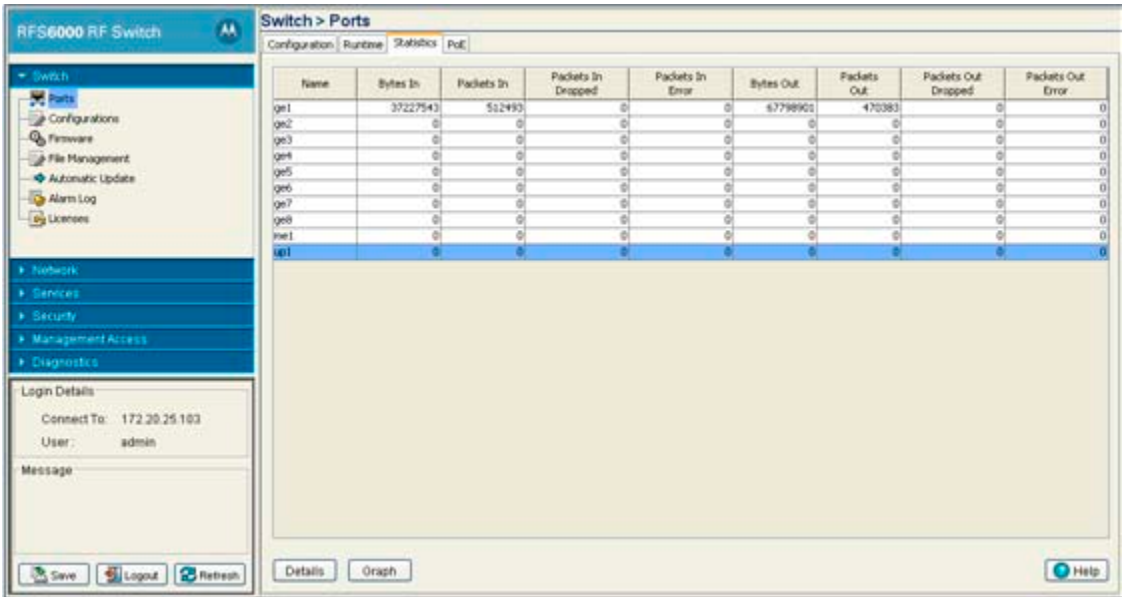
Name	Displays the port's current name.
MAC Address	Displays the port's MAC Address. This value is read-only, set at the factory and cannot be modified.
Oper Status	Displays the link status of the port. The port status can be either Up or Down.
Speed	Displays the current speed of the data transmitted and received over the port.
Duplex	Displays the port as either *half duplex*, *full duplex* or *Unknown.*
MTU	Displays the *maximum transmission unit* (MTU) setting configured on the port. The MTU value represents the largest packet size that can be sent over a link. 10/100 Ethernet ports have a maximum MTU setting of 1500.

3.2.3 Reviewing Port Statistics

The **Statistics** tab displays read-only statistics for ethernet ports. Use this information to assess if configuration changes are required to improve network performance.

To view the runtime configuration details of the switch ports:

1. Select **Switch** > **Port** from the main menu tree.
2. Select the **Statistics** tab.



3. Refer to the Statistics tab to display the following read-only information:

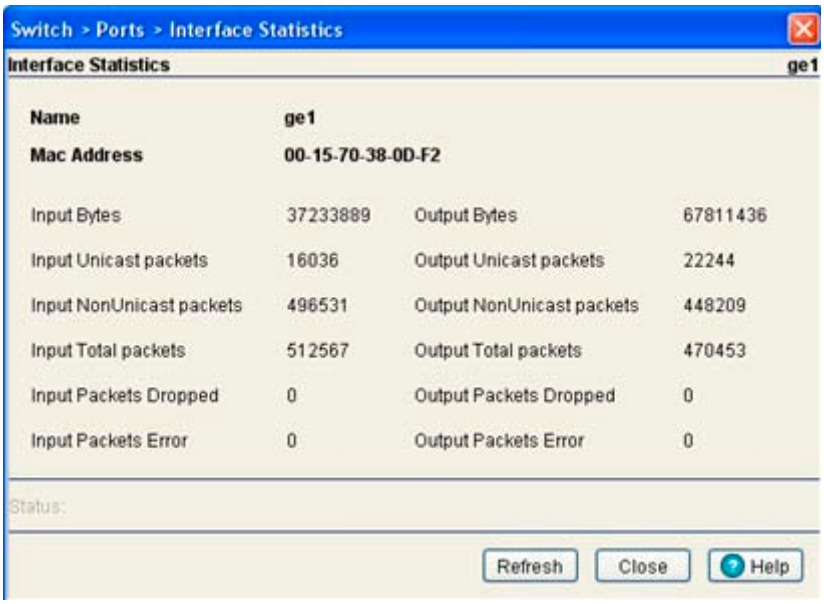
Name	Defines the port name.
Bytes In	Displays the total number of bytes received by the port.
Packets In	Displays the total number of packets received by the port.
Packets In Dropped	Displays the number of packets dropped by the port. If the number appears excessive, a different port could be required.
Packets In Error	Displays the number of erroneous packets received by the port. If the number appears excessive, try using a different port and see if the problem persists.
Bytes Out	Displays the total number of bytes transmitted by the port.
Packets Out	Displays the total number of packets transmitted by the port. A low value could be an indication of a network problem.
Packets Out Dropped	Displays the total number of packets dropped during transmission. A high value may be an indication of network throughput issues.
Packets Out Error	Displays the total number of erroneous transmitted packets.

4. Select a port and click on **Details** button to see the detailed port statistics. For more information, refer to *Detailed Port Statistics*.
5. Select a port and click on **Graph** button to view the port statistics in a graphical format. For more information, refer to *Viewing the Port Statistics Graph*.

3.2.3.1 Detailed Port Statistics

To view detailed statistics for a port:

1. Select a port from the table displayed within the Statistics screen.
2. Click the **Details** button.



3. The **Interface Statistics** screen displays. This screen displays the following statistics for the selected port:

Name	Displays the port name.
MAC Address	Displays physical address information associated with the interface. This address is read-only (hard-coded at the factory) and cannot be modified.
Input Bytes	Displays the number of bytes received on the interface.
Input Unicast Packets	Displays the number of unicast packets (packets directed towards the interface) received on the interface.
Input NonUnicast Packets	Displays the number of NonUnicast Packets (Multicast and Broadcast Packets) received on the interface.
Input Total Packets	Displays the total number of packets received on the interface.
Input Packets Dropped	Displays the number of received packets dropped by the interface by the input Queue of the hardware unit /software module associated with the VLAN. Packets are dropped when the input Queue is full or unable to processing incoming traffic.
Input Packets Error	Displays the number of packets with errors received on the interface. Input Packet Errors are input errors due to; no buffer space/ignored packets due to broadcast storms, packets larger than maximum packet size, framing errors, input rate exceeding the receiver's date handling rate or cyclic redundancy check errors. In all of these cases, an error is reported and logged.
Output Bytes	Displays the number of bytes transmitted from the interface.
Output Unicast Packets	Displays the number of unicast packets (packets directed towards a single destination address) transmitted from the interface.
Output NonUnicast Packets	Displays the number of unicast packets transmitted from the interface.

Output Total Packets	Displays the total number of packets transmitted from the interface.
Output Packets Dropped	Displays the number of transmitted packets dropped from the interface. Output Packets Dropped are packets dropped when the output queue of the device associated with the interface is saturated.
Output Packets Error	Displays the number of transmitted packets with errors. Output Packet Errors are the sum of all the output packet errors, malformed packets and misaligned packets received.

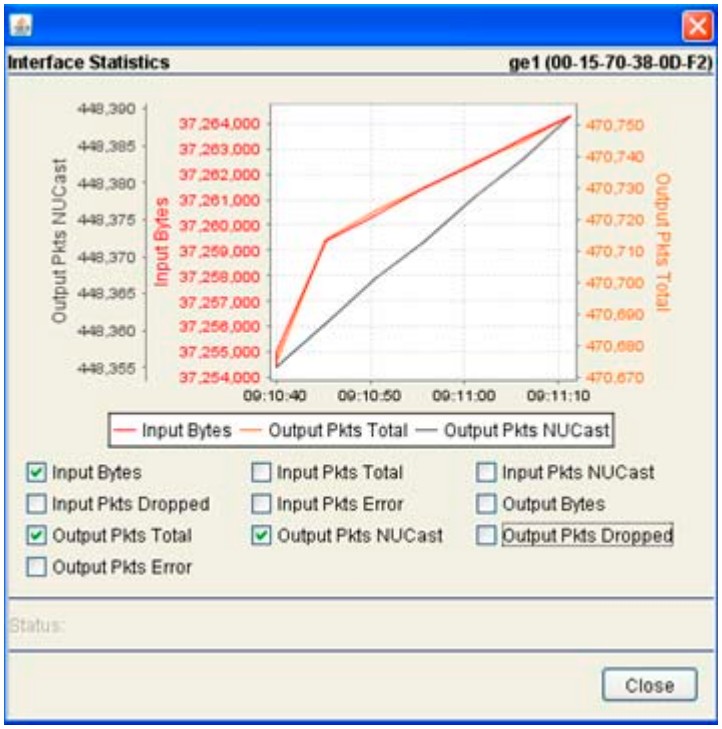
4. The **Status** is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click on the **Refresh** button to refresh the port statistics.
6. Click on the **Close** button to exit out of the screen.

3.2.3.2 Viewing the Port Statistics Graph

The switch continuously collects data for port statistics. Even when the port statistics graph is closed, data is still tallied. Periodically display the port statistics graph for assessing the latest information.

To view a detailed graph for a port:

1. Select a port from the table displayed in the Statistics screen.
2. Click the **Graph** button.



The **Interface Statistics** screen displays for the selected port. The screen provides the option to view the following:

- *Input Bytes*
- *Input Pkts Dropped*
- *Output Pkts Total*
- *Output Pkts Error*
- *Input Pkts Total*
- *Input Pkts Error*
- *Output Pkts NUCast*
- *Input Pkts NUCast*
- *Output Bytes*
- *Output Pkts Dropped*

3. Display any of the above by selecting the checkbox associated with it.

NOTE: You are not allowed to select (display) more than four parameters at any given time.

4. Click on the **Close** button to exit out of the screen.

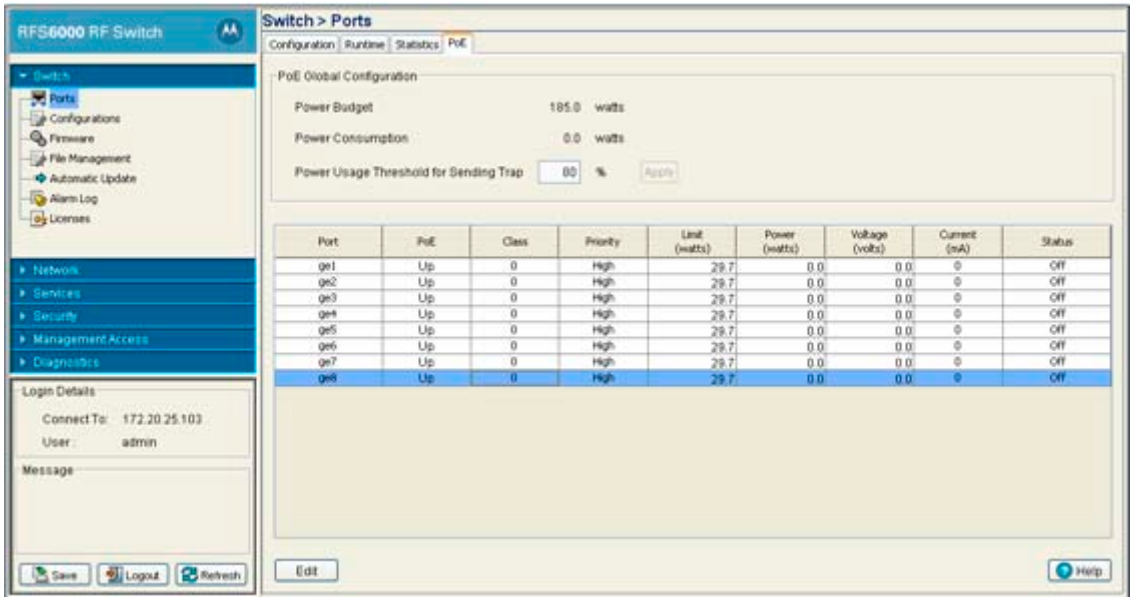
3.2.4 Power over Ethernet (PoE)

SWITCH NOTE: Power over Ethernet is only supported on the RFS6000 switch. The following information only applies to the RFS6000 switch.

The RFS6000 switch supports 802.3af *Power over Ethernet* (PoE) on each of its eight *ge* ports. The PoE screen allows users to monitor the power consumption of the ports and configure power usage limits and priorities for each of the *ge* ports.

To view the PoE configuration:

1. Select **Switch** > **Port** from the main menu tree.
2. Select the **PoE** tab



SWITCH NOTE: The PoE screen is only available on the RF6000 switch. The RFS7000 switch does not have Power over Ethernet on any ports and will not display the PoE tab.

The **PoE Global Configuration** section displays the following power information.

Power Budget	Displays the total watts available for Power over Ethernet on the switch.
Power Consumption	Displays the total watts in use by Power over Ethernet on the switch.
Power Usage Threshold for Sending Trap	Specify a percentage of power usage as the threshold before the switch sends an SNMP trap. The percentage is a percentage of the total power budget of the switch.

If you have modified the **Power Usage Threshold for Sending Trap** value, click the **Apply** button to save the changes.

Port	Displays the port name for each of the PoE capable ports.
PoE	Displays the PoE status of each PoE capable port. Status will display Up when PoE is available on the port and Down when PoE is unavailable on the port.
Class	Displays the IEEE Power Classification for each port:

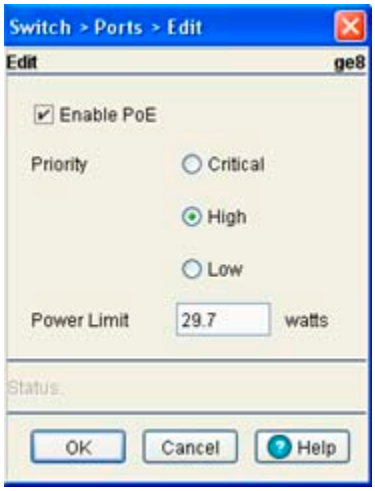
Class Number	*Maximum Power Required from Switch*
0 (unknown)	15.4 Watts
1	4 Watts
2	7 Watts
3	15.4 Watts

Priority	Displays the priority mode for each of the PoE ports. The priority options are: • **Critical** • **High** • **Low**
Limit (watts)	Displays the power limit in watts for each of the PoE ports. The maximum power limit per port is 29.7 watts.
Power (watts)	Displays each PoE ports power usage in watts.
Voltage (volts)	Displays each PoE ports voltage usage in volts.
Current (mA)	Displays each PoE ports current usage in miliAmps.
Status	Displays the operational status for each PoE port. Ports can be either **On** or **Off**.

3.2.5 Editing Port PoE Settings

To modify the PoE settings for a port:

1. Select a port to edit from the table.
2. Click the **Edit** button.
   The **PoE Edit** screen shows the port PoE status, Priority and Power Limit.



3. Check the **Enable PoE** checkbox to configure the selected port to use Power over Ethernet. To disable PoE on a port, uncheck this box.
4. Select the **Priority** level for PoE on this port. The **Priority** level is used in cases where the switch's PoE power consumption exceeds the available power. When this happens, ports with higher **Priority** levels will be given precedence over those with a lower **Priority** level.
5. Set the **Power Limit** (in watts) for this port's PoE usage. Setting the **Power Limit** places a cap on the maximum amount of power which can be drawn from the selected port.
6. Click **OK** to save and add the changes to the running configuration and close the dialog.

3.3 Viewing Switch Configurations

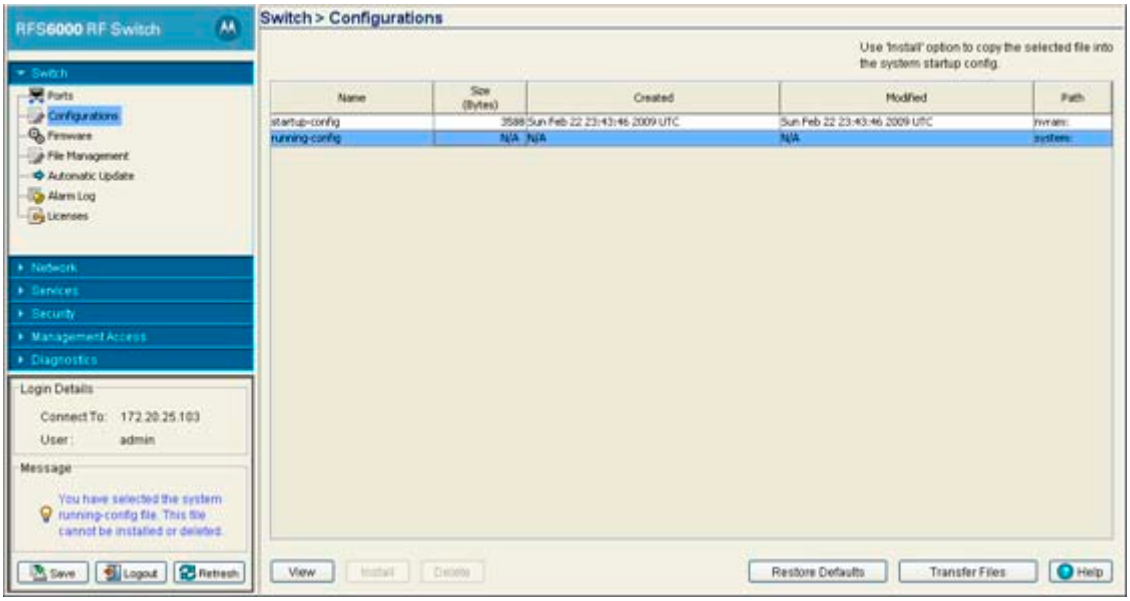
Use the **Configurations** screen to review the configuration files available to the switch. The details of each configuration can be viewed individually. Optionally, edit the file to modify its name or use the file as the switch startup configuration. A file can be deleted from the list of available configurations or transferred to a user specified location.

NOTE: To view the entire switch configuration using SNMP, the switch CLI provides a better medium to review the entire switch configuration.

NOTE: The *Motorola RF Management Software* is a recommended utility to plan the deployment of the switch and view its configuration once operational in the field. Motorola RFMS can help optimize the positioning and configuration of a switch (and its associated radios) in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Motorola Web site.

To view the Configuration files available to the switch:

1. Select **Switch** > **Configurations** from the main menu tree.



The following information is displayed in tabular format. Configuration files (with the exception of startup-config and running-config) can be edited, viewed in detail or deleted.

Name	Displays the name of each existing configuration file.
Size (Bytes)	Displays the size (in bytes) of each available configuration file.
Created	Displays the date and time each configuration file was created. Use this information as a baseline for troubleshooting problems by comparing event log data with configuration file creation data.

Modified	Displays the date and time each configuration file was last modified. Compare this column against the Created column to discern which files were modified and make informed decisions whether existing files should be further modified or deleted.
Path	Displays the path (location) to the configuration file.

2. To view the contents of a config file in detail, select a config file by selecting a row from the table and click the **View** button. For more information, see *Viewing the Detailed Contents of a Config File*.
3. Select a configuration (other than the start-up-config or running config) and click the **Install** button to install the file on the switch and replace the existing startup-config file.

   If a file (for example, *sample-config*) is selected, a message displays stating, "When *sample-config* is installed, it will replace start-up config. Are you sure you want to install *sample-config."* Click **Yes** to continue.

NOTE: Selecting either the startup-config or running-config does not enable the Edit button. A different configuration must be available to enable the Edit function for the purposes of replacing the existing startup-config.

4. To permanently remove a file from the list of configurations available to the switch, select a configuration file from the table and click the **Delete** button.

   If startup-config is deleted, a prompt displays stating the default switch startup-config will automatically take its place. The switch running-config cannot be deleted.
5. To restore the system's default configuration and revert back to factory default, click the **Restore Defaults** button.

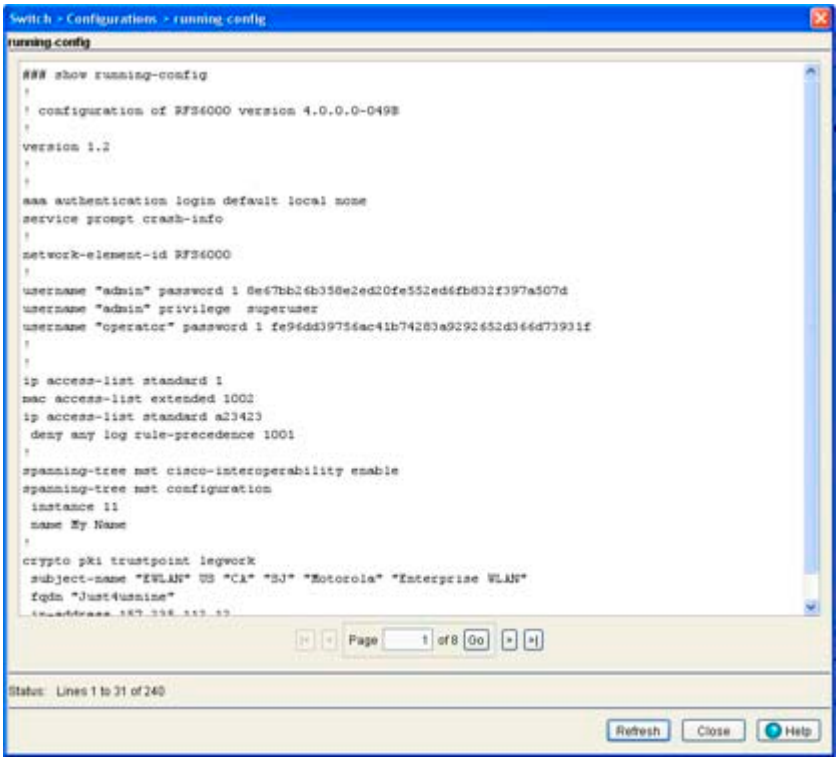
NOTE: After setting the switch to revert to factory default settings, the system must be rebooted before the default settings take effect. When this occurs, the switch IP address may change.

6. Click the **Transfer Files** button to move a target configuration file to a secure location for later use. For more information, see *Transferring a Config File*.

3.3.1 Viewing the Detailed Contents of a Config File

The View screen displays the entire contents of a configuration file. Motorola recommends a file be reviewed carefully before it is selected from the Config Files screen for edit or designation as the switch startup configuration.

1. Select a configuration file from the Configuration screen by highlighting the file.
2. Click the **View** button to see the contents of the selected configuration file.



Use the up and down navigation facilities on the right-hand side of the screen to view the entire page.

3. The **Page** parameter displays the portion of the configuration file in the main viewing area.

   The total number of pages in the file are displayed to the right of the current page. The total number of lines in the file display in the Status field at the bottom of the screen.

   Scroll to corresponding pages as required to view the entire contents of the file. To navigate to a specific page, enter the page number in the text area (next to Page item) and click on the **Go** button. The source parameter differs depending on the source selected.

4. Refer to the **Status** field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.

5. Click the **Refresh** button to get the most recent updated version of the configuration file.

6. Click **Close** to close the dialog without committing updates to the running configuration.

3.3.2 Transferring a Config File

Transfer a configuration file to and from the switch using the **Transfer** screen. Transferring the switch configuration is recommended to keep viable configurations available in a secure location. The following file transfer configurations are possible:

- *switch to switch, server or local disk*
- *server to switch*
- *local disk to switch*

To transfer the contents of a configuration file:

1. Click the **Transfer Files** button on the bottom of the Configuration screen.

2. Refer to the **Source** field to define the location and address information for the source config file.

From	Select the location representing the source file's current location using the **From** drop-down menu. Options include **Server, Local Disk** and **Switch**.
File	Specify a source file for the file transfer. If the switch is selected, the file used at startup automatically displays within the File parameter.
Using	Refer to the **Using** drop down-menu to configure whether the log file transfer is conducted using FTP or TFTP. FTP transfers require a valid user ID and password.
IP Address	Enter the **IP Address** of the server or system receiving the source configuration. Ensure the IP address is valid or risk jeopardizing the success of the file transfer.
User ID	Enter the **User ID** credentials required to transfer the configuration file from a FTP server.
Password	Enter the **Password** required to send the configuration file from an FTP server.
Path	Specify an appropriate **Path** name to the target directory on the local system disk or server. The Target options are different depending on the target selected.

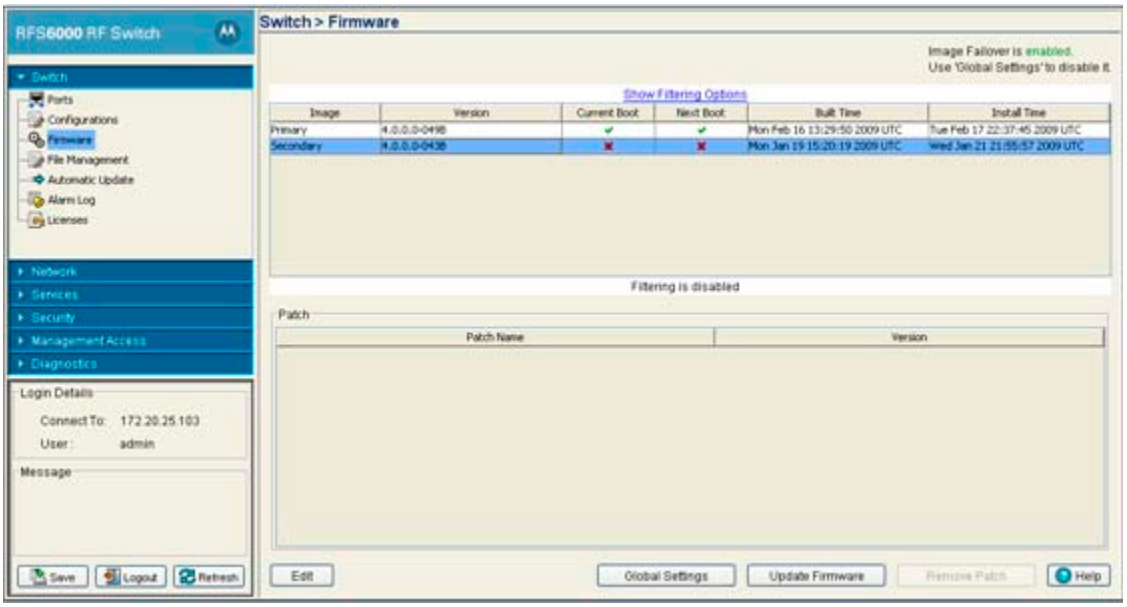
3. Refer to the **Target** field to specify the details of the target file.

To	Use the **To** drop-down menu to define the location of the configuration file. Options include the switch (default location), external server or local disk.
File	Use the **File** field to specify a target file for the file transfer. Use the File Browser icon to search attached files systems for target file location.

4. Refer to the **Status** field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click the **Transfer** button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired configuration file to the specified location.
6. Click the **Abort** button to cancel the file transfer process before it is complete.
7. Click the **Close** button to exit the Transfer screen and return to the Config Files screen. Once a file is transferred, there is nothing else to be saved within the Transfer screen.

3.4 Viewing Switch Firmware Information

The switch can store (retain) two software versions (primary and secondary). Information supporting the two versions displays within the **Firmware** screen. The **Version** column displays the version string. The **Build Time** is the date and time each version was generated. **Install** represents the date and time the upgrade was performed. **Next Boot** indicates which version should be used on the next reboot. The Next Boot version should match the **Running Version**, unless the system has failed over to another version.



To view the firmware files available to the switch:

1. Select **Switch** > **Firmware** from the main menu tree.
2. Refer to the following information displayed within the Firmware screen:

Image	Displays whether a firmware image is the primary image or a secondary image. The primary image is typically the image loaded when the switch boots.
Version	Displays a unique alphanumeric version for each firmware file listed.
Current Boot	A check mark within this column designates this version as the version used by the switch the last time it was booted. An **"X"** in this column means this version was not used the last time the switch was booted.
Next Boot	A check mark within this column designates this version as the version to be used the next time the switch is booted. An **"X"** in this column means this version will not be used the next time the switch is booted. To change the boot designation, highlight an image and click the **Edit** button.
Built Time	Displays the time the version was created (built). Do not confuse the Built Time with the time the firmware was last loaded on the switch.
Install Time	The Install Time is the time this version was loaded with on the switch. Periodically review this information to assess the relevance of older files.

3. Refer to the **Patch** field for a listing of those Patches available to the switch. The name and version of each patch file is displayed. Each patch file has an associated .txt file designation. the text file describes nuances associated with the file that may make it optimal for use with the switch.
4. Select an existing firmware version and click the **Edit** button to change the firmware version used when the switch is booted the next. For more information, see *Editing the Switch Firmware*.
5. Click on the **Global Settings** button to specify a firmware version for use with the failover image. For more information, see *Enabling Global Settings for the Image Failover*.

6. Click on the **Update Firmware** button to update the firmware file loaded onto the switch. For more information, see *Updating the Switch Firmware*.

NOTE: To apply a patch to the switch follow the same instructions for updating the switch's firmware.

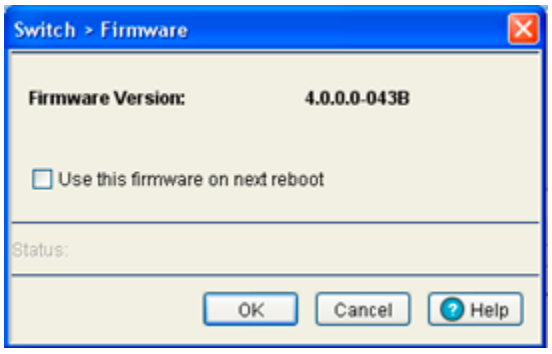
7. To remove a patch, select it from amongst those displayed within the Patch field and click the **Remove Patch** button.

3.4.1 Editing the Switch Firmware

The Edit screen enables the user to select a firmware file and designate it as the version used the next time the switch is booted.

1. Select the primary firmware image from the Firmware screen.
2. Click the **Edit** button.

   The **Firmware** screen displays the current firmware version and whether this version is used for the next reboot.



3. Select the checkbox to use this version on the next boot of the switch.
4. To edit the secondary image, select the secondary image, click the **Edit** button and select the **Use this firmware on next reboot** checkbox.

   This firmware version will now be invoked after the next reboot of the switch.
5. Refer to the **Status** field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click the **OK** button to commit the changes made and exit the screen.

3.4.2 Enabling Global Settings for the Image Failover

Use the **Global Settings** screen to specify a firmware version for use with the failover image.

1. Select an image from the table in the Firmware screen.
2. Click the **Global Settings** button.
3. Select the **Enable Image Failover** checkbox to load an alternative firmware version if the WLAN module fails to load the selected version successfully after 2 reboot attempts.

4. Refer to the **Status** field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click **OK** to save and add the changes to the running configuration and close the dialog.

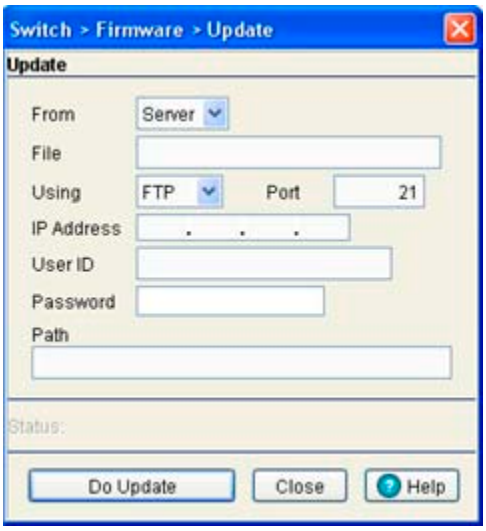
3.4.3 Updating the Switch Firmware

Use the **Update** screen to update the firmware version currently used by the switch.

NOTE: When performing a firmware update using the switch CLI, use the following syntax (specific to FTP) *ftp://username:password@ipaddress:port/path/filename*. If using TFTP, use *tftp://ipaddress/path/filename*.

NOTE: When performing a firmware update using FTP be sure TCP port 21 is open between the switch and the FTP server where the firmware file is located.

1. Select an image from the table in the Firmware screen.
2. Click the **Update Firmware** button.



3. Use the **From** drop-down menu to specify the location from which the file is sent.
4. Enter the name of the file containing the firmware update in the **File** text field.

   This is the file that will append the file currently in use.
5. From the **Using** drop down menu, select either FTP or TFTP as a medium to update the firmware.
   a. Use **FTP** to get the firmware update from a *File Transfer Protocol* (FTP) server. A user account must be established on the FTP server specified for the firmware update.
   b. Use **TFTP** to get the firmware update from a *Trivial File Transfer Protocol* (TFTP) server.

SWITCH NOTE: On the RFS7000, users can also transfer firmware files using USB or Compact Flash. On the RFS6000, users can transfer firmware files using USB.

6. Enter the IP address for the FTP or TFTP server in the **IP address** field.
7. Enter the username for FTP server login in the **User ID** field.

8. Enter the password for FTP server login in the **Password** field.
9. Enter the complete file path for the file that contains the firmware update in the **Path** field.
10. Click the **Do Update** button to initiate the update.

    A warning prompt displays. Upon confirming the firmware update, the switch reboots and completes the firmware update.

CAUTION: When restarting or rebooting the switch, the Radius server is restarted regardless of its state before the reboot.

11. Click **OK** to add the changes to the running configuration and close the dialog.
12. Refer to the **Status** field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
13. Click **Cancel** to close the dialog without committing updates to the running configuration.

3.5 Switch File Management

Use the File Management screen to transfer configuration file to and from the switch and review the files available.

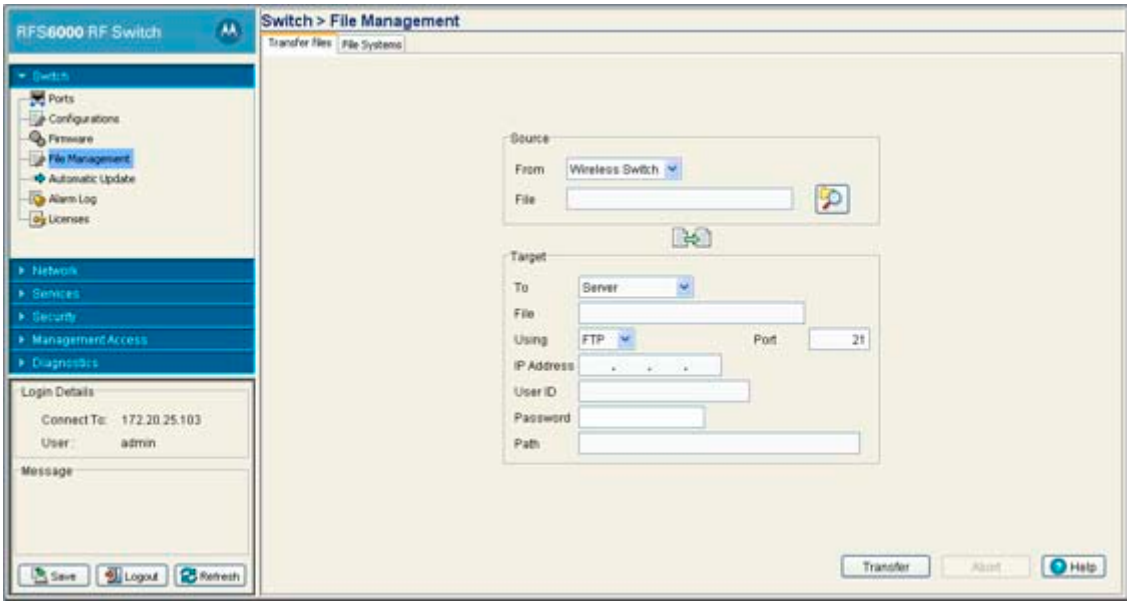
3.5.1 Transferring Files

Use the **Transfer Files** screen to transfer files to and from the switch.Transferring files is recommended to keep files in a secure location. The following file transfer options are available:

- *Wireless Switch to Wireless Switch*
- *Wireless Switch to Server*
- *Server to Wireless Switch*

To define the properties of the file transfer configuration:

1. Select **Switch** > **File Management** from the main menu tree.



2. Refer to the **Source** field to specify the details of the source file.

From

Use the **From** drop-down menu to select the source file's current location. The options include Wireless Switch and Server. The following transfer options are possible:

- *Wireless Switch to Wireless Switch*
- *Wireless Switch to Server*
- *Server to Wireless Switch*

The parameters displayed in the **Source** and **Target** fields differ based on the above selection. These different kinds of file transfer techniques are described in the sections that follow.

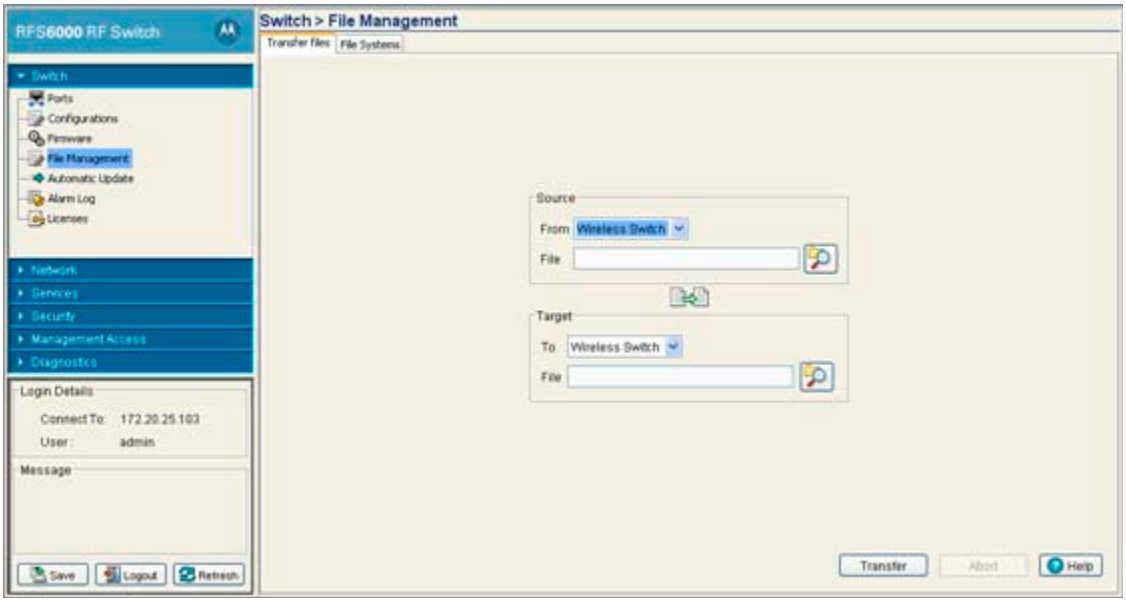
File

Use the **Browse** button to navigate to a target file for transfer. If the switch is selected from the From drop-down menu (within the Source field), the file used at startup automatically displays.

3.5.1.1 Transferring a file from Wireless Switch to Wireless Switch

To transfer a file from one switch to another:

1. Select **Wireless Switch** from the **From** drop-down menu.

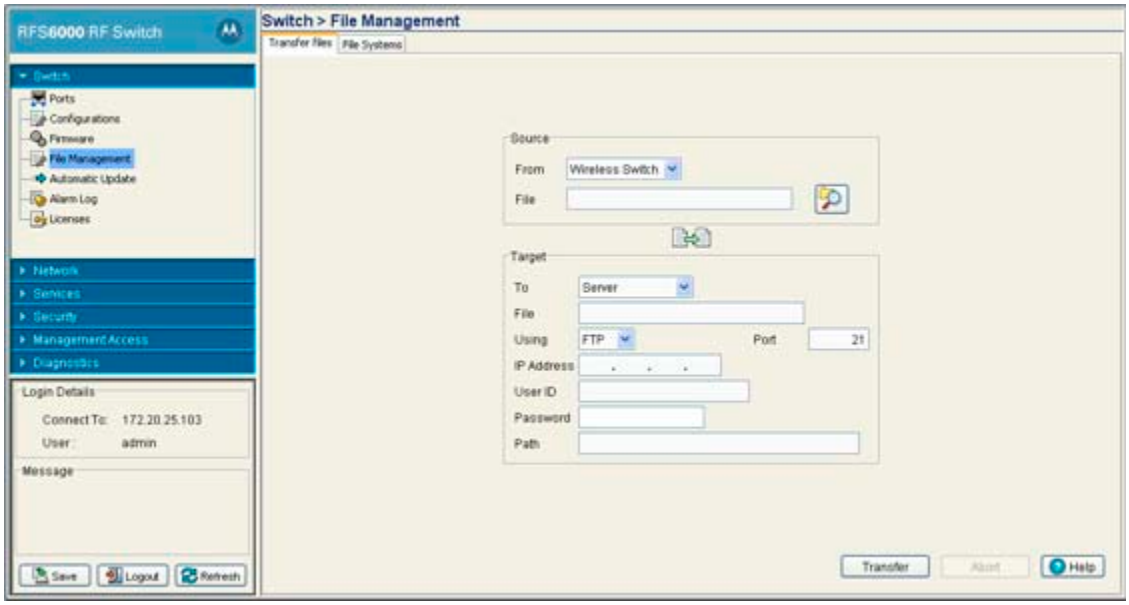


2. Use the **Browse** button to locate a target file for the file transfer.
3. Use the **To** drop-down menu (within the **Target** field) and select **Wireless Switch.** This defines the location of the file.
4. Use the **Browse** button to define a location for the transferred file.
5. Click the **Transfer** button to complete the file transfer.
6. The **Message** section in the main menu area displays the file transfer message.
7. Click **Abort** at any time during the transfer process to abort the file transfer.

3.5.1.2 Transferring a file from a Wireless Switch to a Server

To transfer a file from the switch to a Server:

1. Refer to the **Source** field to specify the source file. Use the **From** drop-down menu and select Wireless Switch.



2. Use the **Browse** button and select a file for transfer.
3. Use the **To** drop-down menu (within the Target field) and select **Server**. This defines the transfer location of the configuration file. Enter the file location marked to store the transferred file.
4. Use the **Using** drop down-menu to configure whether the log file transfer is conducted using FTP, TFTP, HTTP or SFTP. This field display the default port for FTP,TFTP, HTTP or SFTP. The value in this field can be configured as required. Enter the IP Address of the server receiving the source configuration. Ensure the IP address is valid or risk jeopardizing the success of the file transfer. Enter the User ID credentials required to transfer the configuration file from a FTP server.

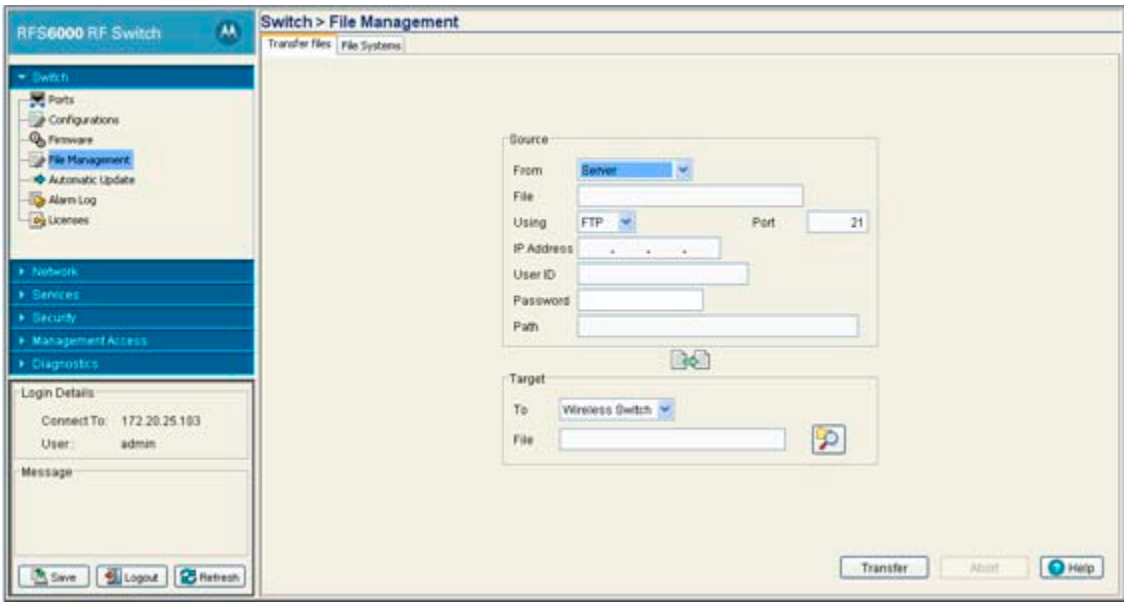
SWITCH NOTE: On the RFS7000 users can also transfer files using USB or Compact Flash. On the RFS6000 users can also transfer files using USB.

5. Enter the **Password** required to send the configuration file from an FTP server.
6. Specify the appropriate **Path** name to the target directory on the server. The target options are different depending on the target selected.
7. Click the **Transfer** button to complete the file transfer. The **Message** section in the main menu area displays the file transfer message.
8. Click **Abort** at any time during the transfer process to abort the file transfer.

3.5.1.3 Transferring a file from a Server to a Wireless Switch

To transfer a file from a Server to the switch:

1. Refer to the **Source** field to specify the details of the source file. Use the **From** drop-down menu and select **Server**.



2. Provide the name of the **File**.
3. Use the **Using** drop-down menu to configure whether the file transfer is conducted using FTP, TFTP or HTTP.

   FTP transfers require a valid user ID and password.
4. Enter an **IP Address** of the server receiving the configuration file. Ensure the IP address is valid or risk jeopardizing the success of the file transfer.
5. Enter the **User ID** credentials required to transfer the configuration file from a FTP server.
6. Enter the **Password** required to send the configuration file from an FTP server.
7. Specify the appropriate **Path** name to the target directory on the server. The Target options are different depending on the target selected.
8. Use the **To** drop-down menu (within the Target field) and select Wireless Switch.
9. Use the **Browse** button to browse and select the location to store the file marked for transfer.
10. Click the **Transfer** button to complete the file transfer. The **Message** section displays the status of the file transfer message.
11. Click **Abort** button any time during the transfer process to abort the file transfer.

3.5.2 Viewing Files

Use the **File System** tab to review the files available to the switch. The switch maintains the following file types:

- *flash*
- *nvram*
- *system*
- *Compact Flash*
- *USB 1*

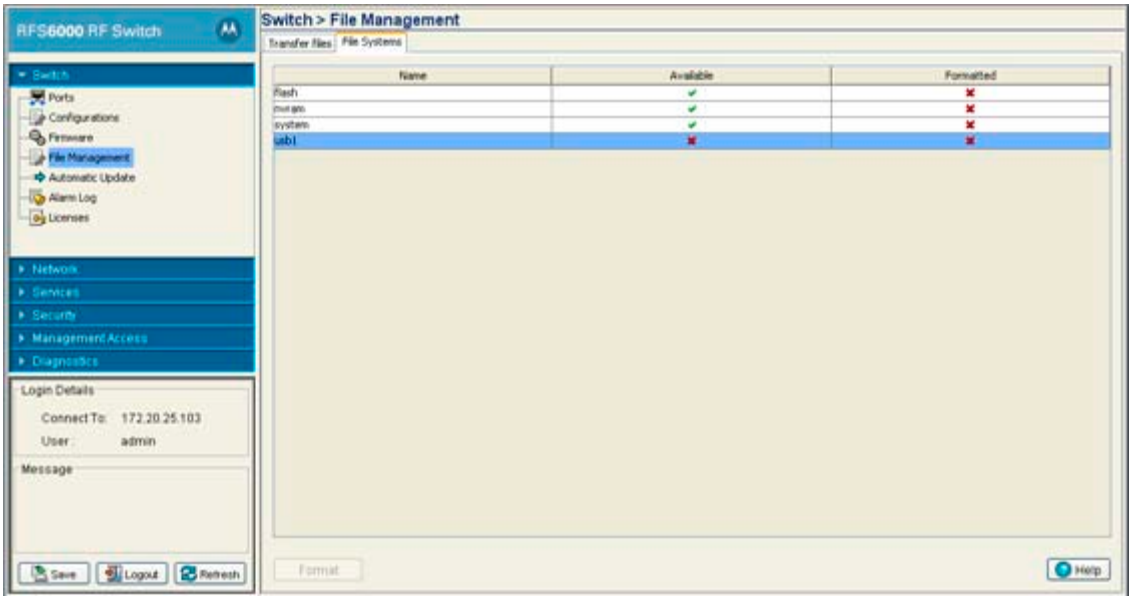
- *USB 2*

SWITCH NOTE: USB 1 is available on the RFS6000 and RFS7000 switches. USB2 and Compact Flash are only available on the RFS7000 switch.

Transfer files between the switch and the server from any one of the above mentioned locations. Since compact flash (CF) and USB are external memory locations, the File System window displays the status of these devices. Transfer files to compact flash and USB only if they are connected and available.

To view the file systems currently available to the switch:

1. Select **Switch** > **File Management** from the main menu tree.
2. Select the **File Systems** tab.



3. Refer to the following **File Systems** information.

Name	Displays the memory locations available to the switch.
Available	Displays the current status of the memory resource. By default, nvram and system are always available. • A green check indicates the device is currently connected to the switch and is available. • A red X indicates the device is currently not available.
Formatted	This displays the format status of the memory devices. This ensures that the external and internal memory device store the files securely. A formatted memory device is less prone to crash and loss of data. • A green check mark indicates the device is currently connected to the switch and is available. • A red X indicates the device is currently not available.

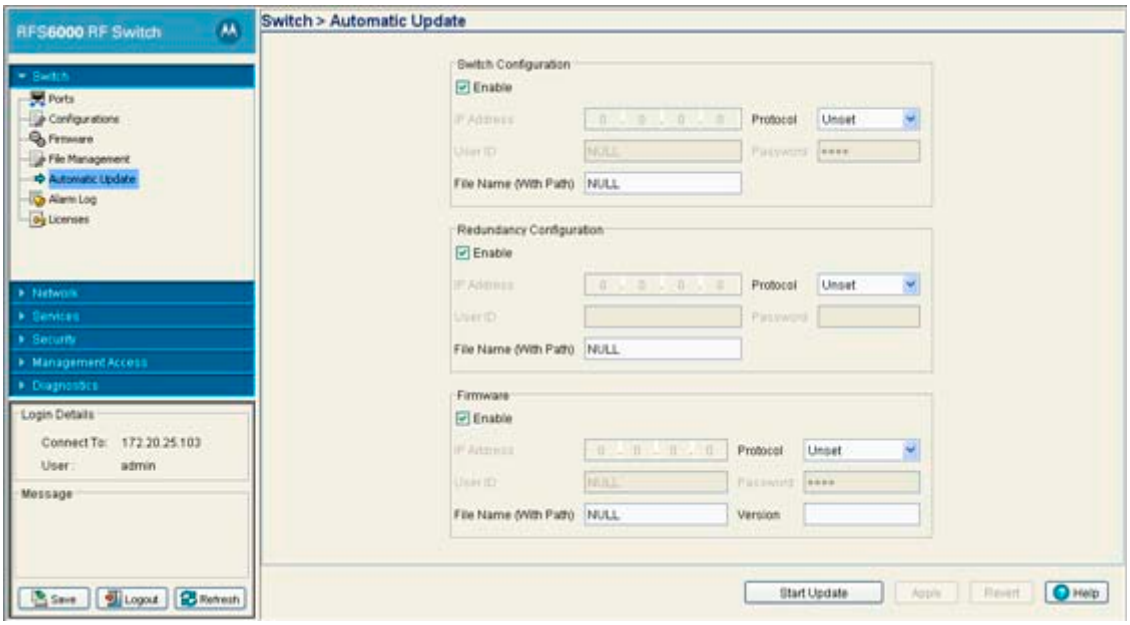
4. Select CF, USB1 or USB2 and click the **Format** button (enabled only if the CF or USB are connected to the switch) to check if the memory device is formatted and available. You will be prompted that proceeding will erase all data on the disk and if you would like to proceed.

3.6 Configuring Automatic Updates

Use the **Automatic Updates** screen to enable a facility that will poll a server address (you designate) when the switch is booted. If updates are found since the last time the switch was booted, the updated version is uploaded to the switch the next time the switch is booted. Enable this option for either the firmware, configuration file or cluster configuration file. Motorola recommends leaving this setting disabled if a review of a new file is required before it is automatically uploaded by the switch.

To enable and configure the automatic update feature for switch firmware, configuration files and cluster configurations:

1. Select **Switch** > **Automatic Updates** from the main menu tree.



2. Refer to the **Switch Configuration** field to enable and define the configuration for automatic configuration file updates. If enabled, the located (updated) configuration file will be used with the switch the next time the switch boots.

Enable	Select the **Enable** checkbox to allow an automatic configuration file update when a newer (updated) file is detected (upon the boot of the switch) at the specified IP address.
IP Address	Define the **IP address** of the server where the configuration files reside. If a new version is detected when the switch is booted, it is uploaded to the switch and used upon the next boot of the switch.
User ID	Enter the **User ID** required to access the FTP or TFTP server.
File Name (With Path)	Provide the complete and accurate path to the location of the configuration files on the server. This path must be accurate to ensure the most recent file is retrieved.

Protocol	Use the **Protocol** drop-down menu to specify the **FTP, TFTP, HTTP, SFTP** or resident switch **FLASH** medium used for the file update from the server. FLASH is the default setting.
Password	Enter the password required to access the server.

SWITCH NOTE: In addition to the **Protocols** listed, on the RFS7000 users can also auto-update using USB or Compact Flash. On the RFS6000 users can also auto-update using USB.

3. Refer to the **Redundancy Configuration** field to enable and define the configuration for automatic cluster file updates.

Enable	Select the **Enable** checkbox to allow an automatic cluster file update when a new (updated) file is detected (upon the boot of the switch) at the specified IP address.
IP Address	Define the **IP address** of the server where the cluster files reside. If a new version is detected when the switch is booted it will be uploaded to the switch and used upon the next boot of the switch.
User ID	Enter the **User ID** required to access the FTP or TFTP server.
File Name (With Path)	Provide the complete and accurate path to the location of the cluster files on the server. This path must be accurate to ensure the most recent file is retrieved.
Protocol	Use the **Protocol** drop-down menu to specify the **FTP, TFTP, HTTP, SFTP** or resident switch **FLASH** medium used for the file update from the server. FLASH is the default setting.
Password	Enter the password required to access the server.

4. Refer to the **Firmware** field to enable and define the configuration for automatic firmware updates. If enabled, the located (updated) switch firmware is used with the switch the next time the switch boots.

Enable	Select the **Enable** checkbox to allow an automatic firmware update when a new (updated) version is detected (upon the boot of the switch) at the specified IP address.
IP Address	Define the **IP address** of the server where the firmware files reside. If a new version is detected when the switch is booted it will be uploaded to the switch and used upon the next boot of the switch.
User ID	Enter the **User ID** required to access the FTP or TFTP server.
File Name (With Path)	Provide the complete and accurate path to the location of the firmware files on the server. This path must be accurate to ensure the file is retrieved.
Protocol	Use the **Protocol** drop-down menu to specify the **FTP, TFTP, HTTP, SFTP** or resident switch **FLASH** medium used for the file update from the server. FLASH is the default setting.
Password	Enter the password required to access the server.
Version	Provide the target firmware version to ensure the switch is upgrading to the intended baseline.

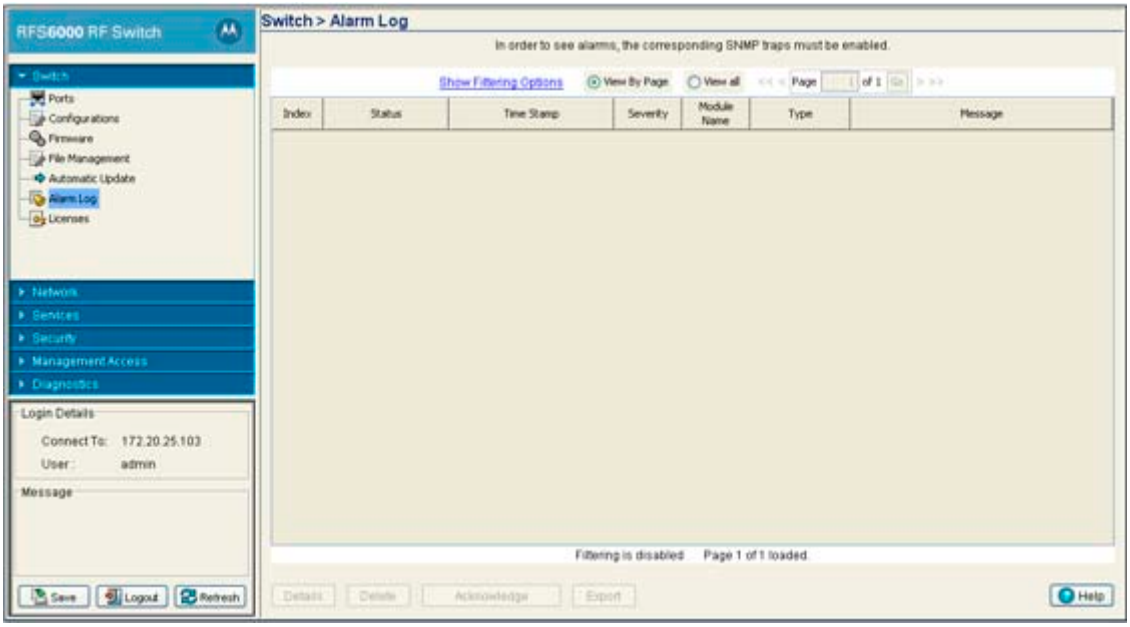
5. Select the **Start Update** button to begin the file updates for the enabled switch configuration, cluster configuration or firmware facilities.
6. Click the **Apply** button to save the changes to the configuration.
7. Click the **Revert** button to revert back to the last saved configuration.

3.7 Viewing the Switch Alarm Log

Use the **Alarm Log** screen as an initial snapshot for alarm log information. Expand alarms (as needed) for greater detail, delete alarms, acknowledge alarms or export alarm data to a user-specified location for archive and network performance analysis.

To view switch alarm log information:

1. Select **Switch** > **Alarm Log** from the main menu tree.



2. Use the Alarm Log screen's filtering options to view alarm log data by page or the by its entire content.
3. Select either of the two available options to view alarm log information:

View By Page	Select the **View By Page** radio button to view alarm log information on a per page basis. Use the View By Page option to page through alarm logs. If there are a large number of alarms, the user can navigate to the page that has been completely loaded. All operations can be performed on the currently loaded data. Enter a page number next to "Page" and click the **Go** button to move to the specific page.
View All	Select the **View All** radio button to display the complete alarm log with in the table. If there are a large number of alarms, the View All option will take several minutes to load.

4. Refer to the table within the **Alarm Log** screen for the following information:

Index	Displays the unique numerical identifier for trap events (alarms) generated in the system. Use the index to help differentiate an alarm from others with similar attributes.
Status	Displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status displays error messages if something goes wrong in the transaction between the applet and the switch.
Time Stamp	Displays the date, year and time the alarm was raised (as well as the time zone of the system). The time stamp only states the time the alarm was generated, not the time it was acknowledged.
Severity	Displays the severity level of the event. Use this (non numerical and verbal) description to assess the criticality of the alarms. Severity levels include: • *Critical* • *Major* • *Warning* • *Informational* • *Normal*
Module Name	Displays the module name that triggered this alarm. Use this information to assess if this alarm is a recurring problem or if it is an isolated incident.
Type	Displays the alarm type.
Message	Displays a detailed event message corresponding to the alarm event. It contains an event specific message for information about the alarm. Use this value along with the Details description for optimal problem event identification.

5. Select an alarm and click the **Details** button to display an alarm description along with a system proposed solution and possible causes. For more information, see *Viewing Alarm Log Details*.
6. Select the alarm(s) from those listed and click the **Delete** button to remove them from the list of alarms.

   This is not recommended in instances where the problem is unacknowledged and the criticality has not yet been assessed.
7. Select the unacknowledged alarm(s) from those listed and click the **Acknowledge** button to acknowledge them.
8. Click the **Export** button to export the content of the table to a *Comma Separated Values* file (CSV).

3.7.1 Viewing Alarm Log Details

Use the **Details** option when additional information is required for a specific alarm to make an informed decision on whether to delete, acknowledge or export the alarm.

To review switch alarm details:

1. Select **Switch** > **Alarm Log** from the main menu tree.
2. Select an alarm and click the **Details** button.

3. Refer to the **Alarm Details** and **Alarm Message** for the following information:

Description	Displays the details of the alarm log event. This information can be used in conjunction with the **Solution** and **Possible Causes** items to troubleshoot the event and determine how the event can be avoided in the future.
Solution	Displays a possible solution to the alarm event. The solution should be attempted first to rectify the described problem.
Possible Causes	Describes the probable causes that could have raised this specific alarm. Determine whether the causes listed can be remedied to avoid this alarm from being raised in the future.
Alarm Message	Displays the radio (and MAC address if relevant) reporting the alarm detail information.

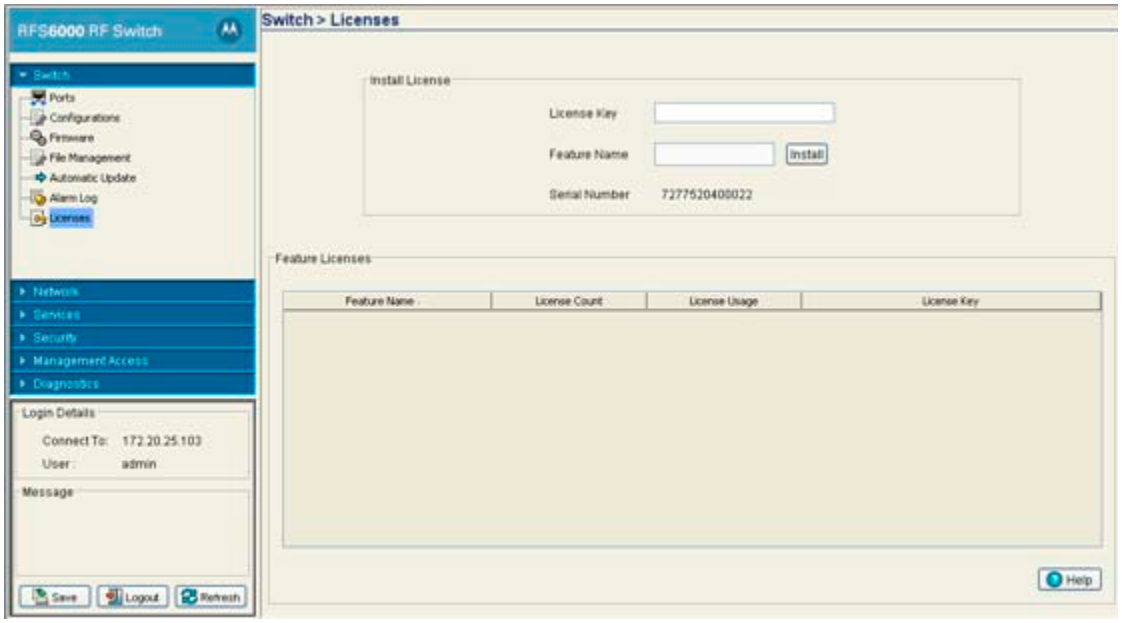
4. Click **Close** to exit the dialog.

3.8 Viewing Switch Licenses

Use the **Licenses** screen to install and add a new switch license.

To install a new license:

1. Select **Switch** > **Licenses** from the main menu tree.



2. Refer to the **Install License** field for the following information:

License Key	Enter the license key required to install a particular feature. The license key is returned when you supply the switch serial number to Motorola support.
Feature Name	Enter the name of the feature you wish to install/upgrade using the license.
Serial Number	Displays the serial number of the switch used for generating the license key.

3. Click the **Install** button to install the selected license.

4. Refer to the **Feature Licenses** table for the following license specific information:

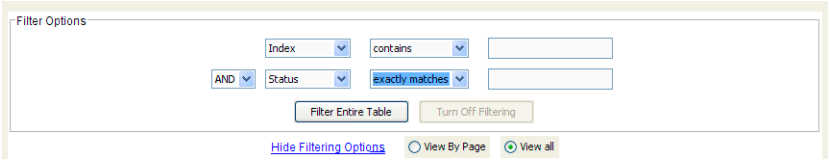
Feature Name	Displays the name of the feature either installed or upgraded on the switch.
License Count	Displays the number of licenses applied while entering the license key.
License Usage	Lists the number of license in use. Determine whether this number adequately represents the number of switches needed to deploy.
License Key	The license key for the feature installed/upgraded.

5. Select a license from the table and click the **Delete** button to remove the license from the list available to the switch.

3.9 How to use the Filter Option

Use the Filter Option to sort the display details of screen that employ the filtering option as a means of sorting how data is displayed within the screen.

1. Click the **Show Filtering Option** to expand the Filter Option zone, whenever it appears in any screen.



2. Enter the filter criteria as per the options provided in the Filter Option zone.

   The parameters in the Filter Option field are populated with the parameters of the screen in which it appears. Not all switch Web UI's contain the filtering option.

3. Click the **Filter Entire Table** button to filter the entire table in which the filter zone appears.

   The result of the filtering operation displays at the bottom of the table

4. Click the **Turn Off Filtering** button to disable the filtering option for the screen where it appears.

   Filtering status (when filtering is turned off) displays at the bottom of the table.

5. Click the **Hide Filtering Option** button to hide the Filter Option zone.

4

Network Setup

This chapter describes the Network Setup menu information used to configure the switch. This chapter consists of the following switch Network configuration activities:

- *Displaying the Network Interface*
- *Viewing Network IP Information*
- *Viewing and Configuring Layer 2 Virtual LANs*
- *Configuring Switch Virtual Interfaces*
- *Viewing and Configuring Switch WLANs*
- *Viewing Associated MU Details*
- *Viewing Access Port Information*
- *Viewing Access Port Adoption Defaults*
- *Viewing Adopted Access Ports*
- *Multiple Spanning Tree*
- *Configuring IGMP Snooping*

NOTE: HTTPS must be enabled to access the switch applet. Ensure HTTPS access has been enabled before using the login screen to access the switch applet.

4.1 Displaying the Network Interface

The main **Network** interface displays a high-level overview of the configuration (default or otherwise) as defined within the Network main menu. Use the information to determine if items require additional configuration using the sub-menu items under the main Network menu item.

NOTE: When the switch's configuration is successfully updated (using the Web UI), the effected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the effected screen's Status field and the screen remains displayed. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To view the switch's Network configuration:

1. Select **Network** from the main menu tree.

2. Refer to the following information to discern if configuration changes are warranted:

DNS Servers	Displays the number of DNS Servers configured thus far for use with the switch. For more information, see *Viewing Network IP Information on page 4-4*.
IP Routes	Displays the number of IP routes for routing packets to a defined destination. For information on defining IP Routes, see *Configuring IP Forwarding on page 4-6*.
Additional Resolution Entries	Displays the number of layer three (IP) address to layer two (MAC) address mappings. For more information, see *Viewing Address Resolution on page 4-8*.
Switch Virtual Interfaces	Displays the number of virtual interfaces (VLANs) defined thus far for the switch. New VLANs can be defined or existing VLANs can be modified as needed. For more information, see *Configuring Switch Virtual Interfaces on page 4-14*.
Wireless LANs	Displays the number of WLANs currently defined on the switch. The switch has 32 default WLANs. New WLANs can be added as needed, and their descriptions, VLAN assignments and security schemes modified. For more information, see *Viewing and Configuring Switch WLANs on page 4-22*.
Mobile Units	Displays the number of MUs currently associated to (and interacting with) the switch. The details of individual MUs can be displayed as needed. For more information, see *Viewing Associated MU Details on page 4-81*.
Access Ports	Displays the number of *Access Ports* (APs) active on the switch. Access ports can be added or existing APs can have their VLAN assignments changed, their descriptions modified and their current authentication and encryption schemes modified. For more information, see *Viewing Access Port Information on page 4-90*.
Radios	Displays the number of AP radios detected over the switch managed network. Displayed with this information is the number of radios detected that have been adopted by the switch. For more information, see *Configuring Access Port Radios on page 4-91*.

The **Apply** and **Cancel** buttons are greyed out within this screen, as there is no data to be configured or saved.

4.2 Viewing Network IP Information

Use the **Internet Protocol** screen to view and configure network associated IP details. The Internet Protocol screen contains tabs supporting the following configuration activities:

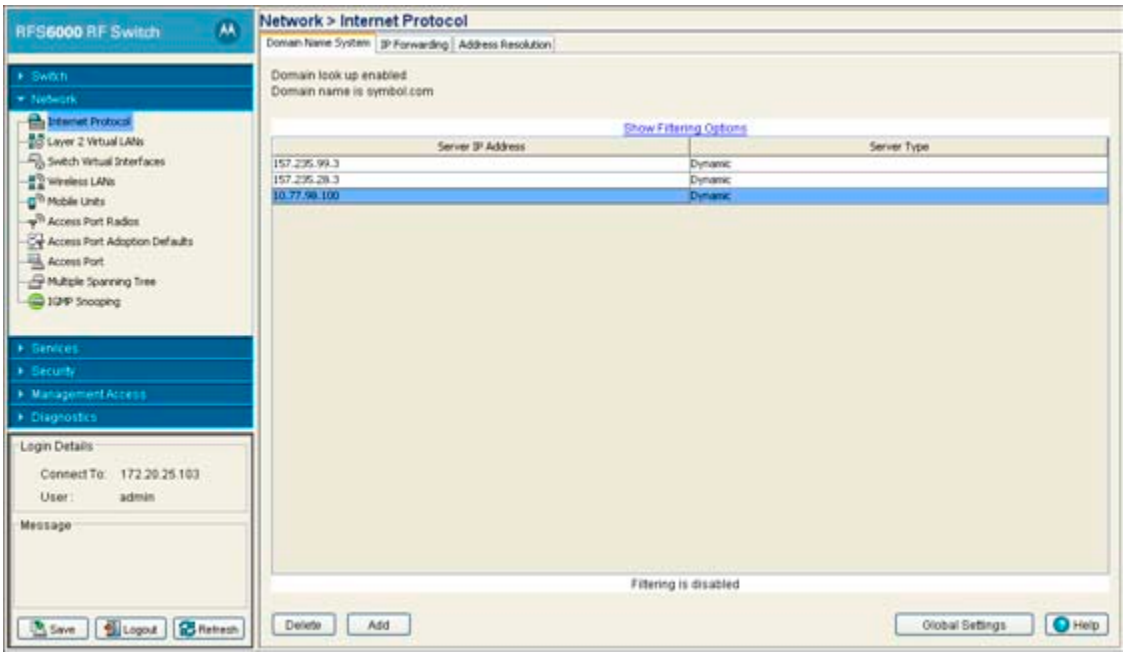
- *Configuring DNS*
- *Configuring IP Forwarding*
- *Viewing Address Resolution*

4.2.1 Configuring DNS

Use the **Domain Name System** tab to view Server address information and delete or add severs to the list of servers available. To configure DNS:

1. Select **Network** > **Internet Protocol** from the main tree menu.
2. Select the **Domain Network System** tab (displayed by default).

   Use the **Show Filtering Options** link to view the details displayed in the table.



3. The **Domain Name System** tab displays DNS details in a tabular format.

Server IP Address	Displays the IP address of the domain name server(s) the system can use for resolving domain names to IP addresses. Domain look up order is determined by the order of the servers listed. The first server queried is the first server displayed. Therefore, ensure obsolete addresses are periodically removed.
Server Type	Displays whether the DNS IP address entry has been created statically (manually) or dynamically. The DHCP server provides the dynamic DNS IP address entry displayed. A static DNS IP address can be created by clicking the **Add** button.

4. Select an IP Address from the table and click the **Delete** button to remove the selected entry from the list.

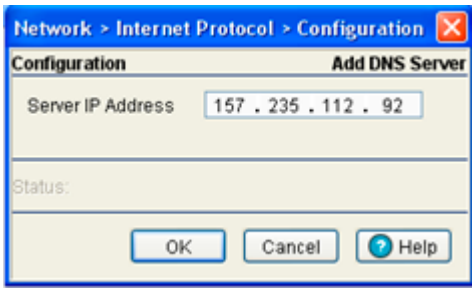
5. Click the **Add** button to display a screen used to add another domain name server. For more information, see *Adding an IP Address for a DNS Server on page 4-5*.
6. Click the **Global Settings** button to open a screen that allows the domain lookup to be enabled/disabled and the domain name to be specified. For more information, see *Configuring Global Settings on page 4-5*.

4.2.1.1 Adding an IP Address for a DNS Server

Add an IP address for a new domain server using the **Add** screen.

1. Click the **Add** button within the Domain Network System screen.

   The new **Configuration** screen displays enabling you to add IP address for the DNS Server.

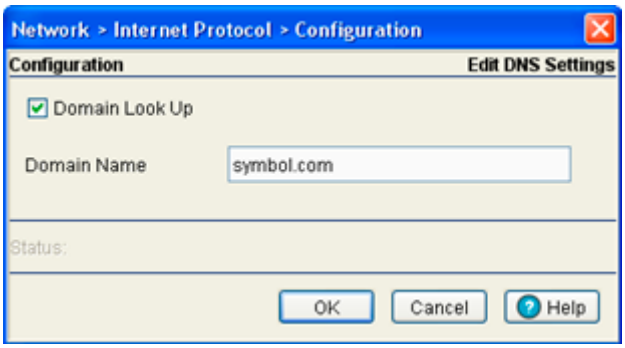


2. Enter the **Server IP Address** to define the IP address of the new static domain name server.
3. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
4. Click **OK** to use the changes to the running configuration and close the dialog.
5. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.2.1.2 Configuring Global Settings

Use the **Global Settings** screen to query domain name servers to resolve domain names to IP addresses. Use this screen to enable/disable the **Domain look up**, which allows you to use commands like ping, traceroute etc. using hostnames rather than IP addresses.

1. Click the **Global Settings** button in the main Domain Network System screen.



   A **Configuration** screen displays for editing the DNS settings of the server.

2. Select the **Domain Look Up** checkbox to enable the switch to query domain name servers to resolve domain names to IP addresses.

NOTE: The order of look up is determined by the order of the servers within **Domain Name System** tab. The first server queried is the first server displayed.

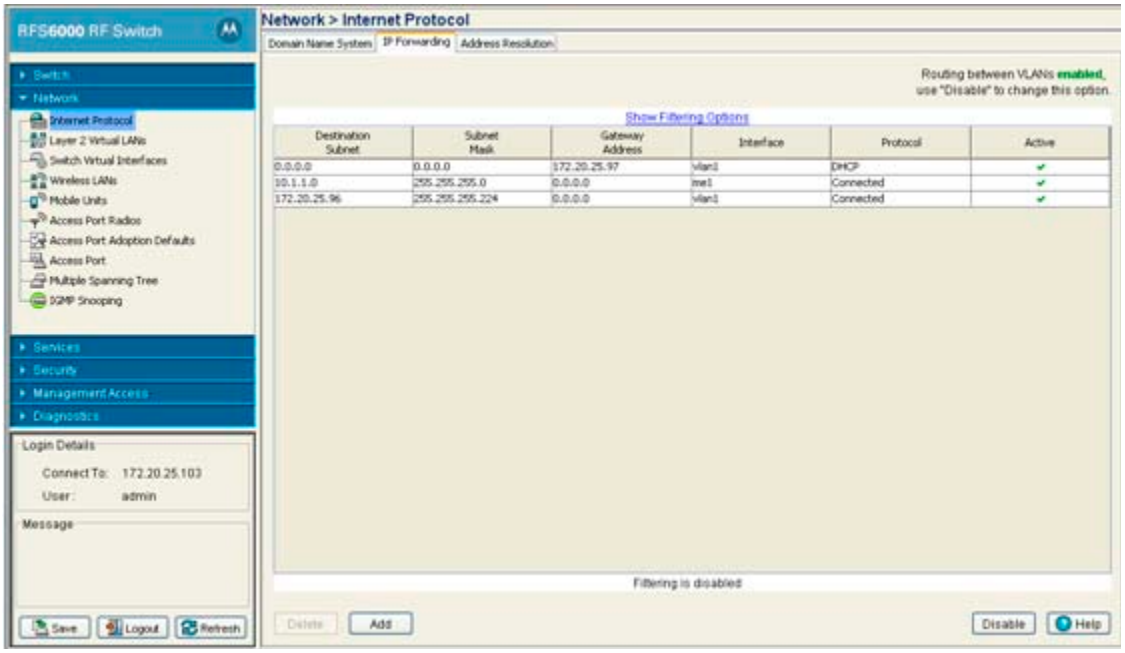
3. Enter a **Domain Name** in the text field. This is the switch's domain.
4. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click **OK** to use the changes to the running configuration and close the dialog.
6. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.2.2 Configuring IP Forwarding

The IP Forwarding table lists all the routing entries to route the packets to a specific destination. To view the IP forwarding configuration:

1. Select **Network** > **Internet Protocol** from the main tree menu.
2. Select the **IP Forwarding** tab.

   Use the Filtering Option to view the details displayed in the table.



3. The read-only **IP Forwarding** tab displays the current status between VLANs. To toggle the status of routing between VLANs, use the **Enable/Disable** options located at the bottom of the screen.

   The following details display in the table:

Destination Subnet	Displays the mask used for destination subnet entries. The Subnet Mask is the IP mask used to divide internet addresses into blocks (known as subnets). A value of 255.255.255.0 will support 256 IP addresses.
Subnet Mask	Displays the mask used for destination subnet entries. The Subnet Mask is the IP mask used to divide internet addresses into blocks (known as subnets). A value of 255.255.255.0 will support 256 IP addresses.
Gateway Address	Displays the IP address of the Gateway used to route the packets to the specified destination subnet. Do not set the gateway address to any VLAN interface used by the switch.
Interface	Displays the interface name with which the destination subnet entries are attached.
Protocol	Displays the name of the routing protocol with which this route was obtained. Possible values are: • *Static* — Routes are statically added by the operator. • *DHCP* — Routes obtained from the DHCP server. • *Connected* — Routes automatically installed by the switch for directly connected networks based on interface IP addresses. • *Kernel/ ICMP* — Routes added as a result of receiving an ICMP redirect from an intermediate router.
Active	When IP Forwarding is enabled for the selected subnet, a green check displays in the Active column. A red X defines the subnet as disabled.

4. Select an entry and click the **Delete** button to remove the selected entry from the IP forwarding table.
5. Click the **Add** button to create a new static route. For more information, see *Adding a New Static Route on page 4-7*.
6. Click **Enable** (to allow) or **Disable** (to deny) routing between VLANs.

4.2.2.1 Adding a New Static Route

Use the **Add** screen to add a new destination subnet, subnet mask and gateway for routing packets to a defined destination. Use the screen when an existing destination subnet does not meet the needs of the network.

To add a new static route:

1. Click the **Add** button.

   A new **Configuration** screen displays enabling you to add a new destination subnet, subnet mask and gateway for routing packets to a defined destination.

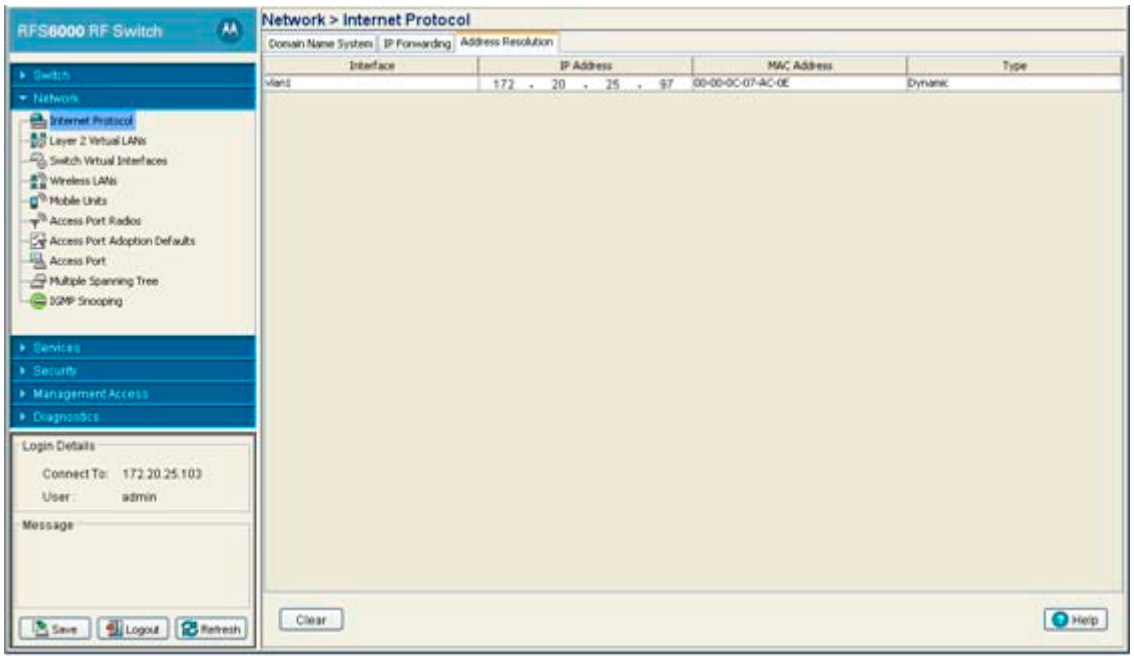
2. In the **Destination Subnet** field, enter an IP address to route packets to a specific destination address.
3. Enter a subnet mask for the destination subnet in the **Subnet Mask** field.

   The Subnet Mask is the IP mask used to divide internet addresses into blocks known as subnets. A value of 255.255.255.0 support 256 IP addresses.
4. In the **Gateway Address** field, enter the IP address of the gateway used to route the packets to the specified destination subnet. Do not set the gateway address to any VLAN interface used by the switch.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.2.3 Viewing Address Resolution

The **Address Resolution** table displays the mapping of layer three (IP) addresses to layer two (MAC) addresses. To view address resolution details:

1. Select **Network** > **Internet Protocol** from the main tree menu.
2. Select the **Address Resolution** tab.



3. Refer to the **Address Resolution** table for the following information:

Interface	Displays the name of the actual interface where the IP address was found (typically a VLAN).
IP Address	Displays the IP address being resolved.
MAC Address	Displays the MAC address corresponding to the IP address being resolved.
Type	Defines whether the entry was added statically or created dynamically in respect to network traffic. Entries are typically static.

4. Click the **Clear** button to remove the selected AP entry if no longer usable.

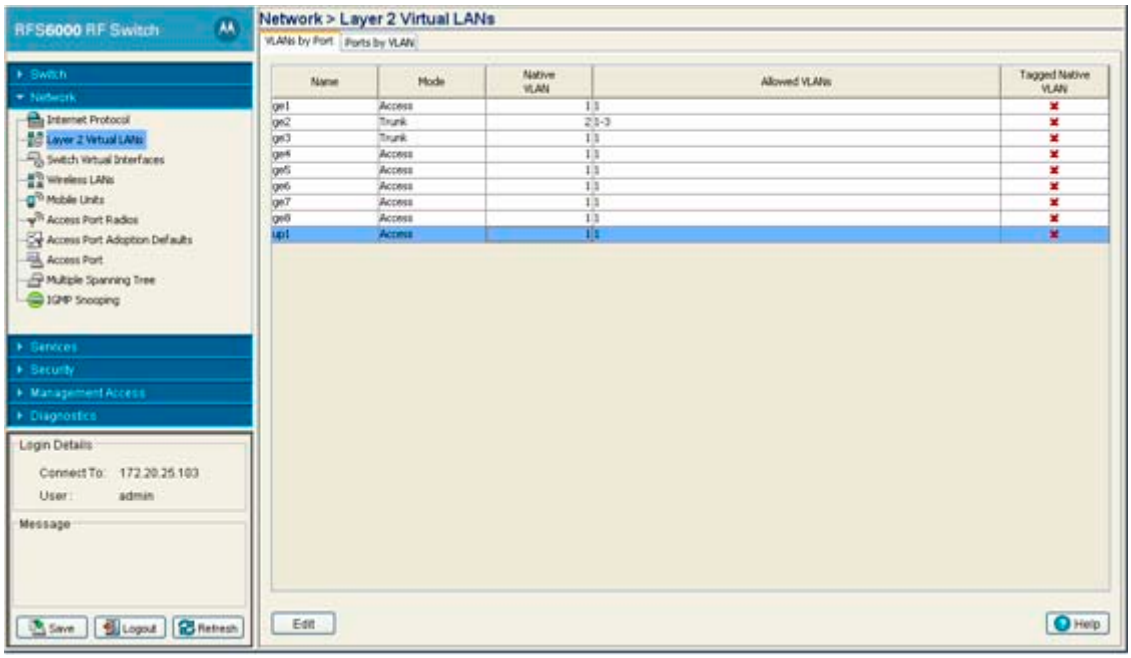
4.3 Viewing and Configuring Layer 2 Virtual LANs

A virtual LAN (VLAN) is similar to a Local Area Network (LAN), however devices do not need to be connected to the same segment physically. Devices operate as if connected to the same LAN, but could be connected at different physical connections across the LAN segment. The VLAN can be connected at various physical points but react as if it were connected directly. One of the biggest advantages of a VLAN, is when a computer is physically moved to another location, it can stay on the same VLAN without reconfiguration. The switch can support multiple VLANs. Use the Layer 2 Virtual LANs screen to view and configure VLANs by Port and Ports by VLAN information. Refer to the following VLAN configuration activities:

- *Viewing and Configuring VLANs by Port*
- *Viewing and Configuring Ports by VLAN*

4.3.1 Viewing and Configuring VLANs by Port

1. Select **Network** > **Layer 2 Virtual LANs** from the main menu tree. **VLAN by Port** details display within the Virtual LANs screen.



2. Refer to following details within the table:

Name	Displays the name of the VLAN to which the switch is currently connected.
Mode	It can be either Access or Trunk. • *Access*– This ethernet interface accepts packets only form the native VLANs. • *Trunk*– The Ethernet interface allows packets from the given list of VLANs you add to the trunk.
Native VLAN	Displays the tag assigned to the native VLAN.

Allowed VLANs	Displays VLAN tags allowed on this interface
Native VLAN Tagged	Displays if the Native VLAN for each port is tagged or not. The column displays a green check mark if the Native VLAN is tagged. If the Native VLAN is not tagged the column will display a red "x". A Native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode.

SWITCH NOTE: For Adaptive AP to work properly with RFS7000 you need to have independent and extended WLANs mapped to a different VLAN than the ge port.

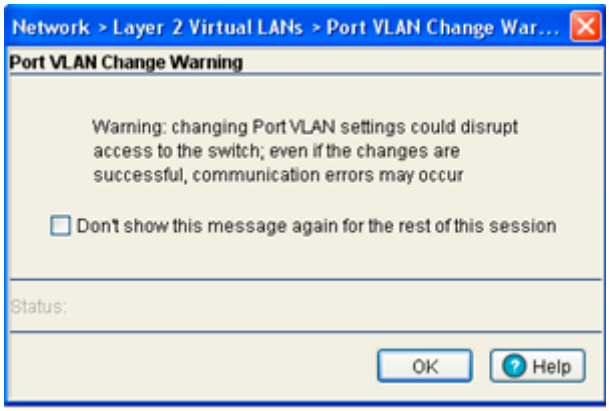
3. Select a record from the table and click the **Edit** button to modify the record. For more information, see *Editing the Details of an Existing VLAN by Port on page 4-11*.

4.3.2 Editing the Details of an Existing VLAN by Port

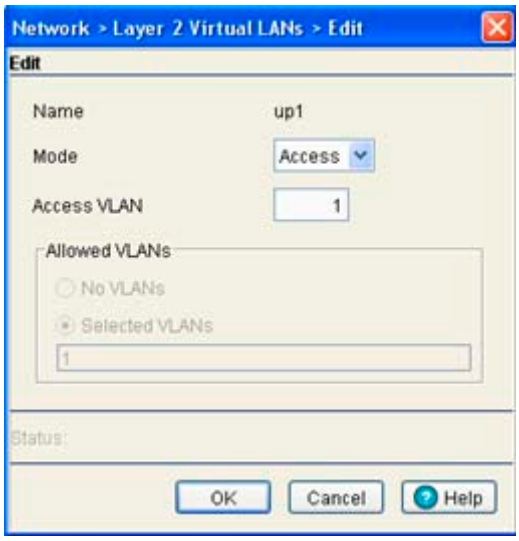
To revise the configuration of an existing VLAN:

1. Select **Network** > **Virtual LANs** from the main menu tree.
2. Select an Ethernet for which you want to configure the VLAN and click on the **Edit** button.

   The system prompts you with a **Port VLAN Change Warning** message stating communication disruptions could occur with the switch.
3. Click **OK** to continue.



4. Use the **Edit** screen to modify the VLAN's mode, access VLAN and allowed VLAN designation.



5. Use the **Edit** screen to modify the following:

Name	Displays a read only field and with the name of the Ethernet to which the VLAN is associated.
Mode	Use the drop-down menu to select the mode. It can be either: • *Access* – This Ethernet interface accepts packets only form the native VLANs. If this mode is selected, the Allowed VLANs field is unavailable. • *Trunk*–The Ethernet interface allows packets from the given list of VLANs you can add to the trunk.
Native VLAN	Use this field to change the tag assigned to the native VLAN.
Allowed VLANs	This section has the following 2 options (and is only available when Trunk is selected from the Mode drop-down menu): • *No VLANs*– Select this option if you do not wish to add any additional VLANs. • *Selected VLANs*– Select this option if you wish to add additional VLANs.

6. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to use the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

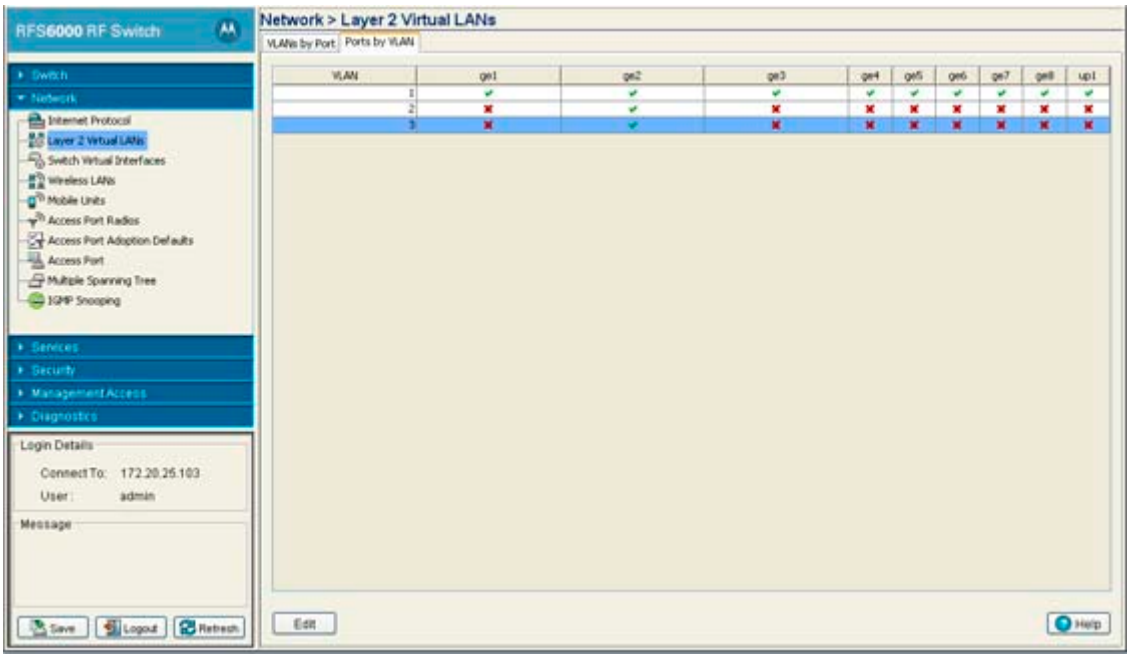
4.3.3 Viewing and Configuring Ports by VLAN

A *Virtual Local Area Network* (VLAN) is a switched network segmented by function or application rather than a traditional LAN segmentation (based on physical location). VLANs allow a greater level of flexibility and enable changes to the network infrastructure without physically disconnecting network equipment.

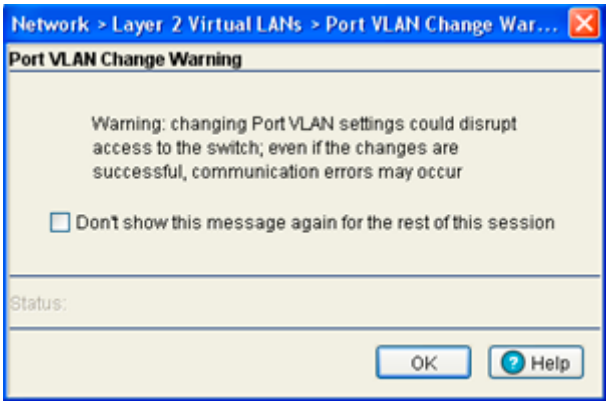
To view VLAN by Port information:

1. Select **Network** > **Layer 2 Virtual LANs** from the main menu tree.
2. Select the **Ports by VLAN** tab.

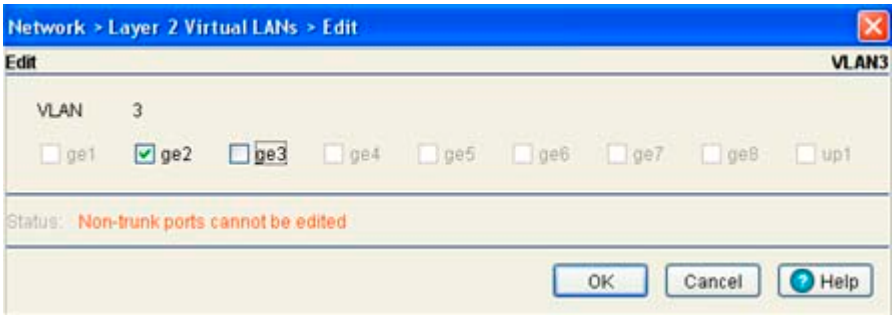
   VLAN details display within the VLANs by Port tab.



3. Highlight an existing VLAN and click the **Edit** button. The system displays a Port VLAN Change Warning message. Be advised, changing VLAN designations could disrupt access to the switch.



4. Click **OK** to continue. A new window displays wherein the VLAN assignments can be modified for the selected VLAN.



SWITCH NOTE: The ports available vary by switch.
On the RFS6000, the available ports are ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8 and up1.
On the RFS7000, the available ports are ge1, ge2, ge3 and ge4.

5. Change VLAN port designations as required.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.4 Configuring Switch Virtual Interfaces

A *switch virtual interface* (SVI) is required for layer 3 (IP) access to the switch or provide layer 3 service on a VLAN. The SVI defines which IP address is associated with each VLAN ID the switch is connected to. A SVI is created for the default VLAN (VLAN 1) to enable remote switch administration. A SVI is also used to map a VLANs to IP address ranges. This mapping determines the destination networks for switch routing.

Each IP address range (IP Address and Subnet Mask) can be mapped to one (and only one) VLAN ID. A VLAN ID does not require an IP address be defined on the switch. Each VLAN ID must be mapped to a physical port using the Layer 2 Virtual LANs configuration to communicate with the rest of the network.

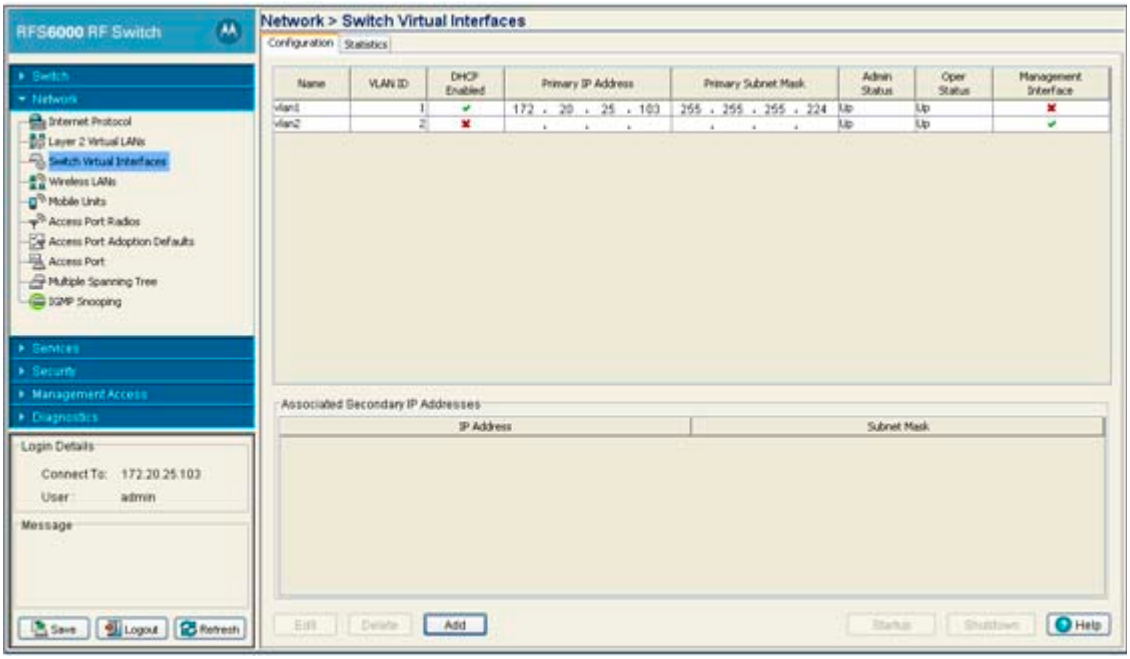
Use the **Switch Virtual Interfaces** screen to view and configure VLAN interfaces. This screen contains two tabs supporting the following activities:

- *Configuring the Virtual Interface*
- *Viewing Virtual Interface Statistics*

4.4.1 Configuring the Virtual Interface

Use the **Configuration** screen to view and configure the virtual interface details.

1. Select **Network** > **Switch Virtual Interface** from the main tree menu.
2. Select the **Configuration** tab.



The following configuration details display in the table:

Name	Displays the name of the virtual interface.
VLAN ID	Displays the VLAN ID associated with the interface.
DHCP Enabled	Displays whether the DHCP client is enabled or not. A green check mark defines the DHCP client as enabled for the interface. A red X means the interface is disabled.
Primary IP Address	Displays the IP address for the virtual interface.
Primary Subnet Mask	Displays the subnet mask assigned for this interface.
Admin Status	Displays whether the virtual interface is operational and available to the switch.
Oper Status	Displays whether the selected Switch Virtual Interface is currently (Up) or not (Down) on the switch.
Management Interface	A green checkmark within this column defines this VLAN as currently used by the switch. This designates the interface settings used for global switch settings in case of conflicts. For example, if multiple SVIs are configured with DHCP enabled on each, the switch could have multiple domain names assigned from different DHCP servers.The one assigned over the selected Management Interface would be the only one used by the switch. This setting does not affect any of the Management Access Interfaces configured using *Configuring Access Control on page 7-2*.

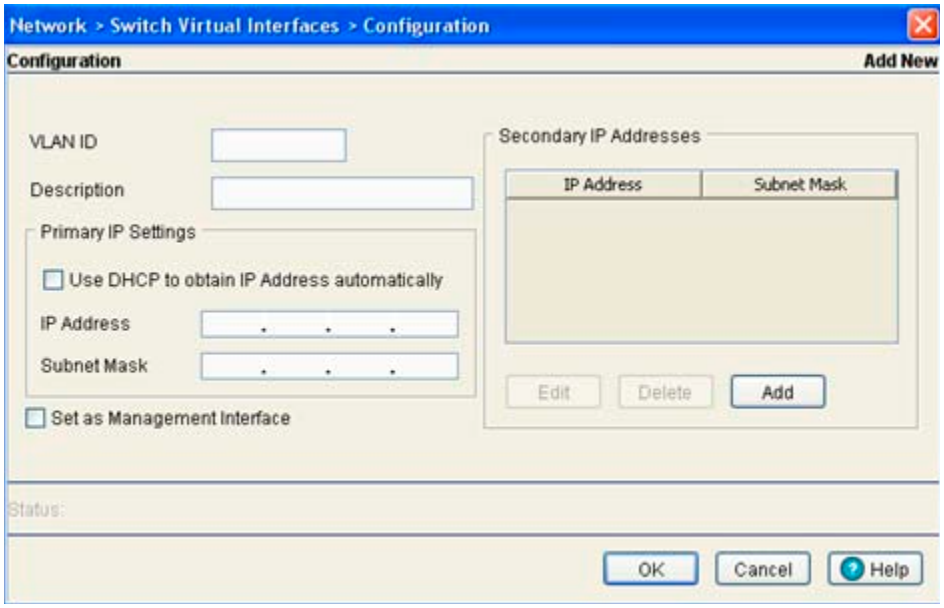
3. Select a record from the table and click the **Edit** button to modify the record. For more information, see *Modifying a Virtual Interface on page 4-17*.
4. Select a record from the table and click the **Delete** button to remove the configuration from the list of switch virtual interfaces.

5. Click the **Add** button to add a new configuration to the switch virtual interface. For more information, see *Adding a Virtual Interface on page 4-16*.
6. Select an interface as click the **Startup** button to invoke the selected interface the next time the switch is booted.
7. Select an interface as click the **Shutdown** button to disable the selected interface.

4.4.1.1 Adding a Virtual Interface

To add a new switch virtual interface:

1. Select **Network** > **Switch Virtual Interface from** the main tree menu.
2. Select the **Configuration** tab.
3. Click on the **Add** button.



4. Enter the **VLAN ID** for the switch virtual interface.
5. Provide a **Description** for the VLAN, representative of the VLAN's intended operation within the switch managed network.
6. The **Primary IP Settings** field consists of the following:
   a. Select **Use DHCP to obtain IP Address automatically** to allow DHCP to provide the IP address for the virtual interface. Selecting this option disables the IP address field.
   b. Enter the **IP Address** for the VLAN associated virtual interface.
   c. Enter the **Subnet Mask** for the IP address.
7. Select the **Set as Management Interface** checkbox to enable any host displayed in this VLAN to configure the switch.
8. Use the **Secondary IP Addresses** field 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.

   Select the **Add** button (within the Secondary IP Addresses field) to define additional addresses from a sub screen. Choose an existing secondary address and select **Edit** or **Delete** to revise or remove a secondary address.

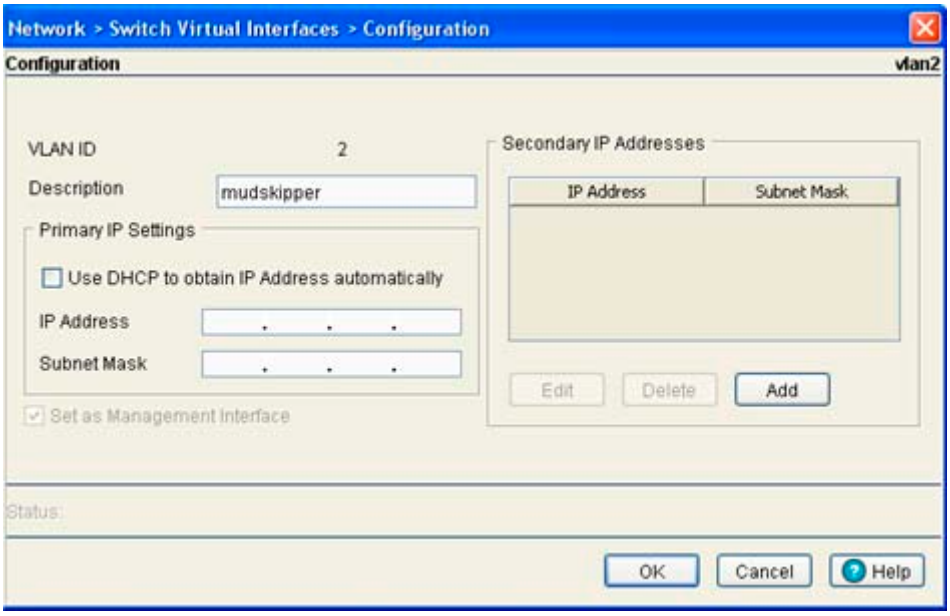
9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.4.1.2 Modifying a Virtual Interface

To modify an existing virtual interface.

CAUTION: When changing from a default DHCP address to a fixed IP address, set a static route first. This is critical when the switch is being accessed from a subnet not directly connected to the switch and the default route was set from DHCP.

1. Select **Network** > **Switch Virtual Interface** from the main tree menu.
2. Select the **Configuration** tab and click the **Edit** button.



The screen displays with the name of the VLAN in the upper left-hand side. The VLAN ID cannot be modified and should be used to associate the VLAN ID with the description and IP address assignments defined.

3. If necessary, modify the **Description** of the VLAN, to make it representative of the VLAN's intended operation within the switch managed network.
4. Unselect the **Use DHCP to obtain IP Address automatically** checkbox to assign IP addresses manually and you do not want DHCP to provide them.
5. Use the **Primary IP Address** field to manually enter the IP address for the virtual interface.
6. Enter the **Subnet Mask** for the IP address.
7. Select the **Set as Management Interface** checkbox to convert the selected VLAN ID to a management interface.

8. Use the **Secondary IP Addresses** field to define/modify additional IP addresses to associate with VLAN IDs. The addresses provided will be used if the primary IP address is unreachable.

   Select the **Add** button (within the Secondary IP Addresses field) to define/modify additional addresses from a sub screen. Select an existing secondary address and select **Edit** or **Delete** to revise or remove a secondary address as needed.

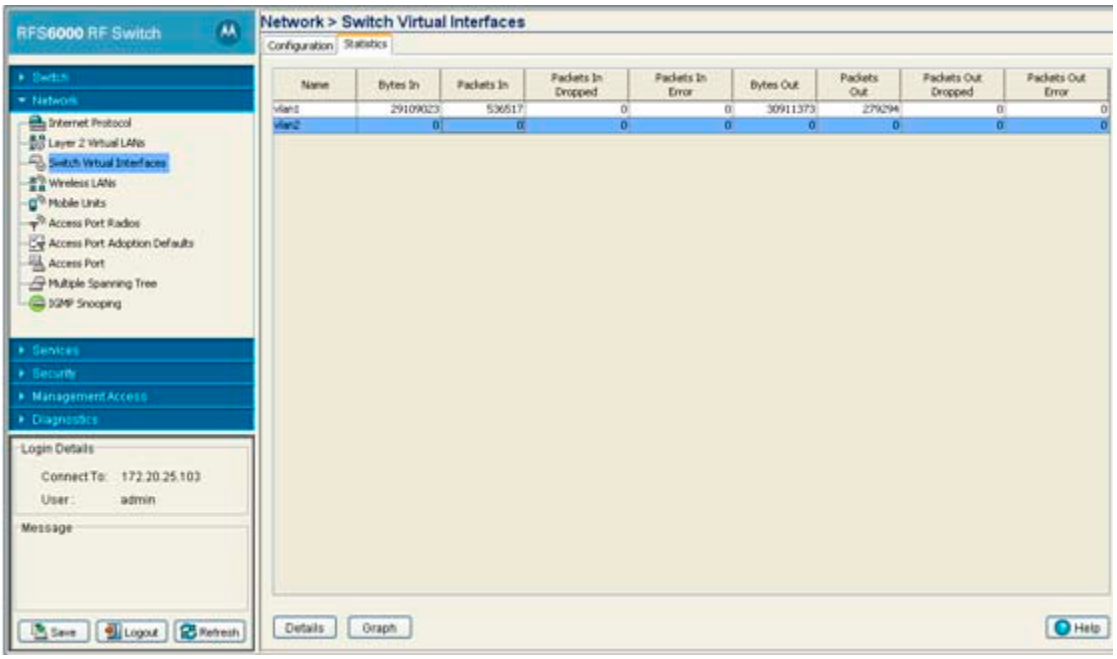
9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.4.2 Viewing Virtual Interface Statistics

The **Statistics** screen displays information about packet level statistics and errors at the interface.

To view virtual interface statistics:

1. Select **Network** > **Switch Virtual Interface** from the main tree menu.
2. Select the **Statistics** tab.



Refer to the following to assess the network throughput of existing virtual interfaces:

Name	Displays the user defined interface name. The corresponding statistics are displayed along the row. The statistics are the total traffic to the interface since its creation.
Bytes In	Displays the number of bytes coming into the interface. The status is not self-updated. To view the current status, click the **Details** button.
Packets In	Displays the number of packets coming into the interface (including packets dropped, error packets, etc.)

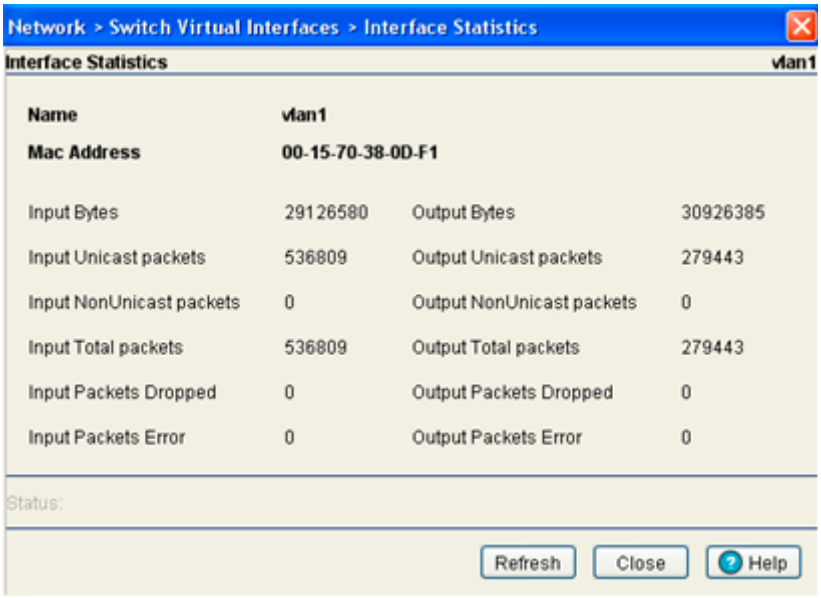
Packets In Dropped	Displays the number of dropped packets coming into the interface. Packets are dropped if: 1. The input queue for the hardware device/software module handling the interface definition is saturated/full. 2. Overruns occur when the interface receives packets faster than it can transfer them to a buffer.
Packets In Error	Displays the number of error packets coming into the interface. • *Runt frames* — Packets shorter than the minimum Ethernet frame length (64 bytes). • *CRC errors* — The *Cyclical Redundancy Check* (CRC) is the 4 byte field at the end of every frame the receiving station uses 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 CRC error. • *Late collisions* — A late collision is any collision that occurs after the first 64 octets of data have been sent by the sending station. Late collisions are not normal and are usually the result of out of specification cabling or a malfunctioning device. • *Misaligned frames* — A misaligned frame is a frame that somehow gets out of sync with the receiving station's receive clock recovery circuit. Misalignment is reported if the frame ends with a CRC error and extra bits are also detected.
Bytes Out	Displays the number of bytes going out on the interface.
Packets Out	Displays the number of packets going out on the interface.
Packets Out Dropped	Displays the number of dropped packets going out of the interface, due to saturated output queues assigned to the interface processor or the physical device/software module. Packets can be dropped due to collisions as well.
Packets Out Error	Displays the number of error packets going out of the interface, including frame forming errors or malformed packets transmitted over the interface.

3. Click the **Details** button to view packet level statistics of any user defined interface. For more information, see *Viewing Virtual Interface Statistics on page 4-19*.
4. Click the **Graph** button to view a graphical representation of the switch virtual interface statistics. For more information, see *Viewing the Virtual Interface Statistics Graph on page 4-21*.

4.4.2.1 Viewing Virtual Interface Statistics

To view detailed virtual interface statistics:

1. Select a virtual interface from the **Statistics** tab
2. Click the **Details** button.



3. The **Interface Statistics** screen displays with the following content:

Name	Displays the title of the logical interface selected.
MAC Address	Displays physical address information associated with the interface. This address is read-only (hard-coded at the factory) and cannot be modified.
Input Bytes	Displays the number of bytes received by the interface.
Input Unicast Packets	Displays the number of unicast packets (packets directed towards the interface) received at the interface.
Input NonUnicast Packets	Displays the number of NonUnicast Packets (Multicast and Broadcast Packets) received at the interface.
Input Total Packets	Displays the total number of packets received at the interface.
Input Packets Dropped	Displays the number of packets dropped at the interface by the input Queue of the hardware unit /software module associated with the VLAN interface. Packets are dropped when the input Queue of the interface is full or unable to handle incoming traffic.
Input Packets Error	Displays the number of packets with errors at the interface. Input Packet Errors are input errors occurring due to; no buffer space/ignored packets due to broadcast storms, packets larger than maximum packet size, framing errors, input rate exceeding the receiver's date handling rate or cyclic redundancy check errors. In all these cases, an error is reported.
Output Bytes	Displays the number of bytes transmitted from the interface.
Output Unicast Packets	Displays the number of unicast packets (packets directed towards a single destination address) transmitted from the interface.
Output NonUnicast Packets	Displays the number of unicast packets transmitted from the interface.
Output Total Packets	Displays the total number of packets transmitted from the interface.

Output Packets Dropped	Displays the number of transmitted packets dropped at the interface. Output Packets Dropped are packets dropped when the output queue of the physical device associated with interface is saturated.
Output Packets Error	Displays the number of transmitted packets with errors. Output Packet Errors are the sum of all the output packet errors, malformed packets and misaligned packets received on an interface.

4. The **Status** is the current state of requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click the **Refresh** button to refresh the virtual interface statistics. Status information is not polled to the applet. Hence you have to refresh the switch to retrieve the data.
6. Click the **Close** button to exit the screen. Clicking Close does not lose any data, as there are no values configured within this screen (it is read-only).

4.4.2.2 Viewing the Virtual Interface Statistics Graph

The switch Web UI continuously updates its virtual interface statistics, even when the graph is closed. Periodically display the virtual statistics graph for the latest information as network performance information is required.

To view detailed graphical statistics for a selected interface:

1. Select a record from the table displayed in the **Statistics** screen.
2. Click the **Graph** button.
3. The Interface Statistics screen displays. The Interface Statistics screen provides the option of viewing graphical statistics for the following parameters:
   - *Input Bytes*
   - *Input Pkts Dropped*
   - *Output Pkts Total*
   - *Output Pkts Error*
   - *Input Pkts Total*
   - *Input Pkts Error*
   - *Output Pkts NUCast*
   - *Input Pkts NUCast*
   - *Output Bytes*
   - *Output Pkts Dropped*

   Select any of the above parameters by clicking on the checkbox associated with it.

NOTE: Only four parameters may be selected at any given time.

4. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click **Close** to close the dialog.

4.5 Viewing and Configuring Switch WLANs

A *wireless LAN* (WLAN) is a *local area network* (LAN) without wires. WLANs transfer data through the air using radio frequencies instead of cables. The WLAN screen displays a high-level overview of the WLANs created for the switch managed network. Use this data as necessary to the WLANs that are active, their VLAN assignments, updates to a WLAN's description and their current authentication and encryption scheme.The Wireless LANs screen is partitioned into 5 tabs supporting the following configuration activities:

- *Configuring WLANs*
- *Viewing WLAN Statistics*
- *Configuring WMM*
- *Configuring the NAC Inclusion List*
- *Configuring the NAC Exclusion List*

4.5.1 Configuring WLANs

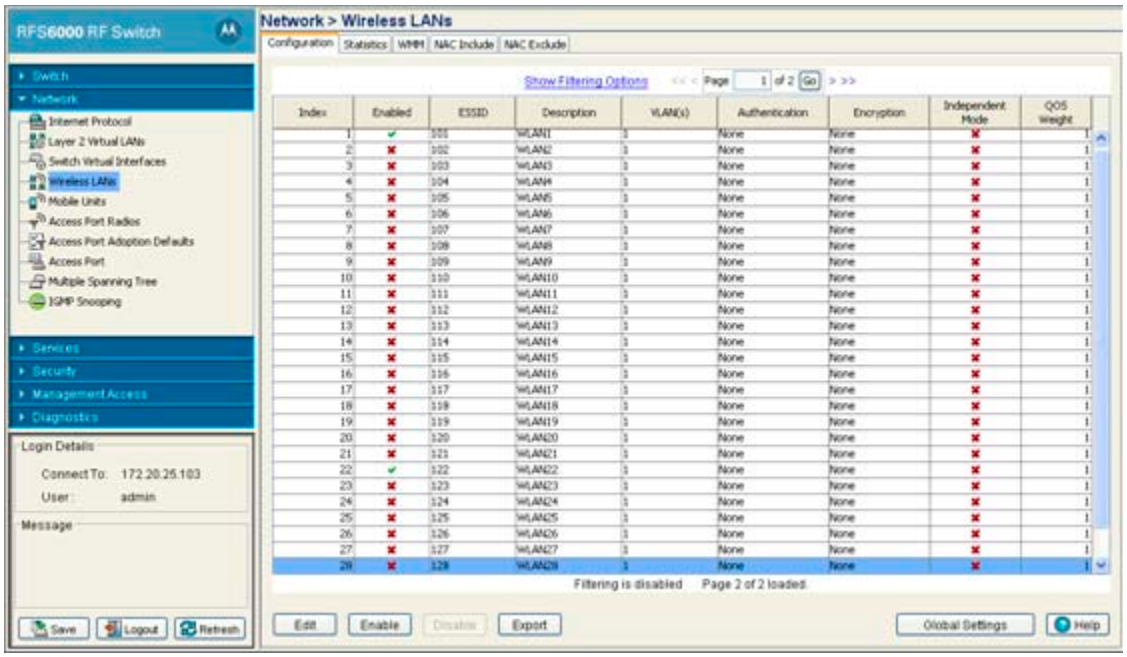
Refer to the **Configuration** screen for a high-level overview of the WLANs created for use within the switch-managed network. Use this data as necessary to keep current of active WLANs, their VLAN assignments,

updates to a WLAN's description and their current authentication and encryption schemes. Be careful to properly map BSS WLANs and security schemes.

SWITCH NOTE: The RFS6000 supports a maximum of 32 WLANs. The RFS7000 supports a maximum of 256 WLANS.

To configure a WLAN:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Click the **Configuration** tab.



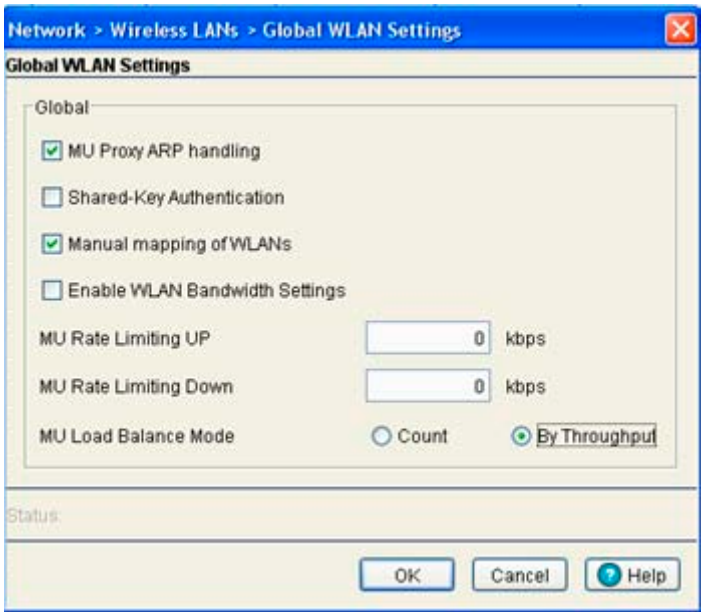
The Configuration tab displays the following details:

Index	Displays the WLAN's numerical identifier. The WLAN index range is from 1 to the maximum number of WLANs supported by the switch. An index can be helpful to differentiate a WLAN from other WLANs with similar configurations.
Enabled	Refer to the Enabled parameter to discern whether the specified WLAN is enabled or disabled. When enabled, a green check mark displays. When disabled, a red "X" displays. To enable or disable a WLAN, select it from the table and click the Enable or Disable button.
ESSID	Displays the Service Set ID associated with each WLAN. Click the Edit button to modify the value to a new unique SSID.
Description	Displays a short description of the associated WLAN. Click the Edit button to modify the value the WLAN description.
VLAN(s)	Displays the name of the VLAN ID(s) of the VLAN(s) this WLAN is mapped to. The VLAN ID can be between 1 and 4094. The default mapping is to a single VLAN with VLAN ID 1.

Authentication	Displays the type of authentication used with the specified WLAN. Click the **Edit** button to modify the WLAN's current authentication scheme. For information on configuring an authentication scheme for a WLAN, see *Configuring Authentication Types on page 4-33*.
Encryption	Displays the type of wireless encryption used on the specified WLAN. When no encryption is used, the field displays *none*. Click the **Edit** button to modify the WLAN's current encryption scheme. For information on configuring an authentication scheme for a WLAN, see *Configuring Different Encryption Types on page 4-55*.
Independent Mode	Determines whether the WLAN is functioning as an independent or extended WLAN in regards its support of *adaptive AP* (AAP) operation. Independent WLANs (defined by a green checkmark) are local to an AAP and configured from the switch. Specify a WLAN as independent for no traffic to be forward to the switch. Independent WLANs behave like WLANs as used on a a standalone Access Point. Extended WLAN (defined by the default red X) are typical centralized WLANs created on the switch. Select an existing WLAN to revise its default extended mode designation if intending to use the WLAN for AAP support. For more information, see *Editing the WLAN Configuration on page 4-26*.
QOS Weight	Defines the Quality of Service weight for the WLAN. WLAN QoS will be applied based on the QoS weight value with higher values representing higher priority. The range for QoS. weight values is between 1 and 10 with 1 being the default value.

3. Click the **Edit** button to display a screen where WLAN information, encryption and authentication settings can be viewed or changed.
4. Click the **Enable** button to enable the selected WLAN. When enabled, a green check mark displays. When disabled, a red "X" displays. Enabled WLANs are display in a number of different switch Web UI configurations for additional configuration activities. To enable or disable a WLAN, select it from the table and click the Enable or Disable button. The Enable button is only available when the selected WLAN is disabled.
5. Click the **Disable** button to disable the selected WLAN. When enabled, a green check mark displays. When disabled, a red "X" displays. To enable or disable a WLAN, select it from the table and click the Enable or Disable button. The Disable button is only available when the selected WLAN is enabled.
6. When using clustering and the **Cluster GUI** feature is enabled a drop-down menu will be available to select which cluster members' WLANs are displayed. To view WLANs from all cluster members, select **All** from the drop-down menu. To view WLANs from a specific cluster member, select that member's IP address from the drop-down menu.
7. Click the **Global Settings** button to display a screen with WLAN settings applying to the all the WLANs on the system. Remember, changes made to any one value impact each WLAN.

   Click **OK** to save updates to the Global WLAN Settings screen. Click **Cancel** to disregard changes and revert back to the previous screen. Checkbox options within the Global Settings screen include:



MU Proxy ARP handling — Enables Proxy ARP handling for MUs. Proxy ARP is provided for MU's in PSP mode whose IP address is known. The WLAN generates an ARP reply on behalf of a MU, if the MU's IP address is known. The ARP reply contains the MAC address of the MU (not the MAC address of WLAN Module). Thus, the MU does not awaken to send ARP replies (helping to increase battery life and conserve bandwidth). If an MU goes into PSP mode without transmitting at least one packet, its Proxy ARP will not work for the MU. This option is selected by default.

Shared-Key Authentication — Enables Shared-Key Authentication for all enabled WLANs on the system. Shared-key authentication is strongly discouraged. This option is enabled in setups where there are legacy mobile units which can only support this authentication method.

Manual mapping of WLANs — Use this option (its selected by default) for custom WLAN to Radio mappings. When Advanced Configuration is disabled, the user cannot conduct Radio – WLAN mapping. Additionally, the user cannot enable WLANs with an index higher than 16. Once the Advanced Configuration option is enabled, the following conditions must be satisfied (to successfully disable it). No WLANs with an index higher than 16 should be enabled. With advanced WLAN mapping the switch evenly distributes the enabled WLANs to BSSIDs. Additionally, the Radio – WLAN mapping should conform to the following:

BSS ID 1 – Possible WLANs 1,5,9,13

BSS ID 2 – Possible WLANs 2,6,10,14

BSS ID 3 – Possible WLANs 3,7,11,15

BSS ID 4 – Possible WLANs 4, 8, 12,16

Enable WLAN Bandwidth Settings — Select this option to enable WLAN bandwidth settings. WLAN bandwidth settings ensures quality of service for applications regardless of network load. This option is selected by default.

MU Rate Limiting UP — Enter an upstream rate limit in kbps for all MUs associated with the switch across all WLANs.

MU Rate Limiting Down	Enter an downstream rate limit in kbps for all MUs associated with the switch across all WLANs.
MU Load Balance Mode	Configure a method for distributing traffic across MUs using the MU Load Balancing Mode. Select Count to set load balancing based on number of MUs. Select By Throughput to set load balancing based on total throughput of MUs.

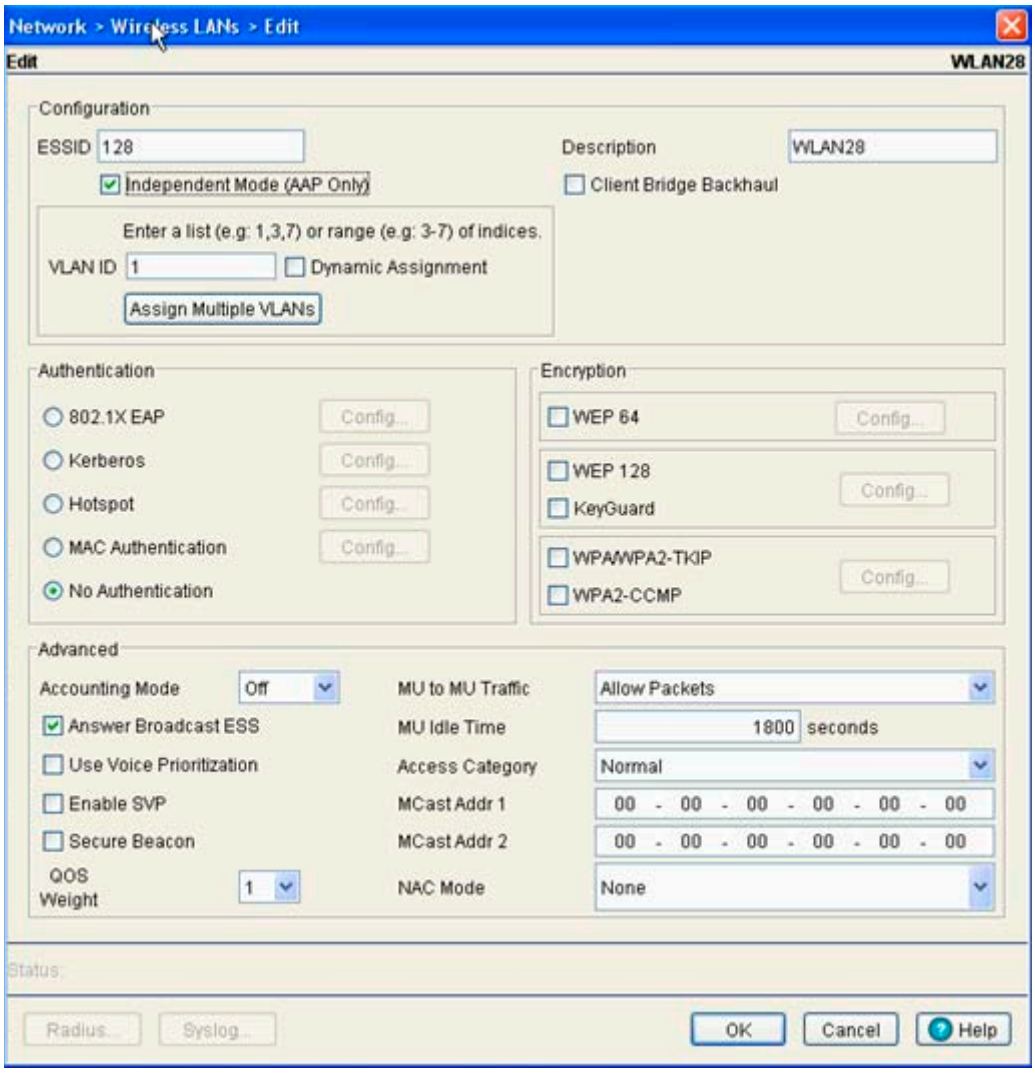
4.5.1.1 Editing the WLAN Configuration

Security measures for the switch and its WLANs are critical. Use the available switch security options to protect each WLAN from wireless vulnerabilities, and secure the transmission of RF packets between WLANs and the MU traffic they support.

The user has the capability of configuring separate security policies for each WLAN. Each security policy can be configured based on the authentication (Kerberos, 802.1x EAP, Hotspot) and /or encryption (WEP, KeyGuard, WPA/WPA2-TKIP or WPA2/CCMP) scheme.

All of the default WLANs are available for modification when the user accesses the Wireless LANs screen. However, the WLAN requires an authentication or encryption scheme be applied before it can begin securing the data traffic within the switch-managed wireless network. The Edit screen provides a mean of modifying the existing WLANs SSID, description, VLAN ID assignment, inter-WLAN communication definition and encryption and authentication scheme. To edit WLAN configuration settings:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Click the **Configuration** tab.
3. Select a WLAN to modify from the table.
4. Click the **Edit** button.



The Wireless LANs Edit screen is divided into the following user-configurable fields:

- *Configuration*
- *Authentication*
- *Encryption*
- *Advanced*

5. Refer to the **Configuration** field to define the following WLAN values

ESSID	Displays the *Extended Service Set ID* (ESSID) associated with each WLAN. If changing the ESSID, ensure the value used is unique.
Description	If editing an existing WLAN, ensure its description is updated accordingly to best describe the intended function of the WLAN.

Independent Mode (AAP Only)	Determines whether the WLAN is functioning as an independent or extended WLAN in regards its support of *adaptive AP* (AAP) operation. Select the checkbox to designate the WLAN as independent and prevent traffic from being forwarded to the switch. Independent WLANs behave like WLANs as used on a a standalone Access Point. Leave this option unselected (as is by default) to keep this WLAN an extended WLAN (a typical centralized WLAN created on the switch). For an overview of AAP and how it is configured and deployed using the switch and Access Point, see *Adaptive AP Overview*
Client Bridge Backhaul	When the Independent Mode (AAP Only) option is selected, this option becomes available for selection. Enable Client Bridge Backhaul to make the WLAN available to support mesh networking. Only WLANs defined for mesh networking support should have this checkbox selected.
VLAN ID	Assign the revised VLAN ID for this WLAN. Select the **Dynamic Assignment** checkbox for an user based VLAN assignment when 802.1x EAP Authentication is used.
Dynamic Assignment	With any authentication method that involves a Radius server, the Radius server may be configured to include a VLAN Id attribute in its "ACCESS Accept" response. This VLAN, instead of the configured VLAN(s) on this WLAN, will be assigned to the mobile unit. Enabling this check mark will enable switch to take VLAN ID from Radius response. When disabled, switch will ignore the VLAN ID from Radius response.
Assign Multiple VLANs	Click this button when it is desirable to assign multiple VLANs to this WLAN. For more information, see*Assigning Multiple VLANs per WLAN on page 4-31*.

NOTE: If the WLAN is to support AAP, the **Independent Mode (AAP Only)** checkbox must be selected. Additionally, the Access Point must have its auto discovery option enabled to be discovered by the switch. For information on configuring an Access Point for AAP support, see *Adaptive AP Configuration*.

NOTE: For a Radius supported VLAN to function, the **Dynamic Assignment** checkbox must be enabled for the WLAN supporting the VLAN.

NOTE: When configuring wireless settings for Adaptive APs all configuration must be done through the switch and not from the AP management console. Making changes directly in the AP management console can lead to unstable operation of the Adaptive AP.

6. Refer to the **Authentication** field to select amongst the following options:

802.1X EAP	A Radius server is used to authenticate users. For detailed information on configuring EAP for the WLAN, see *Configuring 802.1x EAP on page 4-33*.
Kerberos	A Kerberos server is used to authenticate users. For detailed information on configuring Kerberos for the WLAN, see *Configuring Kerberos on page 4-34*.
Hotspot	A Hotspot is used to authenticate users in a unique network segment (hotspot). The attributes of both the hotspot and the Radius Server are required. For more information, see *Configuring Hotspots on page 4-35*.
MAC Authentication	The switch uses a Radius server to see if a target MAC address is allowed on the network. The attributes of the Radius Server are required. For more information, see *Configuring MAC Authentication on page 4-48*
No Authentication	When selected, no Authentication is used and transmissions are made (in the open) without security unless an encryption scheme is used. This setting is not recommended when data protection is important.

7. Refer to the **Encryption** field to select amongst the following options:

WEP 64	Use the WEP 64 checkbox to enable the *Wired Equivalent Privacy* (WEP) protocol with a 40-bit key. WEP is available in two encryption modes: 40 bit (also called WEP 64) and 104 bit (also called WEP 128). The 104-bit encryption mode provides a longer algorithm that takes longer to decode than that of the 40-bit encryption mode. For detailed information on configuring WEP 64 for the WLAN, see *Configuring WEP 64 on page 4-56*.
WEP 128	Use the WEP 128 checkbox to enable the *Wired Equivalent Privacy* (WEP) protocol with a 104-bit key. WEP is available in two encryption modes: WEP 64 (using a 40-bit key) and WEP 128 (using a 104-bit key). WEP 128 encryption mode provides a longer algorithm that takes longer to decode than that of the WEP 64 encryption mode. For detailed information on configuring WEP 128 for the WLAN, see *Configuring WEP 128 / KeyGuard on page 4-57*.
KeyGuard	Uses a Motorola proprietary encryption mechanism to protect data. For detailed information on configuring KeyGuard for the WLAN, see *Configuring WEP 128 / KeyGuard on page 4-57*.
WPA-WPA2-TKIP	Use the WPA-TKIP checkbox to enable *Wi-Fi Protected Access* (WPA) with *Temporal Key Integrity Protocol* (TKIP). For detailed information on configuring TKIP for the WLAN, see *Configuring WPA/WPA2 using TKIP and CCMP on page 4-59*.
WPA2-CCMP	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. For detailed information on configuring CCMP for the WLAN, see *Configuring WPA/WPA2 using TKIP and CCMP on page 4-59*.

8. Refer to the **Advanced** field for the following information:

Accounting Mode	If using a Syslog server to conduct accounting for the switch, select the Syslog option from the **Accounting Mode** drop-down menu. Once selected, a **Syslog Config** button is enabled on the bottom of the Network > Wireless LANs > Edit screen. Use this sub screen to provide the Syslog Server IP address and port for the Syslog Server performing the accounting function. If either Hotspot, MAC Authentication or 802.1x EAP have been selected from within the Authentication field, a **Radius Config** button is enabled (on the bottom of the screen) allowing the user to define a Primary and Secondary Radius Accounting Server IP address, port, shared secret password and timeout and retry. Define these accounting settings as required for the switch. The default Accounting Mode setting is **Off**.
Answer Broadcast ESS	Select this checkbox to allow the WLAN to respond to probes for broadcast ESS.
Use Voice Prioritization	Select the Use Voice Prioritization option if Voice is used on the WLAN. This gives priority to voice packets and voice management packets and is supported only on certain legacy Motorola VOIP phones.
Enable SVP	Enabling SVP (*Spectralink Voice Prioritization*) allows the switch to identify and prioritize traffic from Spectralink/Polycomm phones.
Secure Beacon	Closed system is the secure beacon feature for not answering broadcast SSID. This option still allows MU to MU communication within the WLAN.
QoS Weight	Sets the Quality of Service weight for the WLAN. WLAN QoS will be applied based on the QoS weight value with the higher values given priority.The default value for the weight is 1.
MU to MU Traffic	Allows frames from one MU (where the destination MAC is of another MU) are switched to a second MU. Use the drop-down menu to select one of the following options: • *Drop Packets* – This restricts MU to MU communication based on the WLAN's configuration • *Allow Packets* – This allows MU to MU communication based on the WLAN's configuration
MU Idle Time	Set the MUs idle time limit in seconds. The default value is 1800 seconds.
Access Category	Displays the Access Category for the intended traffic. The Access Categories are the different WLAN-WMM options available to the radio. The Access Category types are: • *Automatic/WMM* – Optimized for WMM • *Voice* – Optimized for voice traffic. Voice packets receive priority. • *Video* – Optimized for video traffic. Video packets receive priority. • *Normal* – Optimized for normal traffic • *Low* – Optimized for background traffic
MCast Addr 1	The address provided takes packets (where the first 4 bytes match the first 4 bytes of the mask) and sends them immediately over the air instead of waiting for the DTIM period. Any multicast/broadcast that does not match this mask will go out only on DTIM Intervals.

MCast Addr 2	The second address also takes packets (where the first 4 bytes match the first 4 bytes of the mask) and sends them immediately over the air instead of waiting for the DTIM period. Any multicast/broadcast that does not match this mask will go out only on DTIM Intervals.
NAC Mode	Using *Network Access Control* (NAC), the switch only grants access to specific network resources. NAC restricts access to only compliant and validated devices (printers, phones, PDAs etc.), thereby limiting the risk of emerging security risks. NAC performs an authorization check for users and MUs without a NAC agent, and verifies a MU's compliance with the network security policy. The switch supports only the EAP/802.1x type of NAC. However, the switch can bypass NAC for MU's without NAC 802.1x support. For the implications of using the include and exclude with NAC, see *Configuring the NAC Inclusion List on page 4-71*, *Configuring the NAC Exclusion List on page 4-75* and *Configuring NAC Server Support on page 4-53*.

9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click on the **Radius...** button (when Radius is selected as the accounting mode) to configure an external primary and secondary Radius and NAC server. For more information, see *Configuring External Radius Server Support on page 4-49*.
11. Select the **Syslog** button (when Syslog is selected as the accounting mode) to view switch syslog accounting details. To enable syslog, select the **Syslog** option from the Accounting Mode drop-down menu. Use this sub screen to provide the Syslog Server IP address and port for the Syslog Server performing the accounting function.
12. If clustering and the **Cluster GUI** feature is enabled the **Apply to Cluster** feature will be available. Click the **Apply to Cluster** button to apply the WLAN settings to all members in the cluster.
13. Click **OK** to use the changes to the running configuration and close the dialog.
14. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.1.2 Assigning Multiple VLANs per WLAN

The switch allows the mapping of a WLAN to more than one VLAN. When a MU associates with a WLAN, it is assigned a VLAN in such a way that users are load balanced across VLANs. The VLAN is assigned from the pool representative of the WLAN. The switch tracks the number of MUs per VLAN, and assigns the least used/loaded VLAN to the MU. This number is tracked on a per-WLAN basis.

To assign multiple VLANs to a WLAN:

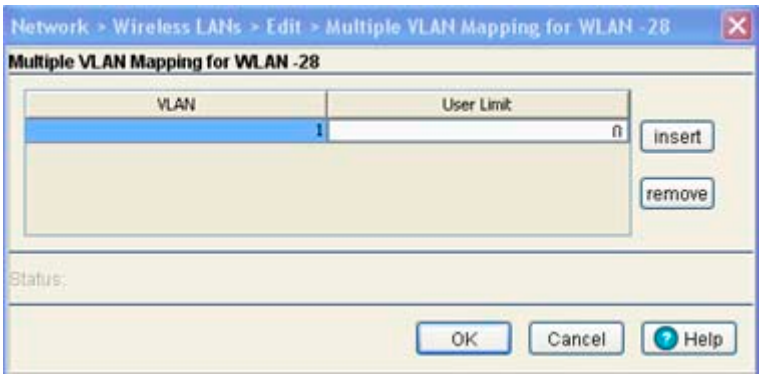
1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.

   A WLAN screen displays with the WLAN's existing configuration.
3. Select the **VLAN** radio button from the Configuration screen to change the VLAN designation for this WLAN.

   By default, all WLANs are initially assigned to VLAN 1.
4. Select the **Dynamic Assignment** checkbox for an user based VLAN assignment with Radius for this WLAN.
5. Select the **Assign Multiple VLAN(s)** button to map a WLAN to more than one VLAN. This displays the Multiple VLAN Mapping screen.

6. Configure the **Multiple VLAN Mapping for WLAN** table as required to add or remove multiple VLANS for the selected WLAN.

   Multiple VLAN's per WLAN are mapped (by default) to a regular VLAN and are not supported on an adaptive AP. Refer to *Editing the WLAN Configuration on page 4-26* to select and define an independent VLAN for adaptive AP support



VLAN	Displays the VLANs currently mapped to the WLAN. By default, VLAN 1 is configured for any selected WLAN.
User Limit	Displays the user limit configured for the mapped VLAN. The maximum allowed user limit is 4096 per VLAN.

7. Select the **Insert** button to add the VLAN using the criteria described above.
8. Select a row from the Multiple VLAN Mapping table and click the **Remove** button to delete the mapping of a VLAN to a WLAN.
9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

NOTE: In a cluster environment with multiple switches, please ensure that the VLAN list is consistent across all switches.

4.5.1.3 Configuring Authentication Types

Refer to the following to configure the WLAN authentication options available on the switch:

- *Configuring 802.1x EAP*
- *Configuring Kerberos*
- *Configuring Hotspots*
  - *Configuring an Internal Hotspot*
  - *Configuring an External Hotspot*
  - *Configuring an Advanced Hotspot*
  - *Configuring an Advanced Hotspot (Using the Local Radius Server)*
  - *Managing Hotspot Files*
  - *Custom Pages*
- *Configuring MAC Authentication*

Configuring 802.1x EAP

The IEEE 802.1x standard ties the 802.1x EAP authentication protocol to both wired and wireless LAN applications.

The EAP process begins when an unauthenticated supplicant (MU) tries to connect with an authenticator (in this case, the authentication server). The switch passes EAP packets from the client to an authentication server on the wired side of the switch. All other packet types are blocked until the authentication server (typically, a Radius server) verifies the MU's identity.

NOTE: As part of the EAP configuration process, ensure a primary and optional secondary Radius server have been properly configured to authenticate the users requesting access to the EAP protected WLAN. For more information on configuring Radius Server support for the EAP 802.1x WLAN, see *Configuring External Radius Server Support on page 4-49*.

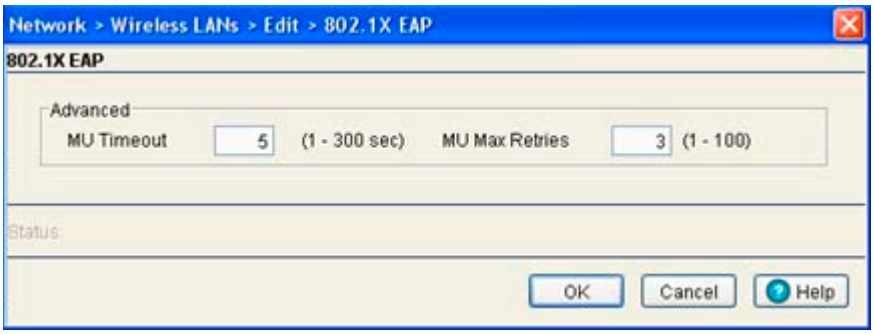
To configure a 802.1x EAP authentication scheme for a WLAN:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.

   A WLAN screen displays with the WLAN's existing configuration. Refer to the **Authentication** and **Encryption** columns to assess the WLAN's existing security configuration.
3. Select the **802.1X EAP** button from within the Authentication field.

   The **Radius Config...** button on the bottom of the screen will become enabled. Ensure a primary and optional secondary Radius Server have been configured to authenticate users requesting access to the EAP 802.1x supported WLAN. For more information, see *Configuring External Radius Server Support on page 4-49*.
4. Click the **Config** button to the right of the 802.1X EAP checkbox.

   The 802.1x EAP screen displays.



5. Define MU timeout and retry information for the authentication server.

MU Timeout	Define the time (between 1- 60 seconds) for the switch's retransmission of EAP-Request packets. The default is 5 seconds.
MU Max Retries	Specify the maximum number of times the switch retransmits an EAP-Request frame to the client before it times out the authentication session. The default is 3 retries, with a maximum of 100 supported.

6. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to use the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

Configuring Kerberos

Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, a MU must prove its identity to a server (and vice versa) across an insecure network connection. Once a MU and server prove their identity, they can encrypt all communications to assure privacy and data integrity. Kerberos can only be used with Motorola clients.

CAUTION: Kerberos makes no provisions for host security. Kerberos assumes it is running on a trusted host with an untrusted network. If host security is compromised, Kerberos is compromised as well

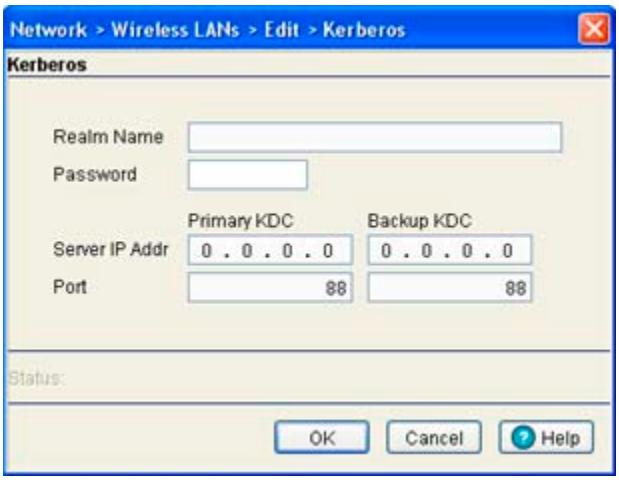
To configure a Kerberos authentication scheme for a WLAN:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab.
3. Click the **Edit** button.

   A WLAN screen displays with the WLAN's existing configuration. Refer to the **Authentication** and **Encryption** columns to assess the WLAN's existing security configuration.
4. Select the **Kerberos** button from within the Authentication field.

NOTE: Kerberos requires at least one encryption scheme be enabled (WEP 128 or other). If neither WEP 128 or KeyGuard is enabled, WEP 128 will automatically be enabled for use with Kerberos.

5. Click the **Config** button to the right of the Kerberos checkbox. The **Kerberos** screen displays.



6. Specify a case-sensitive **Realm Name**.

   The realm name is the name domain/realm name of the KDC Server. A realm name functions similarly to a DNS domain name. In theory, the realm name is arbitrary. However, in practice a Kerberos realm is named by uppercasing the DNS domain name associated with hosts in the realm.

7. Provide the password required to effectively update Kerberos authentication credentials.

8. Enter a **Server IP Addr** (IP address) for the Primary and (if necessary) Backup KDC.

   Specify a numerical (non-DNS) IP address for the Primary *Key Distribution Center* (KDC). The KDC implements an Authentication Service and a Ticket Granting Service, whereby an authorized user is granted a ticket encrypted with the user's password. The KDC has a copy of every user password provided. Optionally, specify a numerical (non-DNS) IP address for a backup KDC. Backup KDCs are often referred to as slave servers.

9. Specify the **Ports** on which the Primary and Backup KDCs reside.

   The default port number for Kerberos Key Distribution Centers is port 88.

10. Refer to the **Status** field for the current state of requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

11. Click **OK** to use the changes to the running configuration and close the dialog.

12. Click **Cancel** to close the dialog without committing updates to the running configuration.

Configuring Hotspots

A hotspot is essentially a Web page granting user access to the Internet (in this case within a switch managed WLAN). With the influx of Wi-Fi enabled mobile devices (laptops, PDAs etc.), hotspots are common and can be found at many airports, hotels and college campuses.

The switch enables hotspot operators to provide user authentication and accounting without a special client application. The switch uses a traditional Internet browser as a secure authentication device. Rather than rely on built-in 802.11security features to control association privileges, configure a WLAN with no WEP (an open network). The switch issues an IP address using a DHCP server, authenticates the user and grants the user access the Internet.

The hotspot feature supports both internal and external radius servers. It also supports the following three HTTP redirection options to satisfy various customer configurations:

1. Simple internal pre-built web-pages.

2. External Web-pages
3. Customized internal Web page (using the Advanced feature in hotspot configuration)

When a user visits a public hotspot and wants to browse a Web page, they can boot up their laptop and associate with the local Wi-Fi network by entering the correct SSID. They then start a browser. The hotspot access controller forces this un-authenticated user to a Welcome page from the hotspot Operator that allows the user to login with a username and password. This form of IP-Redirection requires no special software on the client.

To configure a hotspot, create a WLAN ESSID and select Hotspot as the authentication scheme from the WLAN Authentication menu. This is simply another way to authenticate a WLAN user, as it would be impractical to authenticate visitors using 802.1x authentications. Having enabled a hotspot, you will need to configure it. There are 2 parts to the hotspot configuration process:

- *Setting up the Hotspot Web pages*
- *Setting up the Radius server.*

Switch Hotspot Redirection

The switch uses destination network address translation to redirect user traffic from a default home page to the login page. Specifically, when the switch receives an HTTP Web page request from the user (when the client first launches its browser after connecting to the WLAN), a protocol stack on the switch intercepts the request and sends back an HTTP response after modifying the network and port address in the packet (thereby acting like a proxy between the User and the Web site they are trying to access).

To configure hotspot support:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.

   A WLAN screen displays with the WLAN's existing configuration. Refer to the **Authentication** and **Encryption** columns to assess the WLAN's existing security configuration.
3. Select the **Hotspot** button from within the Authentication field. The **Radius Config...** button on the bottom of the screen becomes enabled. Ensure a primary and optional secondary Radius Server have been configured to authenticate users requesting access to the hotspot supported WLAN. For more information, see *Configuring External Radius Server Support on page 4-49*.
4. Click the **Config** button to the right of the Hotspot checkbox.

   A **Hotspot** screen displays, allowing the user to define one of three available hotspot types.
5. Use the drop-down menu at the top of the screen to define whether this WLAN's Web pages are:
   - *Internal* - three HTML pages with basic functionality are made available on the switch's onboard HTTP server. The HTML pages are pre-created to collect login credentials through Login.htm, send them to a Radius server and display a Welcome.htm or a Faliure.htm depending on the result of the authentication attempt. For more information, see *Configuring an Internal Hotspot on page 4-37*.
   - *External* - a customer may wish to host their own external Web server using advanced Web content (using XML, Flash). Use the External option to point the switch to an external hotspot. For more information, see *Configuring an External Hotspot on page 4-40*.
   - *Advanced* - a customer may wish to use advanced Web content (XML, Flash) but might not have (or would not want to use) an external Web server, choosing instead to host the Web pages on the switch's HTTP Web server. Selecting the Advanced option allows for the importing the Web pages from an external source (like an FTP server) and hosting them on the switch. For more information,

see *Configuring an Advanced Hotspot on page 4-43*.

NOTE: The appearance of the Hotspot screen differs depending on which option is selected from the drop-down menu. You may want to research the options available before deciding which hotspot option to select.

NOTE: As part of the hotspot configuration process, ensure a primary and optional secondary Radius Server have been properly configured to authenticate the users requesting access to the hotspot supported WLAN. For more information on configuring Radius Server support for the hotspot supported WLAN, see *Configuring External Radius Server Support on page 4-49*.

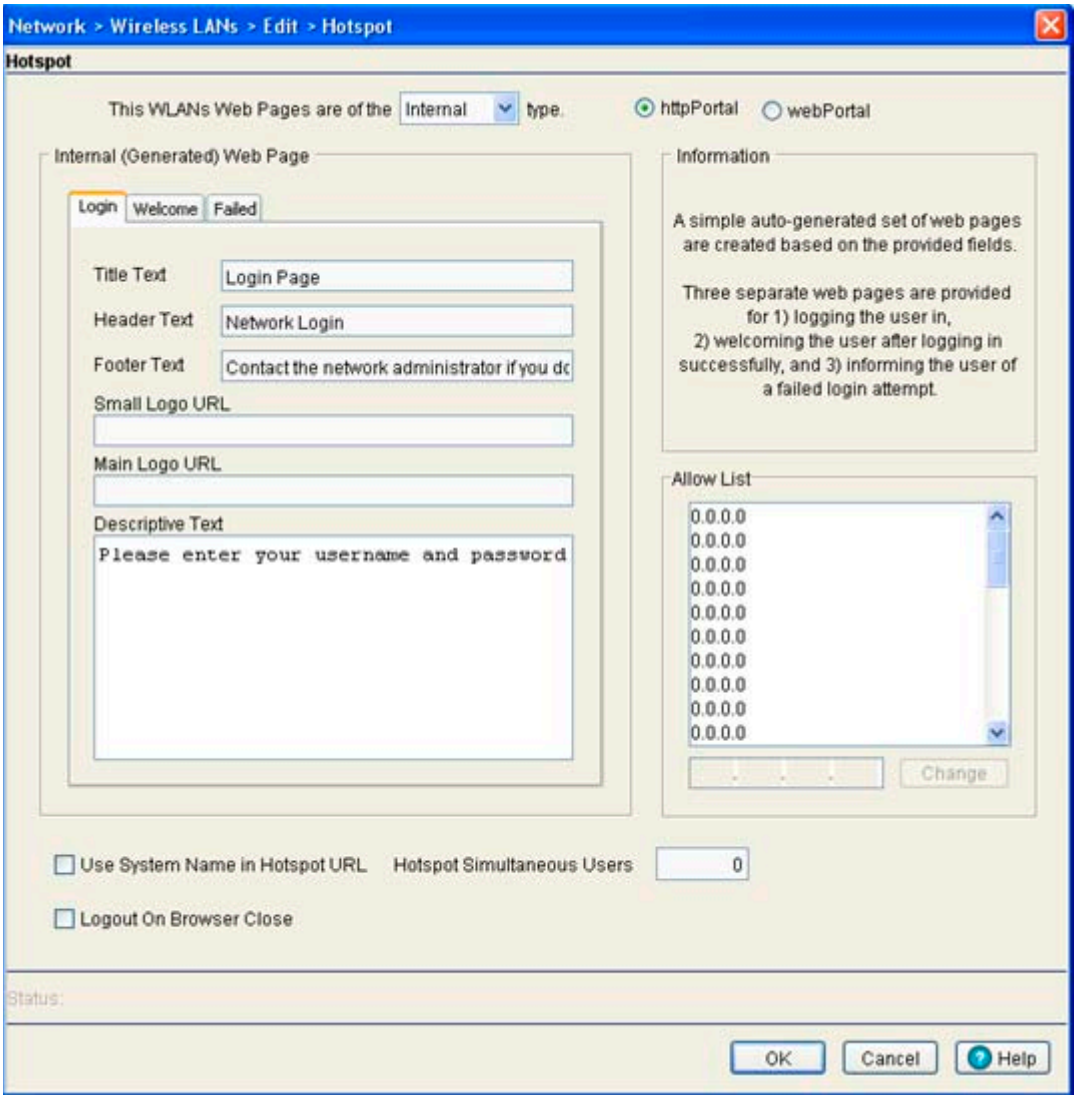
Configuring an Internal Hotspot

Using the Internal option means the user develops the hotspot using the three HTML pages made available on the switch's onboard HTTP server. The HTML pages are pre-created to collect login credentials through Login.htm, send them to a Radius server and display a Welcome.htm or a Faliure.htm depending on the result of the authentication attempt.

NOTE: When using an internal hotspot, ensure that traffic can pass on TCP port 444 between the switch's internal Web server and the hotspot clients.

To create a hotspot maintained by the switch's own internal resources:

1. Select **Network** > **Wireless LANs** from the main menu tree. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.
3. Select the **Hotspot** button from within the Authentication field. Ensure **Internal** is selected from within the **This WLAN's Web Pages are of the** drop-down menu.



4. Click the **Login** tab and enter the title, header, footer Small Logo URL, Main Logo URL and Descriptive Text you would like to display when users login to the switch maintained hotspot.

Title Text	Displays the HTML text displayed on the Welcome page when using the switch's internal Web server. This option is only available if Internal is chosen from the drop-down menu.
Header Text	Displays the HTML header displayed on the Failed page when using the switch's internal Web server. This option is only available if Internal is chosen from the drop-down menu.
Footer Text	Displays the HTML footer text displayed on the Failed page when using the switch's internal Web server. This option is only available if Internal is chosen from the drop-down menu.
Small Logo URL	Displays the URL for a small logo image displayed on the Failed page when using the switch's internal Web server. This option is only available if Internal is chosen from the drop-down menu.

Main Logo URL — Displays the URL for the main logo image displayed on the Failed page when using the switch's internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Descriptive Text — Specify any additional text containing instructions or information for the users who access the Failed page. This option is only available if Internal is chosen from the drop-down menu above. The default text is: "Either the username and password are invalid, or service is unavailable at this time."

5. Click the **Welcome** tab and enter the title, header, footer Small Logo URL, Main Logo URL and Descriptive Text you would like to display when users successfully authenticate with the switch maintained hotspot.

Title Text — The Title Text specifies the HTML title text displayed on the Welcome page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Header Text — The Header Text is the HTML header text displayed on the Welcome page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Footer Text — The Footer Text is the HTML footer text displayed on the Welcome page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Small Logo URL — The Small Logo URL is the URL for a small logo image displayed on the Welcome page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Main Logo URL — The Main Logo URL is the URL for the main logo image displayed on the Welcome page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Descriptive Text — Specify any additional text containing instructions or information for the users who access the Welcome page on the internal Web server. This option is only available if Internal is chosen from the pull down menu above. The default text is: You now have network access. Click the disconnect link on right when you want to end this session.

6. Click the **Failed** tab and enter the title, header, footer Small Logo URL, Main Logo URL and Descriptive Text you would like to display when users fail authentication with the switch maintained hotspot.

Title Text — The Title Text is the HTML title displayed on the Failed page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Header Text — The Header Text specifies the HTML header displayed on the Failed page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Footer Text — The Footer Text is the HTML footer text displayed on the Failed page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Small Logo URL — The Small Logo URL is the URL for a small logo image displayed on the Failed page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.

Main Logo URL	The Main Logo URL is the URL for the main logo image displayed on the Failed page when using the internal Web server. This option is only available if Internal is chosen from the drop-down menu above.
Descriptive Text	Specify any additional text containing instructions or information for the users who access the Failed page on the internal Web server. This option is only available if Internal is chosen from the drop-down menu above. The default text is: Either the username and password are invalid, or service is unavailable at this time.

7. Refer to the **Allow List** field, and enter any IP address (for internal or external Web sites) that may be accessed by the Hotspot user without authentication.

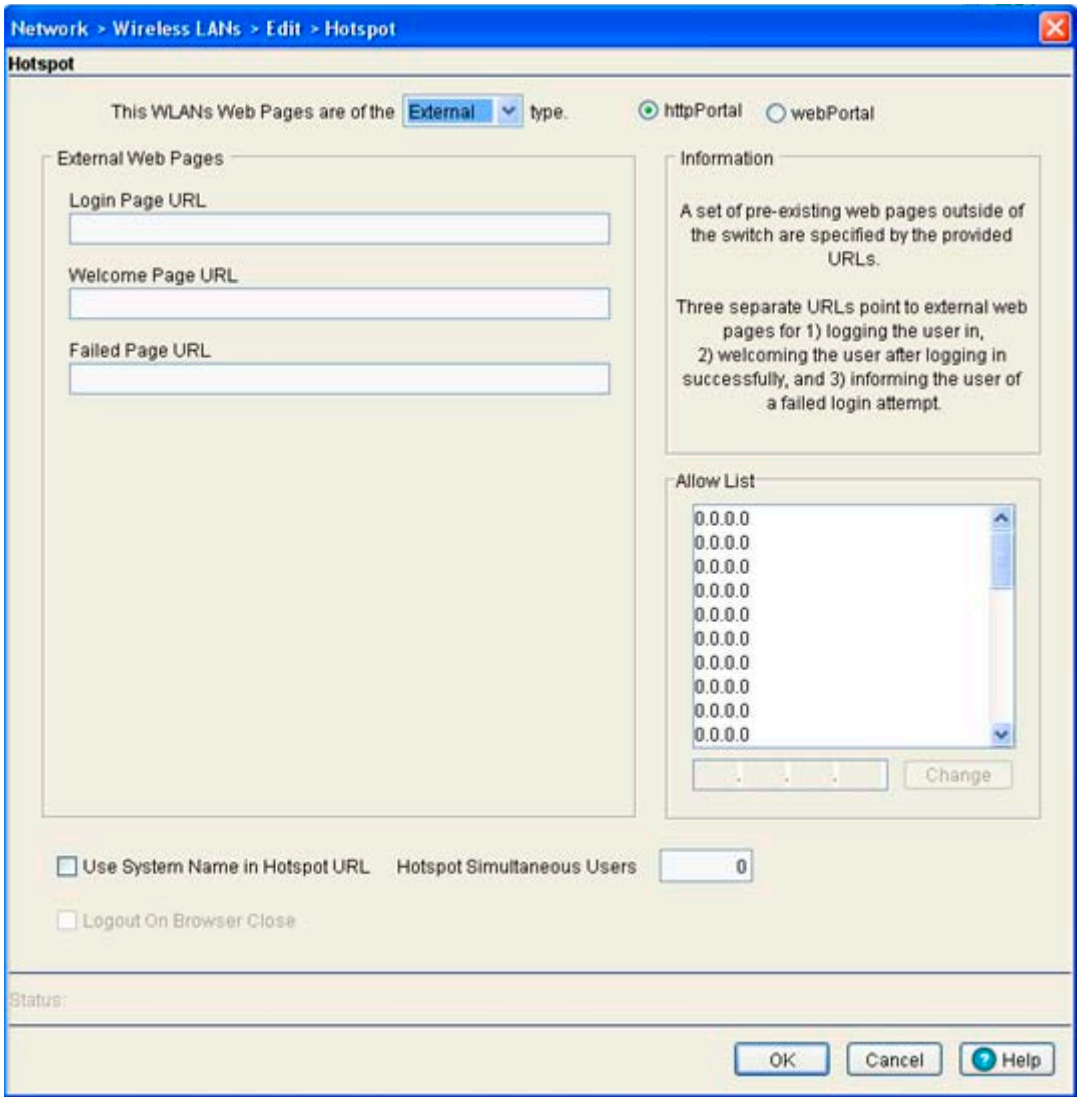
NOTE: In multi-switch hotspot environments if a single switch's internal pages are configured for authentication on the other switches, those switches will redirect to their own internal pages instead. In these environments is recommended to use an external server for all of the switches.

8. Check the **Use System Name in Hotspot URL** to use the **System Name** specified on the main Switch configuration screen as part of the hotspot address.
9. Check the **Logout on Browser Close** button to logout hotspot users from the network when they close their web browsers.
10. Specify the maximum **Hotspot Simultaneous Users** to set a limit on the number of concurrent unique hotspot users for the selected WLAN.
11. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
12. Click **OK** to use the changes to the running configuration and close the dialog.
13. Click **Cancel** to close the dialog without committing updates to the running configuration.

Configuring an External Hotspot

Selecting the external option entails hosting your own external Web server using advanced Web content (using XML, Flash). To create a hotspot maintained by an external server:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.
3. Select the **Hotspot** button from within the Authentication field. Ensure **External** is selected from within the **This WLAN's Web Pages are of the** drop-down menu.



4. Refer to the **External Web Pages** field and provide the Login, Welcome and Failed Page URLs used by the external Web server to support the hotspot.

Login Page URL Define the complete URL for the location of the Login page. The Login screen will prompt the hotspot user for a username and password to access the Welcome page. Ensure the RADIUS server port number is included in the URL using the following format:

https://192.168.0.70:444/wlan2/login.html

Welcome Page URL	Define the complete URL for the location of the Welcome page. The Welcome page assumes the hotspot user has logged in successfully and can access the Internet. Ensure the RADIUS server port number is included in the URL using the following format: https://192.168.0.70:444/wlan2/login.html
Failed Page URL	Define the complete URL for the location of the Failed page. The Failed screen assumes the hotspot authentication attempt has failed, you are not allowed to access the Internet and you need to provide correct login information to access the Web.Ensure the RADIUS server port number is included in the URL using the following format: https://192.168.0.70:444/wlan2/login.html

NOTE: When using an external hotspot page for redirection, certain HTML codes must be included on the pages to properly redirect to the switch.
For the **Login** and **Welcome** pages, the following code must be modified:

form action="https ://<ip address of the switch>:444/cgi-bin/hslogin.cgi" method="POST "

For the Welcome page the following code must also be modified:

href="http://<ip address of the web server>/login.htm

If the above code is not modified and included, switch redirection may not work.

NOTE: When using hotspot features in a cluster enviornment additional steps must be taken when specifying the external URLs. In order for the browser to return the login information correctly the IP address and port must be specified as part of the URL in the following format:
http://external_url<login | welcome | fail>.html?ip_address=a.b.c.d&port=x

5. Refer to the **Allow List** field, and enter any IP address (for internal or external Web sites) that may be accessed by the Hotspot user without authentication.

NOTE: If the Web-server is located on a VLAN other than the one on which the MUs will be associated, specify the IP address for the VLAN on which the server is located within the **Allow List**.

6. Check the **Use System Name in Hotspot URL** to use the **System Name** specified on the main Switch configuration screen as part of the hotspot address.
7. Specify the maximum **Hotspot Simultaneous Users** to set a limit on the number of concurrent unique hotspot users for the selected WLAN.
8. Check the **Logout on Browser Close** button to logout hotspot users from the network when they close their web browsers.
9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

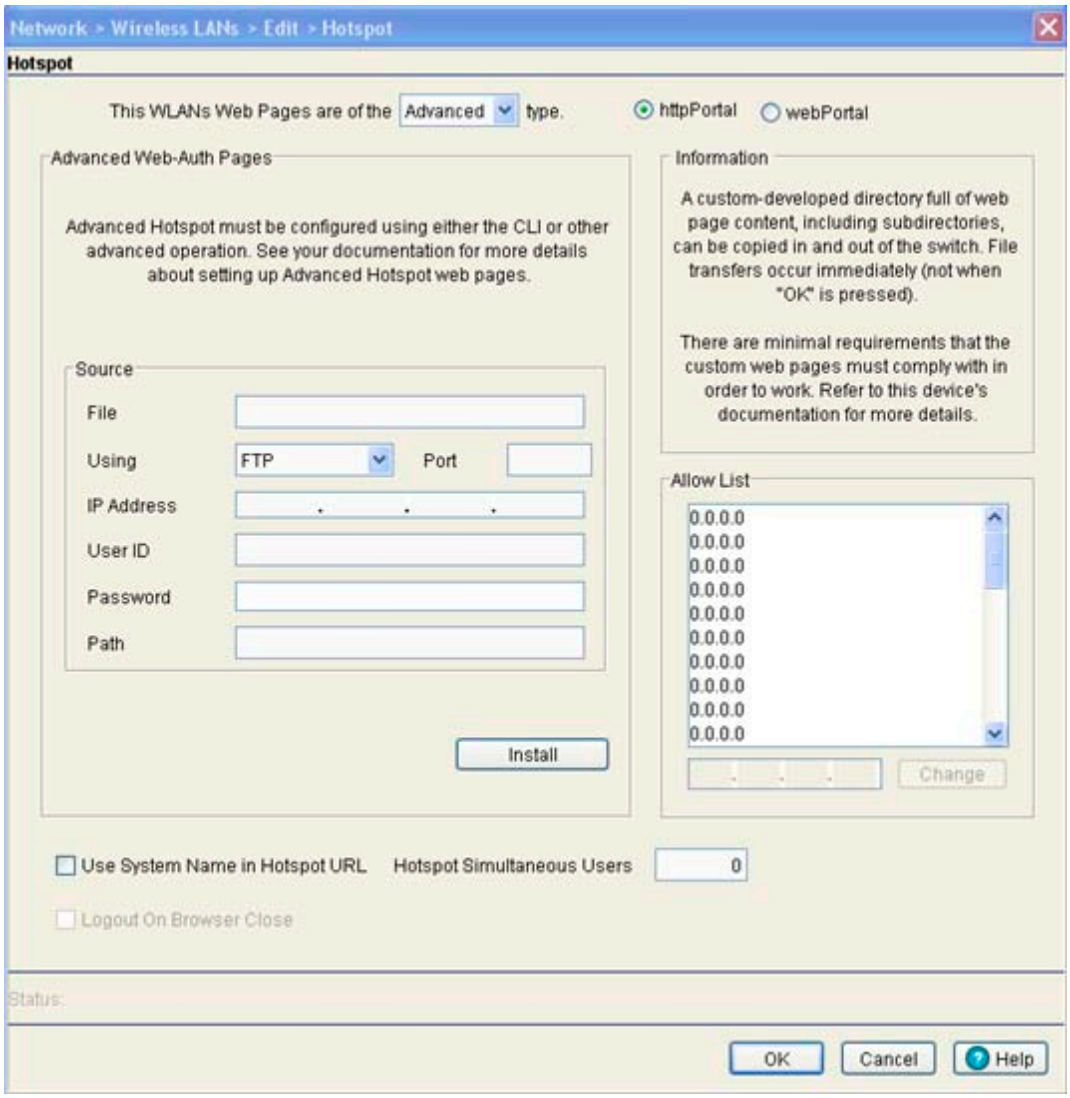
Configuring an Advanced Hotspot

A customer may wish to use advanced Web content (XML, Flash) but might not have (or would not want to use) an external Web server, choosing instead to host the Web pages on the switch's HTTP Web server. Selecting the Advanced option allows for importing the Web pages from an external source (like an FTP server) and hosting them on the switch.

To use the Advanced option to define the hotspot:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab.
3. Click the **Edit** button.
4. Select the **Hotspot** button from within the Authentication field.

   Ensure **Advanced** is selected from within the **This WLAN's Web Pages are of the** drop-down menu.



NOTE: Advanced hotspot configuration is not permissible using the switch Web UI. Refer to the switch CLI or other advanced configuration options to define a hotspot with advanced properties. However, the switch can still install and maintain directories containing Web page content.

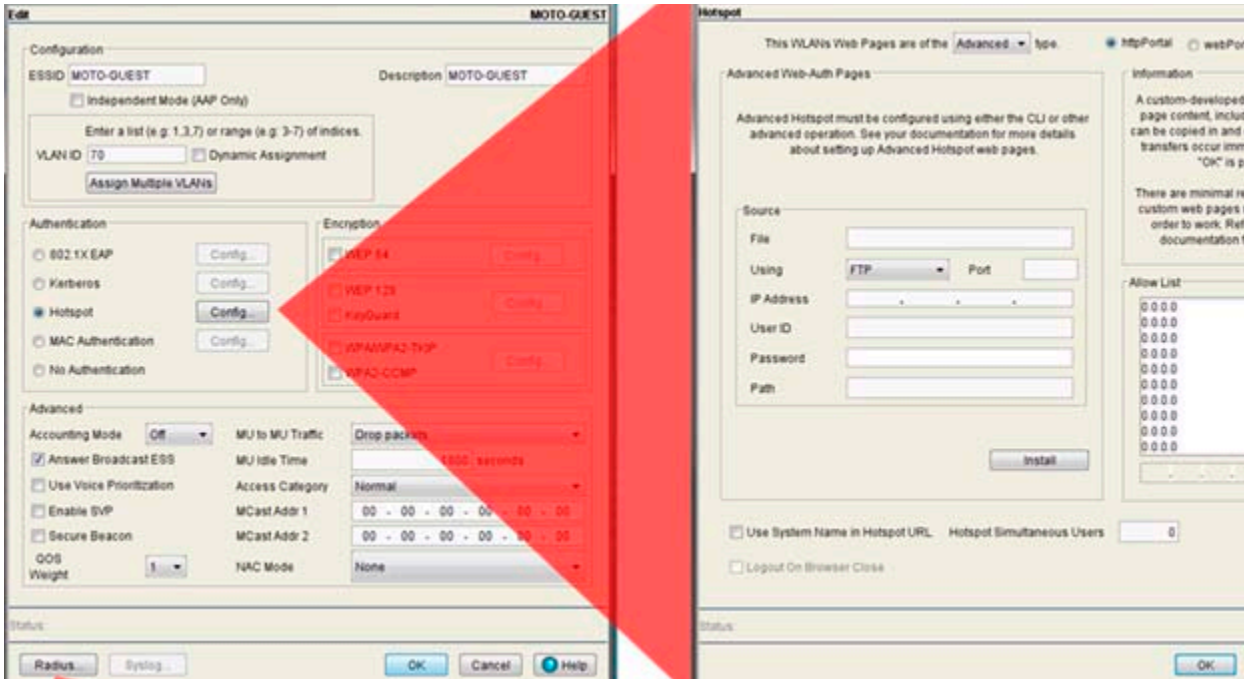
5. Once the properties of the advanced hotspot have been defined, the file can be installed on the switch and used to support the hotspot. The following parameters are required to upload the file:
   a. Specify a source hotspot configuration file. The file used at startup automatically displays within the **File** parameter.
   b. Refer to the **Using** drop-down menu to configure whether the hotspot file transfer is conducted using FTP or TFTP.
   c. Enter the **IP Address** of the server or system receiving the source hotspot configuration. Ensure the IP address is valid or risk jeopardizing the success of the file transfer.
   d. If using FTP, enter the **User ID** credentials required to transfer the configuration file from a FTP server.
   e. If using FTP, enter the **Password** required to send the configuration file from an FTP server.
   f. Specify the appropriate **Path** name to the hotspot configuration on the local system disk or server.
   g. Once the location and settings for the advanced hotspot configuration have been defined, click the **Install** button to use the hotspot configuration with the switch.
6. Refer to the **Allow List** field, and enter any IP address (for internal or external Web sites) that may be accessed by the Hotspot user without authentication.
7. Check the **Use System Name in Hotspot URL** to use the **System Name** specified on the main Switch configuration screen as part of the hotspot address.
8. Specify the maximum **Hotspot Simultaneous Users** to set a limit on the number of concurrent unique hotspot users for the selected WLAN.
9. Check the **Logout on Browser Close** button to logout hotspot users from the network when they close their web browsers.
10. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
11. Click **OK** to use the changes to the running configuration and close the dialog.
12. Click **Cancel** to close the dialog without committing updates to the running configuration.

Configuring an Advanced Hotspot (Using the Local Radius Server)

The example below shows how to create and upload a customized login, failed and welcome page onto the switch. This example uses the switch's local AAA server.

To define a hotspot using the switch's local Radius server:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab.
3. Click the **Edit** button.
4. Select the **Hotspot** button from within the Authentication field.
5. Select the **Config...** button.



6. Ensure **Advanced** is selected from within the **This WLAN's Web Pages are of the** drop-down menu.

   Define the advanced hotspot configuration following step 5 onward in *Configuring an Advanced Hotspot on page 4-43*.

NOTE: For information on configuring external Radius server support for supporting a advanced hotspot, see *Configuring External Radius Server Support on page 4-49*.

7. Use the switch CLI to define the attributes of the local Radius server configuration.

   The following is an example of just the CLI needed to support the local Radius server configuration:

```
wlan 2 enable
wlan 2 description MOTO-GUEST
wlan 2 ssid MOTO-GUEST
wlan 2 vlan 70
wlan 2 authentication-type hotspot
wlan 2 mu-mu-disallow
wlan 2 hotspot webpage-location advanced
wlan 2 radius server primary 192.168.10.14
wlan 2 radius server primary radius-key 0 ESELAB
wlan 2 radius reauth 3600
wlan 2 radius accounting server primary 192.168.10.14
wlan 2 radius accounting server primary radius-key 0 ESELAB
!
! Output Omitted
!
radius-server local
authentication eap-auth-type all
nas 192.168.10.0/24 key 0 ESELAB
ldap-group-verification disable
```

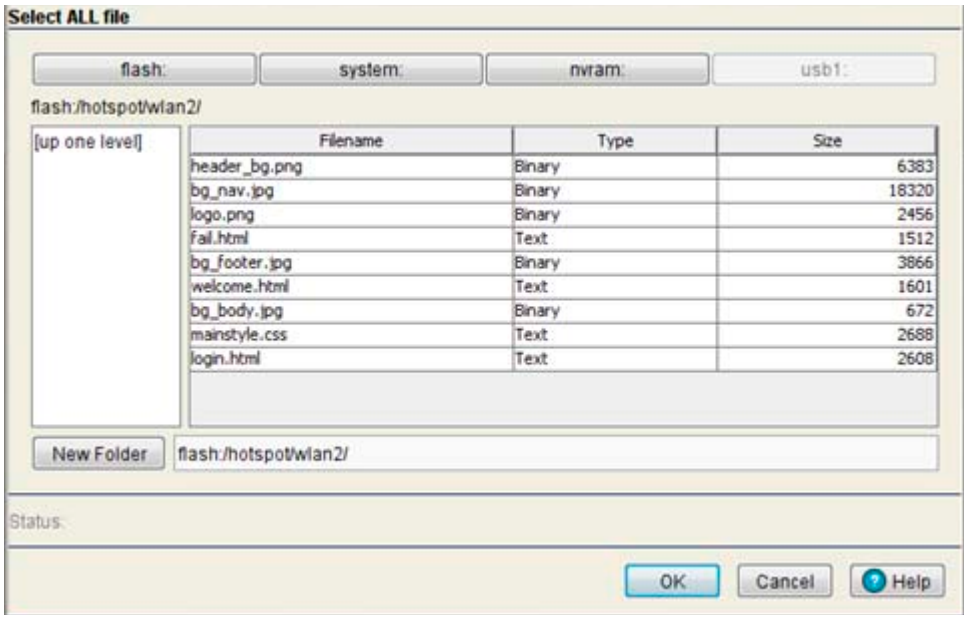
```
ca trust-point ESELAB
server trust-point ESELAB
group "Guests"
guest-group enable
policy vlan 70
policy wlan 2
!
radius-server local
rad-user "guest" password 0 password group "Guests" guest expiry-time
20:27 expiry-date 11:17:2009 start-time 20:

27 start-date 11:16:2008
```

Managing Hotspot Files

When creating a new hotspot, the switch builds a directory in flash named *hotspot* with a subdirectory named *wlanX* (where X is the WLAN ID). The switch also creates a default login, welcome and failed html files in the directory. These files can be copied to a FTP or TFTP server and customized.

Use the CLI or the Web UI to upload files from the switch to a FTP/TFTP server. If you want to use the Web UI, use **Switch** > **File Management**. Upload customized content ether using the CLI's `copy` command or TFTP/FTP in the hotspot configuration (you can also use **Switch** > **File Management**).

The example below displays samples (both from a file manager and the switch CLI) of the directory and files used by an advanced hotspot. These examples use pages supporting various graphics files. These pages also use a HTML style sheet to define certain elements. Create custom pages using standard HTML elements and formatting as long as they include the content required by the switch to pass credential information.



```
RFS6000#dir flash:/hotspot/wlan2/
Directory of flash:/hotspot/wlan2/
-rw-   6383      Wed Sep 24 12:44:09 2008   header_bg.png
-rw-   18320     Wed Sep 24 12:23:21 2008   bg_nav.jpg
-rw-   2456      Wed Sep 24 12:39:28 2008   logo.png
-rw-   1512      Wed Sep 24 12:38:16 2008   fail.html
-rw-   3866      Wed Sep 24 12:23:20 2008   bg_footer.jpg
-rw-   1601      Wed Sep 24 12:38:15 2008   welcome.html
-rw-   672       Wed Sep 24 12:23:20 2008   bg_body.jpg
-rw-   2688      Wed Sep 24 12:21:50 2008   mainstyle.css
-rw-   2608      Wed Sep 24 12:38:15 2008   login.html
```

Custom Pages

The critical required components for a customized *login*, *welcome* and *failed* page includes:

Login Page

The login.html page is presented to all unauthenticated users when they connect to the hotspot. The critical part of this login page is a HTML form which must be included to present the username and password to the switch.

The following examples show both raw and formatted HTML. You'll need to put this in a table somewhere in the custom login page and include text, such as username/ password etc.

Raw HTML Example

```
<form name="frmLogin" id="frmLogin" action="/cgi-bin/hslogin.cgi" method="POST" >
<input type="text" size="20" name="f_user">
<input type="password" size="20" name="f_pass">
<input type="submit" name="submit" value="Log In">
</form>
```

Formatted HTML Example

```
<table border="0">
    <form name="frmLogin" id="frmLogin" action="/cgi-bin/hslogin.cgi" method="POST" >
    <tr><td><b>Username:</b></td><td><input type="text" size="20" name="f_user"></td></tr>
    <tr><td><b>Password:</b></td><td><input type="password" size="20" name="f_pass"></td></tr>
    <tr><td colspan="2" align="center"><input type="submit" name="submit" value="Log In"></td></tr>
    </form>
</table>
```

Welcome Page

The welcome.html page displays upon successful authentication. On the welcome page, you'll want to include a simple welcome message, as well as the following URL allowing users to manually disconnect from the hotspot.

```
<a href="/cgi-bin/hslogout.cgi">Disconnect</a>
```

Failed Page

The failed page is presented to users who fail authentication or enter incorrect login information. On this page you can include support information, a link to sign-up for service (assuming the external server is included in the allowed list) as well as a URL to re-attempt authentication.

Try Again

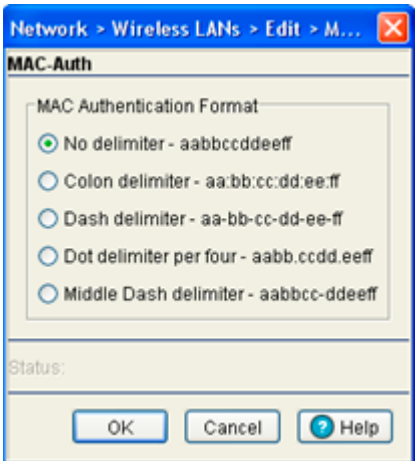
Configuring MAC Authentication

The MAC Authentication option allows the user to configure a Radius server for user authentication with the range of MAC addressees defined as allowed or denied access to the switch managed network.

NOTE: As part of the MAC Authentication process, ensure a primary and optional secondary Radius Server have been properly configured to authenticate the users requesting access to the ACL supported WLAN. For more information on configuring Radius Server support for the MAC Authentication supported WLAN, see *Configuring External Radius Server Support on page 4-49*.

To configure the format of MAC addresses used in MAC Authentications:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab.
3. Click the **Edit** button.
4. Select the **MAC Authentication** button from within the Authentication field.
   This enables the **Radius** button at the bottom of the **Network** > **Wireless LANs** > **Edit** screen.
5. Click the Config button next to the **MAC Authentication** option to open a dialogue where the format of MAC Addresses can be configured.



   The MAC Authentication Format setting determines the text format that MAC addresses are transmitted when using MAC-Auth authentication

6. Select a format for MAC Addresses used in MAC Authentication:
   - *No delimiter*. The 12 digit MAC Address is in a format with no spaces or delimeters.
   - *Colin delimiter*. The 12 digit MAC Address is in a format separated by colons after every pair.
   - *Dash delimiter*. The 12 digit MAC Address is in a format separated by dashes after every pair.
   - *Dot delimiter per four*. The 12 digit MAC Address is in a format separated by periods after every four digits.

- *Middle Dash delimiter*: The 12 digit MAC Address is in a format separated in the middle by a dash.

7. Click **OK** to use the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

Configuring External Radius Server Support

If either the EAP 802.1x, Hotspot or Dynamic MAC ACL options have been selected as an authentication scheme for a WLAN, the **Radius Config...** button at the bottom of the Network > Wireless LANs > Edit becomes enabled. The Radius Configuration screen provides users the option of defining an external primary and secondary Radius Server as well as a NAC Server if you do not use the switch's resident Radius Server.

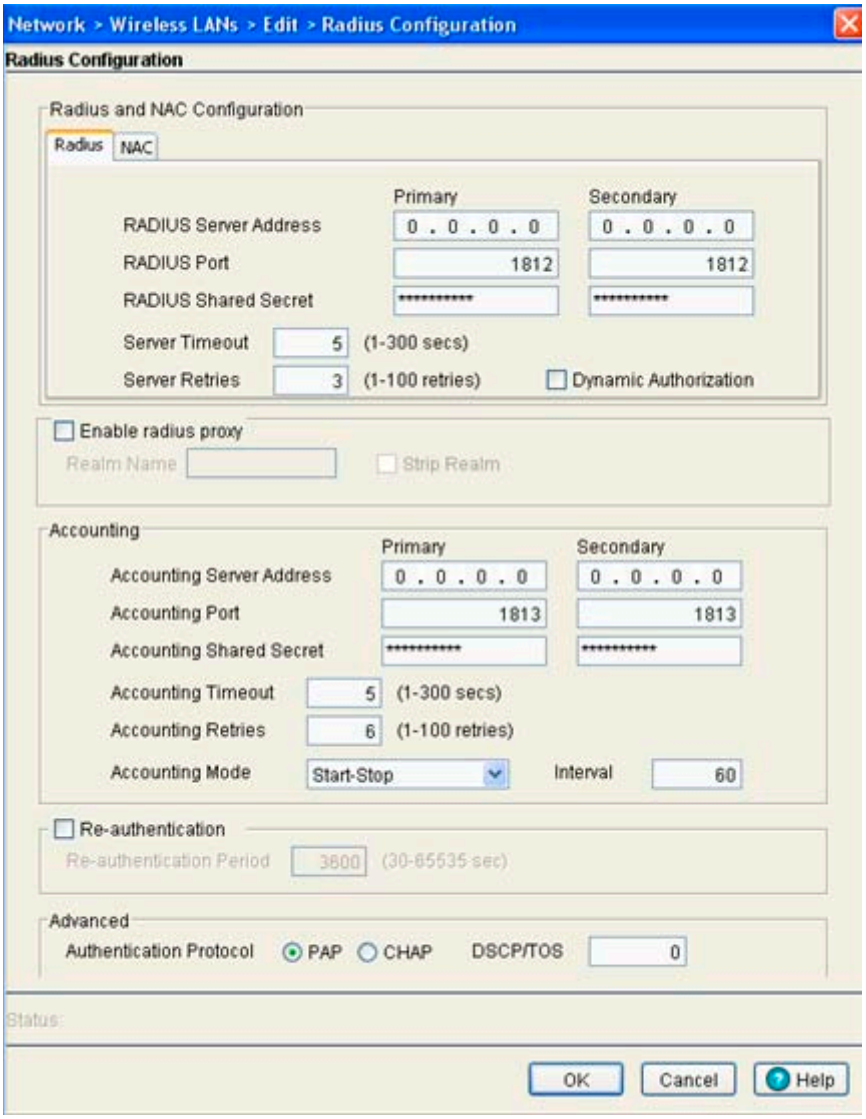
NOTE: If using the switch's local Radius Server for user authentication instead of an external primary or secondary Radius Server, see *Configuring the Radius Server on page 6-84*. The switch's local Radius Server provides an easy setup option and offers a high degree of security and accountability.

The switch ships with a default configuration defining the local Radius Server as the primary authentication source (default users are admin with superuser privileges and operator with monitor privileges). No secondary authentication source is specified. However, Motorola recommends using an external Radius Server as the primary user authentication source and the local switch Radius Server as the secondary user authentication source. To use an external Radius Server as either a primary or secondary authentication source, it must be specified appropriately.

To configure an external Radius Server for EAP 802.1x, Hotspot or Dynamic MAC ACL WLAN support:

NOTE: To optimally use an external Radius Server with the switch, Motorola recommends defining specific external Server attributes to best utilize user privilege values for specific switch permissions. For information on defining the external Radius Server configuration, see *Configuring an External Radius Server for Optimal Switch Support on page 4-52*.

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab.
3. Click the **Edit** button.
4. Select either the **EAP 802.1x, Hotspot** or **Dynamic MAC ACL** button from within the Authentication field. This enables the **Radius Config...** button at the bottom of the Network > Wireless LANs > Edit screen.
5. Select the **Radius Config...** button. The Radius Configuration screen displays for defining an external Radius or NAC Server.



The Radius Configuration screen contains tabs for defining both the Radius and NAC server settings. For NAC overview and configuration information, see *Configuring NAC Server Support on page 4-53*.

6. Refer to the **Server** field and define the following credentials for a primary and secondary Radius server.

RADIUS Server Address	Enter the IP address of the primary and secondary server acting as the Radius user authentication data source.
RADIUS Port	Enter the TCP/IP port number for the primary and secondary server acting as the Radius user authentication data source. The default port is 1812.
RADIUS Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary Radius server.
Server Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the switch to time out on a request to the primary or secondary server.

Server Retries	Enter a value between 1 and 100 to indicate the number of times the switch attempts to reach the primary or secondary Radius server before giving up.
Dynamic Authorization	Authorization amongst the Radius servers is conducted dynamically as they connect and disconnect periodically.

NOTE: The Radius or NAC server's **Timeout** and **Retries** should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fall back to the secondary server will not work.

7. Refer to the **Accounting** field and define the following credentials for a primary and secondary Radius Server.

Accounting Server Address	Enter the IP address of the primary and secondary server acting as the Radius accounting server.
Accounting Port	Enter the TCP/IP port number for the primary and secondary server acting as the Radius accounting data source. The default port is 1813.
Accounting Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary Radius accounting server.
Accounting Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the switch to time out a request to the primary or secondary accounting server.
Accounting Retries	Enter a value between 1 and 100 to indicate the number of times the switch attempts to reach the primary or secondary Radius accounting server before giving up.
Accounting Mode	Use the Accounting Mode drop-down menu to define the accounting mode as either **Start-Stop**, **Stop Only** or **Start-Interim-Stop**. Define the **Interval** (in seconds) used with the selected accounting mode.

8. Select the **Re-authentication** checkbox to force a periodic re-authentication with the Radius server. Periodic repetition of the authentication process provides ongoing security for currently authorized connections. Define an interval between 30 and 65535 seconds.
9. Refer to the **Advanced** field to define the authentication protocol used with the Radius Server.

PAP	PAP - *Password Authentication Protocol* sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized.
CHAP	CHAP is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
DSCP/TOS	Optionally mark packets with a *DiffServ CodePoint* (DSCP) in the header. The DSCP value is stored in the first 6 bits of the Type of Service (ToS) field that is part of the standard IP header. The DCSP values are associated with a forwarding treatment called P*er Hop Behaviors* (PHB). Service can be provisioned (if necessary) by assigning a DCSP point code from 1 - 6.

10. Click **OK** to save the changes made to this screen.

11. Click **Cancel** to revert back to the last saved configuration and move back to the **Network** > **Wireless LANs** > **Edit** screen.

Configuring an External Radius Server for Optimal Switch Support

The switch's external Radius Server should be configured with Motorola RF Switch specific attributes to best utilize the user privilege values assignable by the Radius Server. The following two values should be configured on the external Server for optimal use with the switch:

- *Motorola user privilege values*
- *User login source*

Configuring Motorola Specific Radius Server User Privilege Values

The following recommended Radius Server user privilege settings specify access privilege levels for those accessing the switch managed network. To define user privilege values, assign the following attributes in the external Radius Server:

1. Set the attribute number to 1 and its type as "integer."
2. Define the following possible decimal values for user access permissions:
   a. Set the **Monitor Role** value to 1 (read-only access to the switch).
   b. Set the **Helpdesk Role** value to 2 (helpdesk/support access to the switch).
   c. Set the **Nwadmin Role** value to 4 (wired and wireless access to the switch).
   d. Set the **Sysadmin Role** value to 8 (system administrator access).
   e. Set the **WebAdmin Role** value to 16 (guest user application access).
   f. Set the **Superuser Role** value to 32768 (grants full read/write access to the switch).
3. Specify multiple privileges (for a single user) by specifying different attributes as needed. The privilege values can be *ORed* and specified once. For example, if a user needs monitor (read-only) and helpdesk access, configure the Radius Server with two attributes. Once with a value 1 for monitor access and then with a value 2 for the helpdesk role.

   Multiple roles can also be defined by configuring the Radius Server with attribute 1 and value 3 (or monitor value 1 and helpdesk value 2).

NOTE: If user privilege attributes are not defined for the Radius Server, users will be authenticated with a default privilege role of 1 (Monitor read-only access).

Configuring the User Login Sources

The following recommended Radius Server user login sources specify the location (ssh/telnet/console/Web) from which users are allowed switch access. If login access permissions are not defined (restricted), users will be allowed to login from each interface. To define login source access locations:

1. Set the attribute number to 100 and its type as "integer."
2. Define the following possible decimal values for login sources:
   a. Set the **Console Access** value to 128 (user is allowed login privileges only from console).
   b. Set the **Telnet Access** value to 64 (user is allowed login privileges only from a Telnet session).
   c. Set the **SSH Access** value to 32 (user is allowed login privileges only from ssh session).
   d. Set the **Web Access** value to 16 (user is allowed login privileges only from Web/applet).

3. Specify multiple access sources by using different values. The privilege values can be ORed and specified once. For example, if a user needs access from both the console and Web, configure the Radius Server with the 100 attribute twice, once with value 128 for console and next with value 16 for Web access.

Configuring NAC Server Support

There is an increasing proliferation of insecure devices (laptops, mobile computers, PDA, smart-phones) accessing WiFi networks. These devices often lack proper anti-virus software and can potentially infect the network they access. Device compliance per an organization's security policy must be enforced using NAC. A typical security compliance check entails verifying the right operating system patches, anti-virus software etc.

NAC is a continuous process for evaluating MU credentials, mitigating security issues, admitting MUs to the network and monitoring MUs for compliance with globally-maintained standards and policies. If a MU is not in compliance, network access is restricted by quarantining the MU.

Using NAC, the switch hardware and software grants access to specific network devices. NAC performs a user and MU authorization check for devices without a NAC agent. NAC verifies a MU's compliance with the switch's security policy. The switch supports only EAP/802.1x NAC. However, the switch provides a mean to bypass NAC authentication for MU's without NAC 802.1x support (printers, phones, PDAs etc.).

For a NAC configuration example using the switch CLI, see *Configuring the NAC Inclusion List on page 4-71* or *Configuring the NAC Exclusion List on page 4-75*.

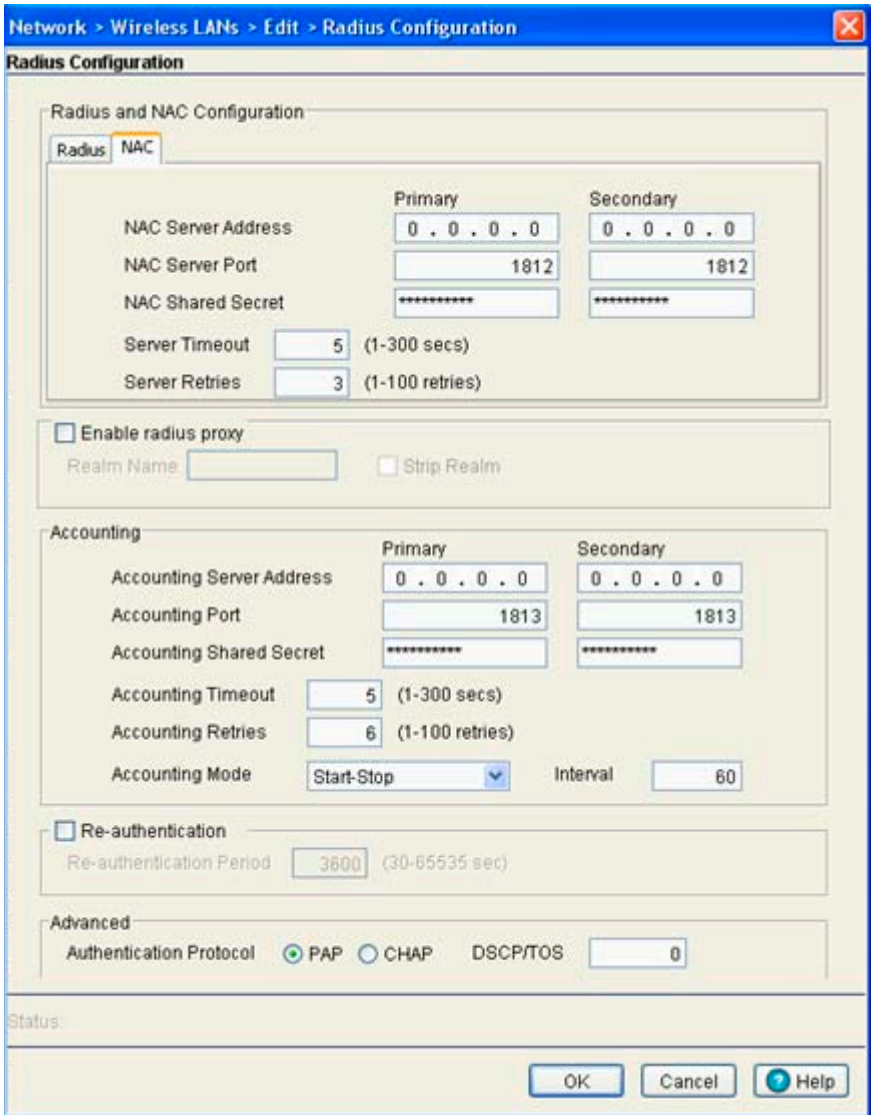
- *None* – NAC disabled, no NAC is conducted. A MU can only be authenticated by a Radius server.
- *Do NAC except exclude list* – A MU NAC check is conducted except for those in the exclude-list. Devices in the exclude-list will not have any NAC checks.
- *Bypass NAC except include list* – A MU NAC check is conducted only for those MUs in the include-list.

To configure NAC Server support:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed with the **Configuration** tab.
3. Click on the **Edit** button.
4. Select either the **EAP 802.1x**, **Hotspot** or **Dynamic MAC ACL** button from within the Authentication field.

   This enables the Radius button at the bottom of the *Network > Wireless LANs > Edit* screen.
5. Select the **Radius** button.

   The Radius Configuration screen displays (with the Radius tab displayed by default) for defining an external Radius or NAC Server.
6. .Select the **NAC** tab to configure NAC support.



7. Refer to the **Server** field and define the following credentials for a primary and secondary NAC server.

NAC Server Address — Enter the IP address of the primary and secondary NAC server.

NAC Server Port — Enter the TCP/IP port number for the primary and secondary server. The default port is 1812.

NAC Shared Secret — Provide a shared secret (password) for user credential authentication with the primary or secondary NAC server.

Server Timeout — Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the switch to time out on a request to the primary or secondary NAC server.

Server Retries — Enter a value between 1 and 100 to indicate the number of times the switch attempts to reach the primary or secondary server before giving up.

CAUTION: The server's **Timeout** and **Retries** should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fall back to the secondary server will not work.

8. Refer to the **Accounting** field and define the following credentials for a primary and secondary NAC Server.

Accounting Server Address	Enter the IP address of the primary and secondary server acting as the NAC accounting server.
Accounting Port	Enter the TCP/IP port number for the primary and secondary server acting as the NAC accounting data source. The default port is 1813.
Accounting Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary NAC accounting server.
Accounting Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the switch to time out a request to the primary or secondary accounting server.
Accounting Retries	Enter a value between 1 and 100 to indicate the number of times the switch attempts to reach the primary or secondary NAC accounting server before giving up.
Accounting Mode	Use the Accounting Mode drop-down menu to define the accounting mode as either **Start-Stop**, **Stop Only** or **Start-Interim-Stop**. Define the interval (in seconds) used with the selected accounting mode

9. Select the **Re-authentication** checkbox to force a periodic re-authentication with the NAC server.

   Periodic repetition of the authentication process provides ongoing security for currently authorized connections. Define an interval between 30 and 65535 seconds.

10. Refer to the **Advanced** field to define the authentication protocol used with the NAC Server.

PAP	PAP - *Password Authentication Protocol* sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized.
CHAP	CHAP is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
DSCP/TOS	Optionally mark packets with a *DiffServ CodePoint* (DSCP) in its header. The DSCP value is stored in the first 6 bits of the Type of Service (ToS) field that is part of the standard IP header. The DCSP values are associated with a forwarding treatment called *Per Hop Behaviors* (PHB). Service can be provisioned (if necessary) by assigning a DCSP point code from 1 - 6.

11. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
12. Click **OK** to use the changes to the running configuration and close the dialog.
13. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.1.4 Configuring Different Encryption Types

To configure the WLAN data encryption options available on the switch, refer to the following:

- *Configuring WEP 64*
- *Configuring WEP 128 / KeyGuard*
- *Configuring WPA/WPA2 using TKIP and CCMP*

Configuring WEP 64

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.

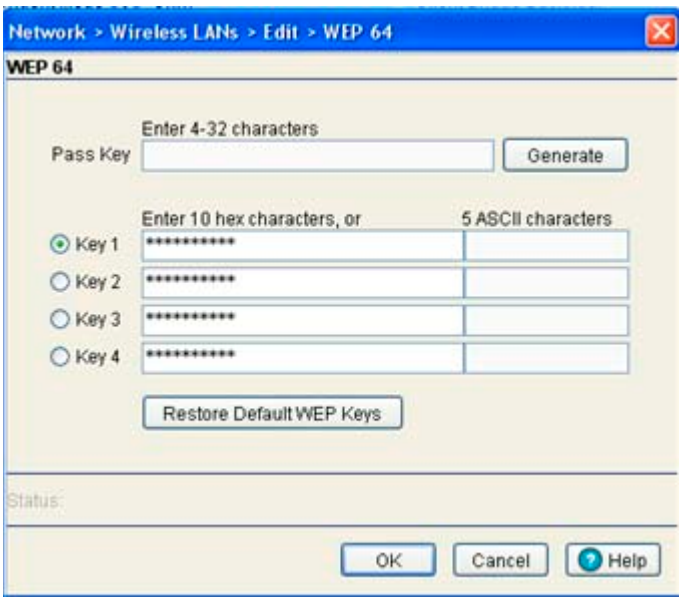
WEP 64 is a less robust encryption scheme than WEP 128 (shorter WEP algorithm for a hacker to duplicate), but WEP 64 may be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP 64:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.

   A WLAN screen displays with the WLAN's existing configuration. Refer to the **Authentication** and **Encryption** columns to assess the WLAN's existing security configuration.
3. Select the **WEP 64** button from within the Encryption field.
4. Click the **Config** button to the right of the WEP 64 checkbox.

   The **WEP 64** screen displays.



5. Specify a 4 to 32 character **Pass Key** and click the **Generate** button.

   The pass key can be any alphanumeric string. The switch, other proprietary routers and Motorola MUs use the algorithm to convert an ASCII string to the same hexadecimal number. MUs without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers.

6. Use the **Key #1-4** areas to specify key numbers.

   The key can be either a hexadecimal or ASCII. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length or 5 ASCII characters. Select one of these keys for activation by clicking its radio button.

   Default (hexadecimal) keys for WEP 64 include:

Key 1	1011121314
Key 2	2021222324
Key 3	3031323334
Key 4	4041424344

7. If you feel it necessary to restore the WEP algorithm back to its default settings, click the **Restore Default WEP Keys** button. This may be the case if you feel the latest defined WEP algorithm has been compromised and longer provides its former measure of data security.
8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

Configuring WEP 128 / KeyGuard

WEP 128 provides a more robust encryption algorithm that WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys. WEP 128 may be all that a small-business user needs for the simple encryption of wireless data.

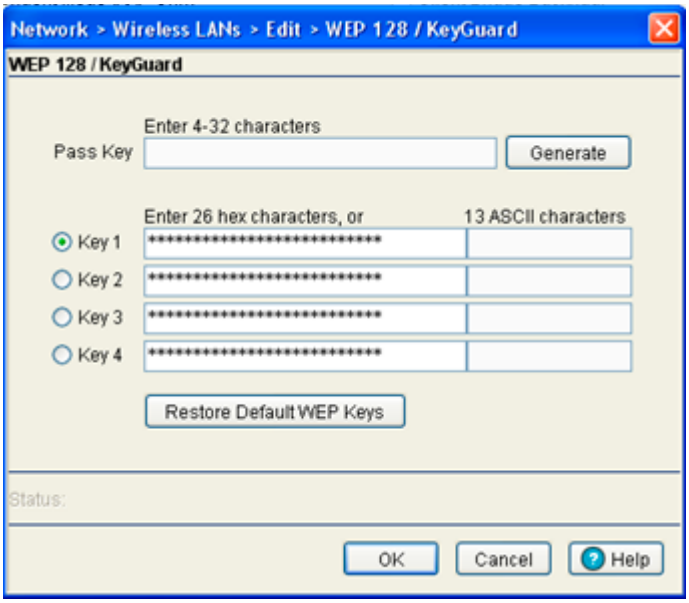
KeyGuard is a proprietary encryption method developed by Motorola Technologies. KeyGuard is Motorola's enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

To configure WEP 128 or KeyGuard:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.

   A WLAN screen displays with the WLAN's existing configuration. Refer to the **Authentication** and **Encryption** columns to assess the WLAN's existing security configuration.
3. Select either the **WEP 128** or **KeyGuard** button from within the Encryption field.
4. Click the **Config** button to the right of the WEP 128 and KeyGuard checkboxes.

   The **WEP 128 / KeyGuard** screen displays.



5. Specify a 4 to 32 character **Pass Key** and click the **Generate** button.

   The pass key can be any alphanumeric string. The switch and Motorola MUs use the algorithm to convert an ASCII string to the same hexadecimal number. MUs without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers.

6. Use the **Key #1-4** areas to specify key numbers.

   The key can be either a hexadecimal or ASCII. The keys are 26 hexadecimal characters in length or 13 ASCII characters. Select one of these keys for activation by clicking its radio button.

   Default (hexadecimal) keys for WEP 128 and KeyGuard include:

Key 1	101112131415161718191A1B1C
Key 2	202122232425262728292A2B2C
Key 3	303132333435363738393A3B3C
Key 4	404142434445464748494A4B4C

7. If you feel it necessary to restore the WEP algorithm back to its default settings, click the **Restore Default WEP Keys** button. This may be the case if you feel the latest defined WEP algorithm has been compromised and no longer provides its former measure of data security.
8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

Configuring WPA/WPA2 using TKIP and CCMP

Wi-Fi Protected Access (WPA) is a robust 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.

WPA's 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. WPA also provides strong user authentication based on 802.1x EAP.

WPA2 is a newer 802.11i standard that provides even stronger wireless security than 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.

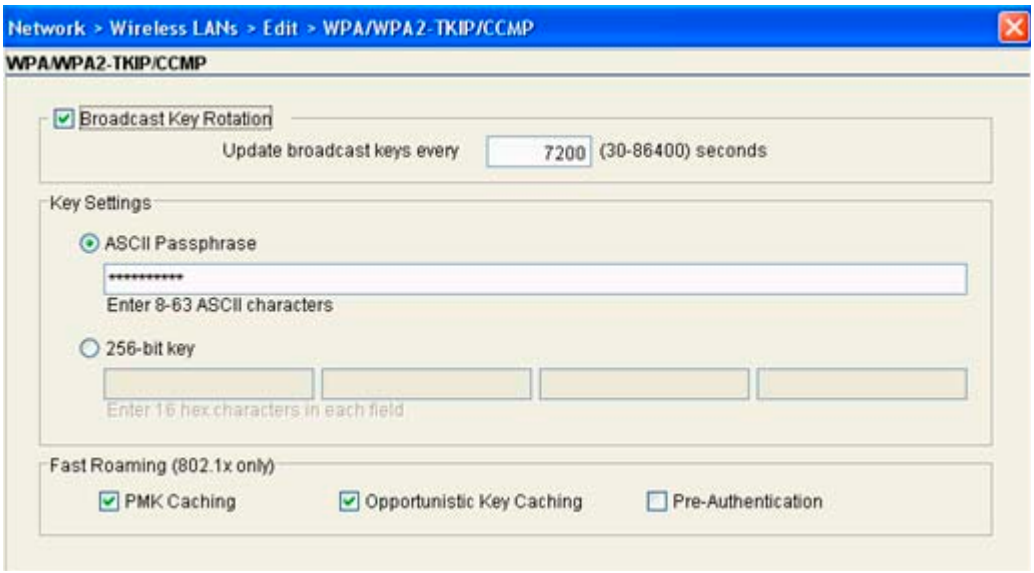
WPA2-CCMP is based on the concept of a *Robust Security Network* (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any the switch provides.

To configure WPA/WPA2-TKIP/CCMP encryption:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.

   A WLAN screen displays with the WLAN's existing configuration. Refer to the **Authentication** and **Encryption** columns to assess the WLAN's existing security configuration.
3. Select either the **WPA/WPA2-TKIP** or **WPA2-CCMP** button from within the Encryption field.
4. Click the **Config** button to the right of the WPA/WPA2-TKIP and WPA2-CCMP checkboxes.

   The **WPA/WPA2-TKIP/CCMP** screen displays. This single screen can be used to configure either WPA/WPA2-TKIP or WPA-CCMP.



5. Select the **Broadcast Key Rotation** checkbox to enable periodically changing the broadcast key for this WLAN.

   Only broadcast key changes when required by associated MUs to reduce the transmissions of sensitive key information. This value is enabled by default.

6. Refer to the **Update broadcast keys every** field to specify a time period (in seconds) for broadcasting encryption-key changes to MUs.

   Set key broadcasts to a shorter interval (at least 60 seconds) for tighter security on wireless connections. Set key broadcasts to a longer interval (at most, 86400 seconds) to extend key times for wireless connections. The default is 7200 seconds.

7. Configure the **Key Settings** field as needed to set an ASCII Passphrase and key values.

ASCII Passphrase	To use an ASCII passphrase (and not a hexadecimal value), select the checkbox and enter an alphanumeric string of 8 to 63 characters. The alphanumeric string allows character spaces. The switch converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.
256-bit Key	To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.

NOTE: The Web UI does not support saving passphrases in encrypted format. To save passphrases in an encrypted format, configure the passphrases using the Command Line Interface. Refer to the CLI Reference Guide for details on configuring passphrases using the CLI.

Default (hexadecimal) 256-bit keys for WPA/TKIP include:

- *1011121314151617*
- *18191A1B1C1D1E1F*
- *2021222324252627*
- *28292A2B2C2D2E2F*

8. Optionally select one of the following from within the **Fast Roaming (8021x only)** field.

PMK Caching	Select *Pairwise Master Key* (PMK) caching to store Pairwise Master Key derived from 802.1x authentication between a client device and its authenticator. When a client roams between devices, the client's credentials no longer need to completely reauthenticated (a process that can take up to 100 milliseconds). In the instance of a voice session, the connection would likely be terminated if not using a PMK. PMK cache entries are stored for a finite amount of time, as configured on the wireless client.

Opportunistic Key Caching	**Opportunistic Key Caching** allows the switch to use a PMK derived with a client on one Access Port with the same client when it roams over to another Access Port. Upon roaming, the client does not have to conduct 802.1x authentication and can start sending/receiving data sooner.
Pre-Authentication	Selecting the **Pre-Authentication** option enables an associated MU to carry out an 802.1x authentication with another switch (or device) before it roams to it. This enables the roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. This is only supported when 802.1x EAP authentication is enabled.

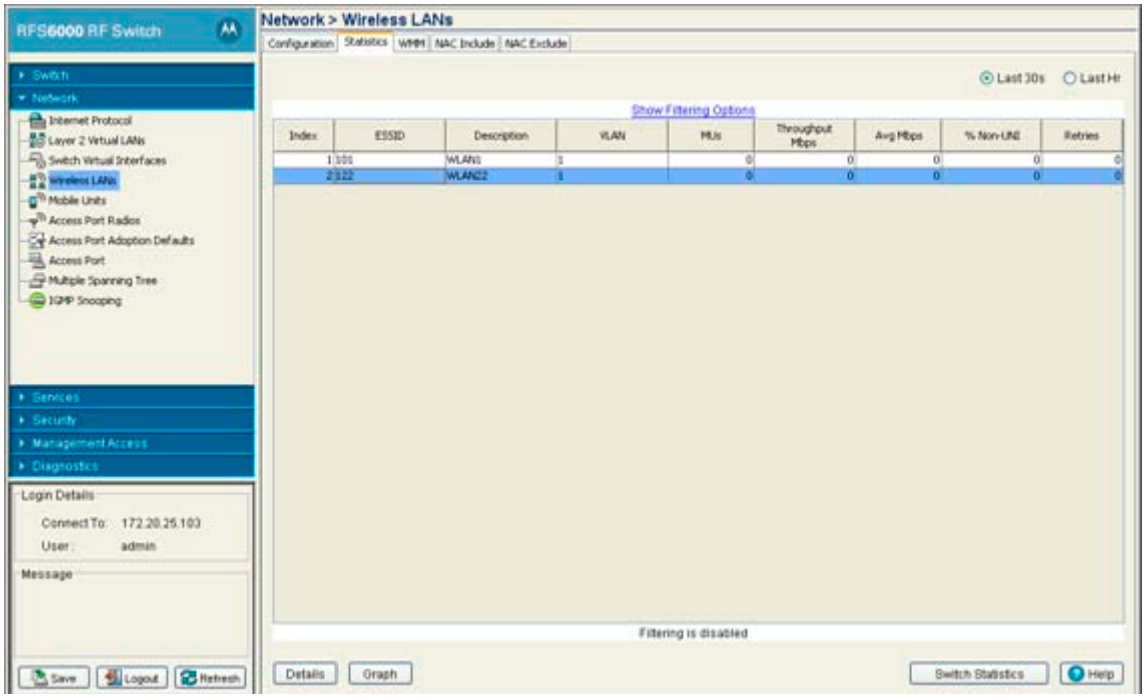
9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.2 Viewing WLAN Statistics

The **Statistics** screen displays read-only statistics for each WLAN. Use this information to assess if configuration changes are required to improve network performance. If a more detailed set of WLAN statistics is required, select a WLAN from the table and click the **Details** button.

To view WLAN configuration details:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Click the **Statistics** tab.



3. Refer to the following details displayed within the table:

Last 30s	Click the Last 30s radio button to display statistics for the WLAN over the last 30 seconds. This option is helpful when troubleshooting issues as they actually occur.
Last Hr	Click the Last Hr radio button to displays statistics for the WLAN over the last 1 hour. This metric is helpful in baselining events over a one hour interval.
Index	The Idx (or index) is a numerical identifier used to differentiate the WLAN from other WLANs that may have similar characteristics.
ESSID	The SSID is the *Service Set ID* (SSID) for the selected WLAN.
Description	The Descr item contains a brief description of the WLAN. Use the description (along with the index) to differentiate the WLAN from others with similar attributes.
VLAN	The VLAN parameter displays the name of the VLAN the WLAN is associated with.
MUs	Lists the number of MUs associated with the WLAN.
Throughput Mbps	Throughput Mbps is the average throughput in Mbps on the selected WLAN. The Rx value is the average throughput in Mbps for packets received on the selected WLAN. The Tx value is the average throughput for packets sent on the selected WLAN.
Avg BPS	Displays the average bit speed in Mbps for the selected WLAN. This includes all packets sent and received.
% Non-UNI	Displays the percentage of the total packets for the selected WLAN that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the average number of retries for all MUs associated with the selected WLAN.

4. To view WLAN statistics in greater detail, select a WLAN and click the **Statistics** button. For more information, see *Viewing WLAN Statistics in Detail on page 4-62*.

NOTE: When using mesh enabled WLAN statistics, no statistics are shown. This is because WLAN statistics are generated by mobile unit traffic for that particular WLAN. In a mesh configuration, there are typically no mobile units associated and therefore no statistical information to display.

5. To view WLAN statistics in a graphical format, select a WLAN and click the **Graph** button. For more information, see *Viewing WLAN Statistics in a Graphical Format on page 4-65*.
6. To view WLAN packet data rates and retry counts, select a WLAN and click the **Switch Statistics** button. For more information, see *Viewing WLAN Switch Statistics on page 4-66*.

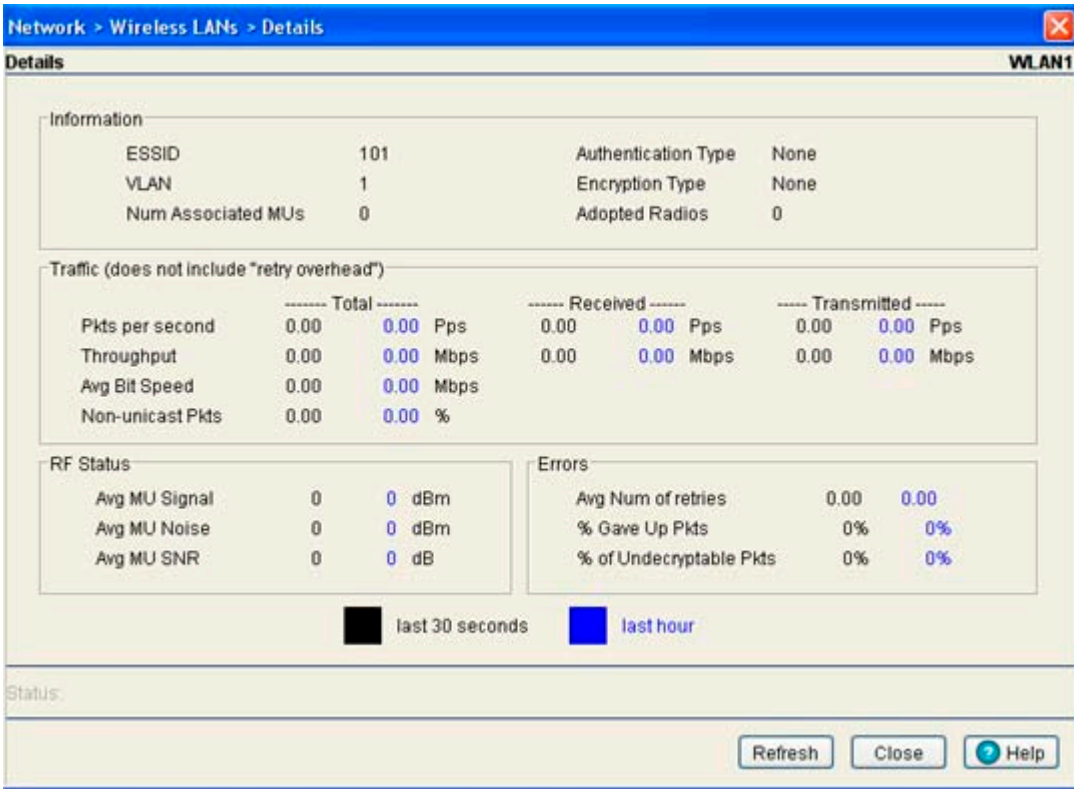
4.5.2.1 Viewing WLAN Statistics in Detail

When the WLAN Statistics screen does not supply adequate information for an individual WLAN, the **Details** screen is recommended for displaying more granular information for a single WLAN. Use this information to discern if a WLAN requires modification to meet network expectations.

To view detailed statistics for a WLAN:

1. Select a **Network** > **Wireless LANs** from the main menu tree.
2. Click the **Statistics** tab.

3. Select a WLAN from the table displayed in the Statistics screen. and click the **Details** button.



The Details screen displays the WLAN statistics of the selected WLAN. The Details screen contains the following fields:

- *Information*
- *Traffic*
- *RF Status*
- *Errors*

Information in **black** represents the statistics from the last 30 seconds and information in **blue** represents statistics from the last hour.

4. Refer to the **Information** field for the following information:

ESSID	Displays the *Service Set ID* (SSID) for the selected WLAN.
VLAN	Displays the name of the VLAN the WLAN is associated with.
Num Associated MUs	Displays the total number of MUs currently associated with the selected WLAN.
Authentication Type	Displays the authentication method deployed on the WLAN.
Encryption Type	Displays the encryption type deployed on the selected WLAN.
Adopted Radios	Displays the radios adopted by the selected WLAN.

5. Refer to the **Traffic** field for the following information (both received and transmitted):

Pkts per second	Displays the average total packets per second that cross the selected WLAN. The Rx column displays the average total packets per second received on the selected WLAN. The Tx column displays the average total packets per second sent on the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Throughput	Displays the average throughput in Mbps on the selected WLAN. The Rx column displays the average throughput in Mbps for packets received on the selected WLAN. The Tx column displays the average throughput for packets sent on the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Avg Bit Speed	Displays the average bit speed in Mbps on the selected WLAN. This includes all packets sent and received. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Non-unicast Pkts	Displays the percentage of the total packets for the selected WLAN that are non-unicast. Non-unicast packets include broadcast and multicast packets. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

6. Refer to the **RF Status** field for the following information:

Avg MU Signal	Displays the average RF signal strength in dBm for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Avg MU Noise	Displays the average RF noise for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Avg MU SNR	Displays the average *Signal to Noise Ratio* (SNR) for all MUs associated with the selected WLAN. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

7. Refer to the **Errors** field for the following information:

Average Number of Retries	Displays the average number of retries for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
% Gave Up Pkts	Displays the percentage of packets the switch gave up on for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
% Non-decryptable Pkts	Displays the percentage of undecryptable packets for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

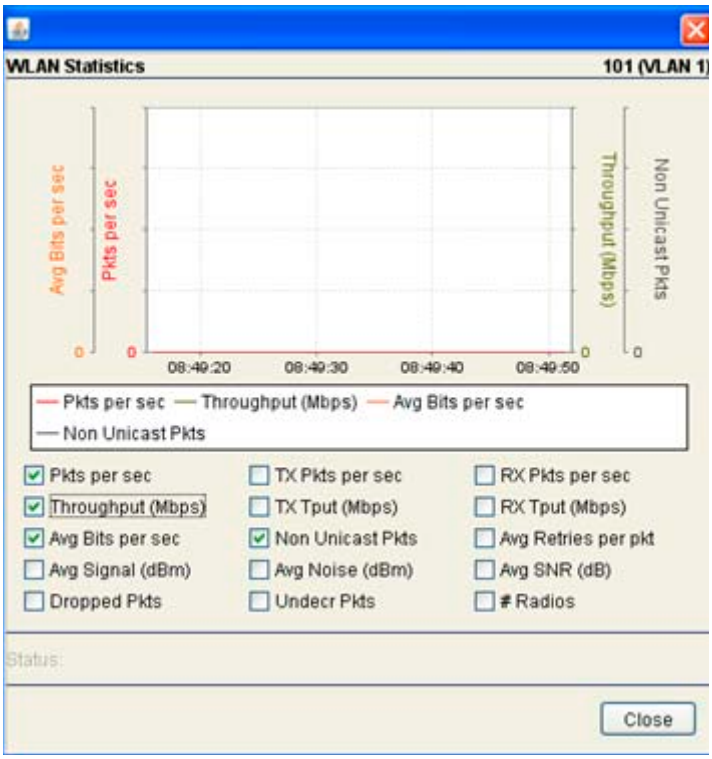
8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.2.2 Viewing WLAN Statistics in a Graphical Format

The switch Web UI continuously collects WLAN statistics even when the graph is not displayed. Periodically display the WLAN statistics graph for the latest WLAN throughput and performance information.

To view detailed graphical statistics for a WLAN:

1. Select a WLAN from the table displayed in the **Statistics** screen.
2. Click the **Graph** button.



The WLAN Statistics screen displays for the select port. The WLAN Statistics screen provides the option of viewing the graphical statistics of the following parameters:

- *Pkts per sec*
- *Throughput (Mbps)*
- *Avg Bits per sec*
- *Avg Signal (dBm)*
- *Dropped Pkts*
- *TX Pkts per sec*
- *TX Tput (Mbps)*
- *NUcast Pkts*
- *Avg Noise (dBm)*
- *Undecr Pkts*
- *RXPkts per sec*
- *RX Tput (Mbps)*

- *Avg Retries*
- *Avg SNR (dB)*
- *# Radios*

NOTE: You cannot select (and trend) more than four parameters at any given time.

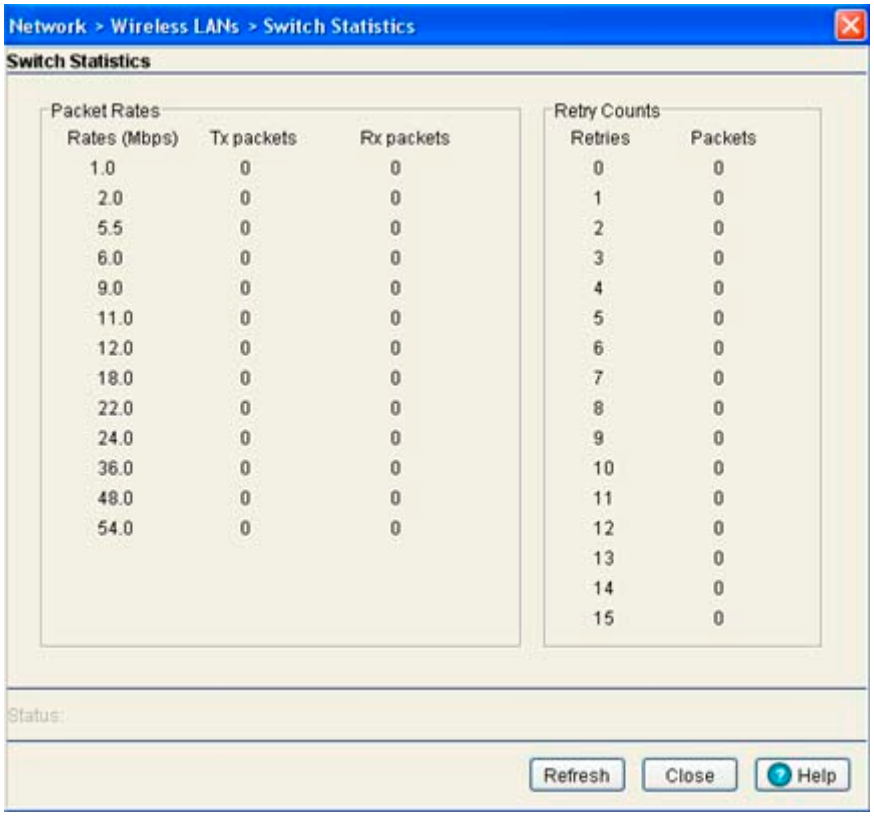
3. Select any of the above listed parameters by clicking on the checkbox associated with it.
4. Click the **Close** button to exit the screen.

4.5.2.3 Viewing WLAN Switch Statistics

The **Switch Statistics** screen displays the sum of all WLAN statistics. The Switch Statistics screen is optimal for displaying a snapshot of overall WLAN traffic on your switch.

To view detailed statistics for a WLAN:

1. Select a **Network** > **Wireless LANs** from the main menu tree.
2. Click the **Statistics** tab.
3. Select a WLAN from the table displayed in the Statistics screen and click the **Switch Statistics** button.



4. Refer to the **Packet Rates** field to review the number of packets both transmitted (Tx) and received (Rx) at data rates from 1.0 to 54.0 Mbps. If a large number of packets are sent and received at a slower data

rate, then perhaps the switch is not adequately positioned or configured to support the MUs within that WLAN.

NOTE: The *Motorola RF Management Software* is recommended to plan the deployment of the switch. Motorola RFMS can help optimize the positioning and configuration of a switch in respect to a WLAN's MU throughput requirements. For more information, refer to the Motorola Web site.

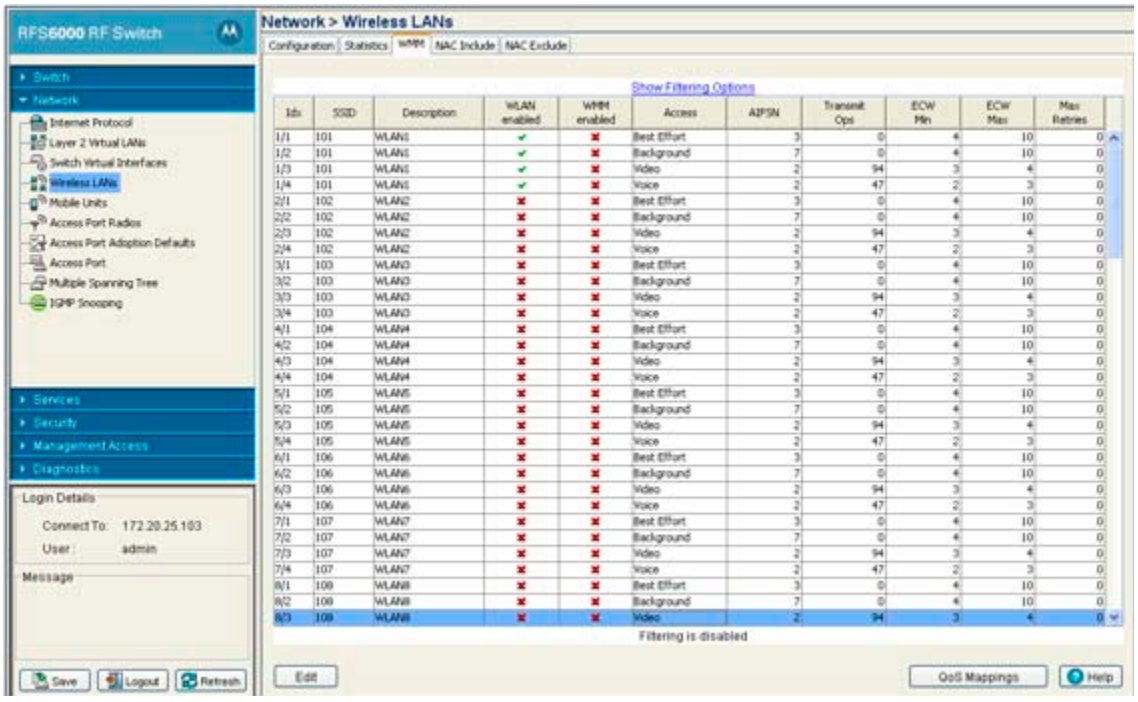
5. Refer to the **Retry Counts** field to review the number packets requiring retransmission from the switch.
6. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **Refresh** to update the Packet Rate and Retry Count data displayed within the screen.
8. Click **Close** to close the dialog and re turn to the Network > Wireless LANs > Statistics screen.

4.5.3 Configuring WMM

Use the **WMM** tab to review a WLAN's current index (numerical identifier), SSID, description, current enabled/disabled designation, and Access Category.

To view existing WMM Settings:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Click the **WMM** tab.

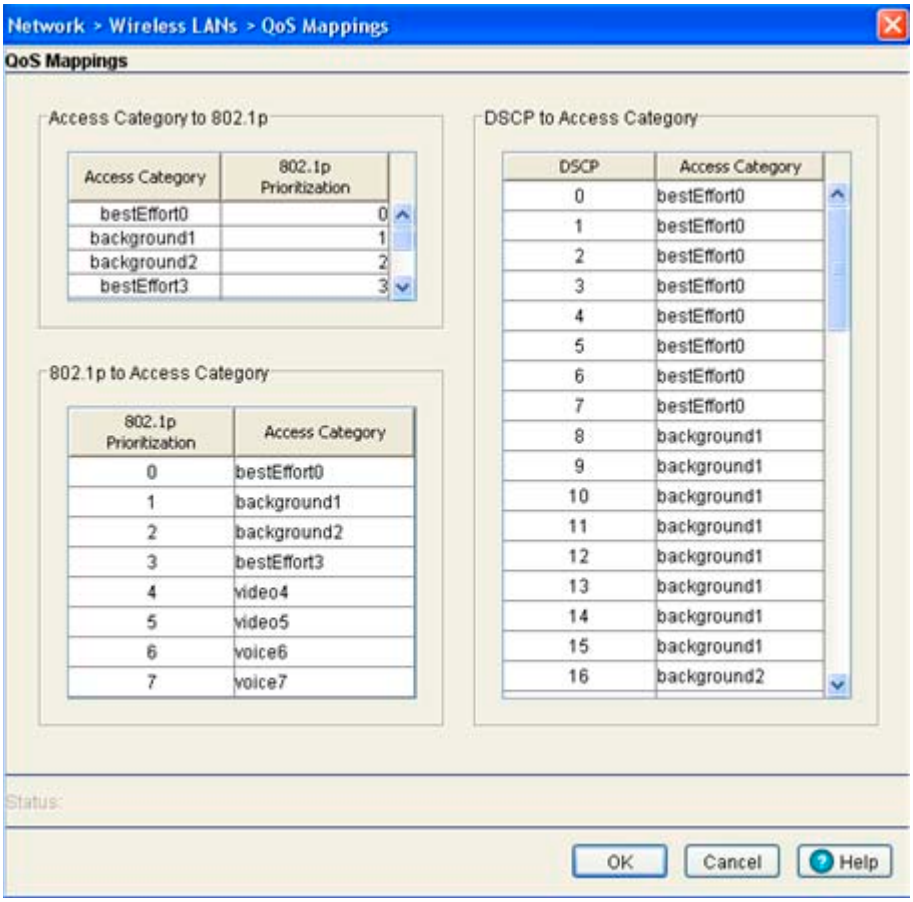


The **WMM** tab displays the following information:

Idx	Displays the WLANs numerical identifier. This field is displayed in a two part format. The first number is the WLAN index and the second number is a sub-index corresponding to the access category. Click the Edit button to modify this property.
SSID	Displays the Service Set ID (SSID) associated with each WLAN.

Description	Displays a brief description of the WLAN.
WLAN enabled	Displays the status of the WLAN. A Green check defines the WLAN as enabled and a Red "X" means it is disabled. The enable/disable setting can be defined using the WLAN Configuration screen.
WMM enabled	Displays WLAN-WMM status. It can be enabled (for a WLAN) from the WLAN Configurations Edit screen by selecting the Enable WMM checkbox.
Access	Displays the Access Category for the intended radio traffic. Access Categories are the different WLAN-WMM options available. The four Access Category types are: • *Background* — Optimized for background traffic • *Best-effort* — Optimized for best effort traffic • *Video* — Optimized for video traffic • *Voice* — Optimized for voice traffic
AIFSN	Displays the current *Arbitrary Inter-frame Space Number* (AIFSN). Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will causes lower-priority traffic to wait longer before trying attempting access.
Transmit Ops	Displays 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.
ECW Min	The ECW Min is combined with the ECW Max to make the Contention screen. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
ECW Max	The ECW Max is combined with the ECW Min to make the Contention screen. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
Max Retries	Displays the maximum number of retries for each WMM index.

3. Click the **Edit** button to display a screen used to modify the WMM parameters. For more information, see *Editing WMM Settings on page 4-70*.
4. Select the **QoS Mappings** button to revise the existing mappings of access category to 802.1p and DSCP to access category settings.



With a drastic increase in bandwidth absorbing network traffic (VOIP, multimedia etc.), the importance of data prioritization is critical to effective network management.

Refer to the following fields within the QoS Mapping screen to optionally revise the existing settings to in respect to the data traffic requirements for this WLAN.

Access Category to 802.1p — Optionally revise the **802.1p Prioritization** for each access category to prioritize the network traffic expected on this WLAN.

802.1p to Access Category — Set the access category accordingly in respect to its importance for this WLAN's target network traffic.

DSCP to Access Category — Set the access category accordingly in respect to its DSCP importance for this WLAN's target network traffic.

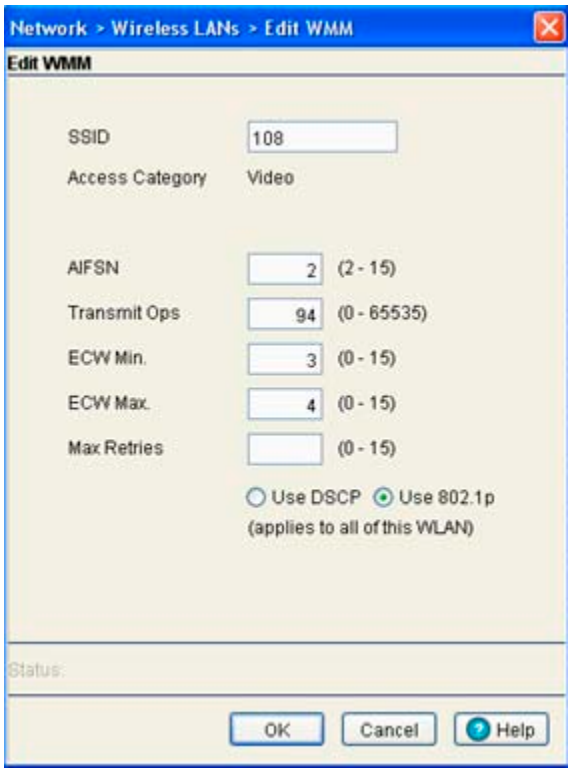
Differentiated Services Code Point (DSCP) is a field in an IP packet that enables different levels of service to be assigned to network traffic. This is achieved by marking each packet on the network with a DSCP code and appropriating to it the corresponding level of service or priority. QoS enabled programs request a specific service type for a traffic flow through the *generic QoS* (GQoS) *application programming interface* (API).

4.5.3.1 Editing WMM Settings

WLAN WMM configuration affects your upstream traffic parameters. Use *Configuring WMM on page 4-110* to configure downstream traffic parameters. Use the WMM Edit screen to modify existing Access Category settings for the WLAN selected within the WMM screen. This could be necessary in instances when data traffic has changed and high-priority traffic (video and voice) must be accounted for by modifying AIFSN Transmit Ops and CW values.

To edit existing WMM Settings:

1. Select **Network Setup** > **WLAN Setup** from the main menu tree.
2. Click the **WMM** tab.
3. Select a Access Category from the table and click the **Edit** button to launch a dialog with WMM configuration for that radio.



4. Refer to the **Edit WMM** screen for the following information:

SSID	Displays the *Service Set ID* (SSID) associated with the selected WMM index. This SSID is read-only and cannot be modified within this screen.
Access Category	Displays the Access Category for the intended radio traffic. The Access Categories are the different WLAN-WMM options available to the radio. The four Access Category types are: • *Background* - Optimized for background traffic • *Best-effort* - Optimized for best effort traffic • *Video* - Optimized for video traffic. Video traffic receives priority. • *Voice* - Optimized for voice traffic. Voice traffic receives priority.

AIFSN	Define the current *Arbitrary Inter-frame Space Number* (AIFSN). Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will causes lower-priority traffic to wait longer before trying to access the medium.
Transmit Ops	Define 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.
ECW Minimum	The ECW Minimum is combined with the ECW Maximum to make the Contention screen. From this range, a random number is selected for the back off mechanism. Select a lower value for high priority traffic.
ECW Maximum	The ECW Maximum is combined with the ECW Minimum to make the Contention screen. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic
Max Retries	Define a maximum number of retries for each Access Category.
Use DSCP or 802.1p	Select the DSCP or 802.1p radio buttons to choose between DSCP and 802.1p.

5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.4 Configuring the NAC Inclusion List

Using NAC, the switch acts as an enforcement entity before allowing MU access to specific network resources. NAC performs a MU host integrity check wherein a MU sends host integrity information to the NAC server. The NAC server configuration is defined on the switch on a per WLAN basis. NAC verifies a MU's compliance with the NAC server's security policy (not the switch).

For a NAC configuration example using the switch CLI, see *NAC Configuration Examples Using the Switch CLI on page 4-78*.

An include list is a list of MAC addresses configured for a WLAN. During EAP authentication, the EAP server (Radius or NAC server) is determined based on the MU's MAC address.

- All non-802.1x devices are partitioned into a WLAN (separate from a 802.1x enabled WLAN).
- Communication between devices in a 802.1x supported WLAN and a non 802.1x supported WLAN is achieved by merging the WLANs within the same VLAN.

The switch uses the include list to add devices that are NAC supported. The following explains how authentication is achieved using 802.1x. The switch authenticates 802.1x enabled devices using one of the following:

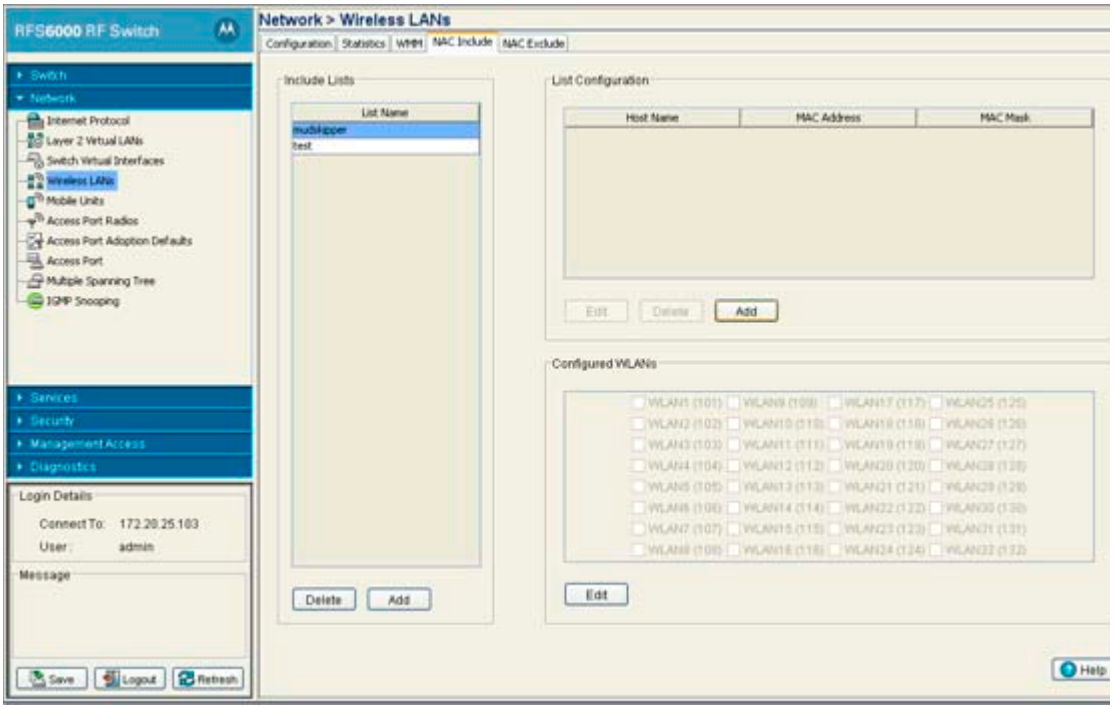
- *NAC Agent* – NAC support is added in the switch to allow the switch to communicate with a LAN enforcer (a laptop with a NAC agent installed).
- *No NAC Agent* – NAC support is achieved using an exclude list. For more information, see *Configuring the NAC Exclusion List on page 4-75*.

By default, a WLAN is NAC disabled. Each WLAN can be configured to:

- Conduct a NAC check for MU's connecting to the WLAN as well as perform an additional exclude function, by attaching an exclude list to the WLAN.
- Do not perform NAC validation for MUs connecting to the WLAN.
- Include a few MU's for NAC validation and bypass the rest of the MU's.

To view the attributes of a NAC Include list:

1. Select **Network > Wireless LANs** from the main menu tree.
2. Select the **NAC Include List Configuration** tab to view and configure NAC enabled devices.



3. The **Include Lists** field displays the list of devices that can be included on a WLAN (a printer for example).

   Use the **Add** button to add a device for configuration on a WLAN. A maximum of 6 MAC addressees are allowed per device. For more information, see *Adding an Include List to a WLAN on page 4-73*.

   The **List Configuration** field displays a list of MAC addresses that can be included on a WLAN. You can add more than one device in this list. For example, printer 1, printer 2 etc.

4. Use the **Add** button (within the **List Configuration** field) to add more than one device to the WLAN. You can create 32 lists (both include and exclude combined together) and 64 MAC entries per list. For more information, see *Configuring Devices on the Include List on page 4-73*.
5. The **Configured WLANs** field displays available WLANs. Associate a list item (within the Include Lists field) with as many WLANs as required.

   For information on mapping NAC Include list items with WLANs, see *Mapping Include List Items to WLANs on page 4-74*.

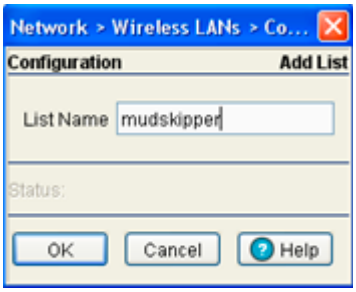
6. To delete a device (and its configuration), select it from the **Include Lists** and click the **Delete** button
7. Use the **Edit** button in the **List Configuration** section to modify the devices parameters.

8. To delete any list configuration for a particular device, select the row from the **List Configuration** section and click on the **Delete** button.

4.5.4.1 Adding an Include List to a WLAN

To add a device to a WLAN's include list configuration:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select the **NAC Include** tab to view and configure NAC Include enabled devices.
3. Click on the **Add** button in the **Include Lists** area.



4. Enter the name of the device to include for NAC authentication.
5. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to save the new configuration and close the dialog window.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.4.2 Configuring Devices on the Include List

To add a multiple number of devices for a single device type:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select the **NAC Include** tab to view and configure all the NAC Include enabled devices.
3. Click on the **Add** button within the **List Configuration** area.

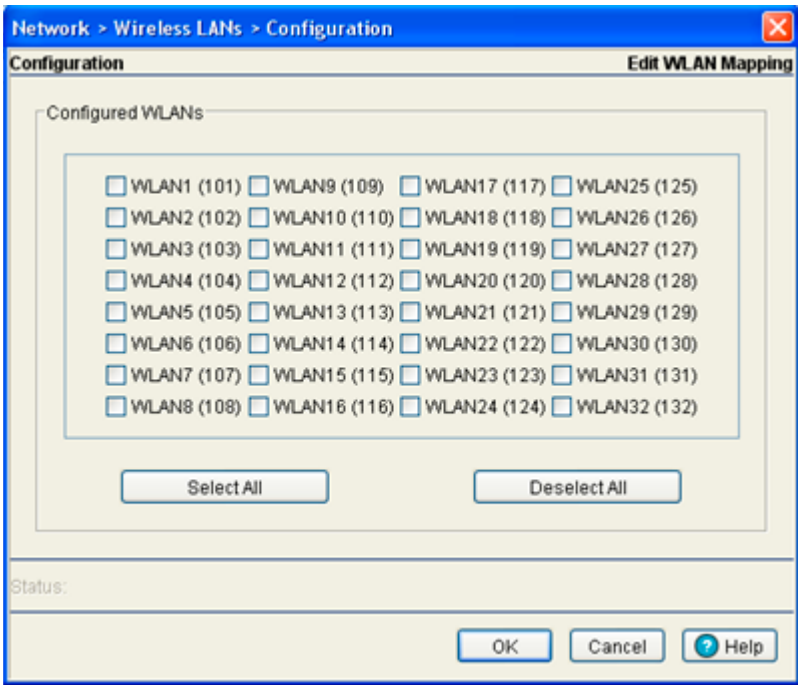
The **List Name** field displays the name of the device list used. This parameter is read-only.

4. Enter the **Host Name** for the device you wish to add.
5. Enter a valid **MAC Address** of the device you wish to add.
6. Optionally, enter the **MAC Mask** for the device you wish to add.
7. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to save and add the new configuration and close the dialog window.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.4.3 Mapping Include List Items to WLANs

To assign include list items to a one or more WLANs:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select the **NAC Include** tab to view NAC Included devices.
3. Select an item from the Include List's **List Name** field and click the **Edit** button (within the **Configured WLANs** field).



4. Map the selected list item with as many WLANs as needed (be selecting the WLAN's checkbox). Use the **Select All** button to associate each WLAN with the selected list item.
5. To remove the WLAN Mappings, select the **Deselect All** button to clear the mappings.
6. Refer to the **Status** field for a display of the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to save and add the new configuration and close the dialog window.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.5 Configuring the NAC Exclusion List

The switch provides a means to bypass NAC for 802.1x devices without a NAC agent. For Motorola handheld devices (like the MC9000), authentication is achieved using an exclusion list.

A list of MAC addresses (called an exclusion list) can be added to each WLAN. Each has a separate configuration for the Radius server (which only conducts EAP authentication). An exclusion list is a global index-based configuration. An exclusion list can be configured and associated to any WLAN.

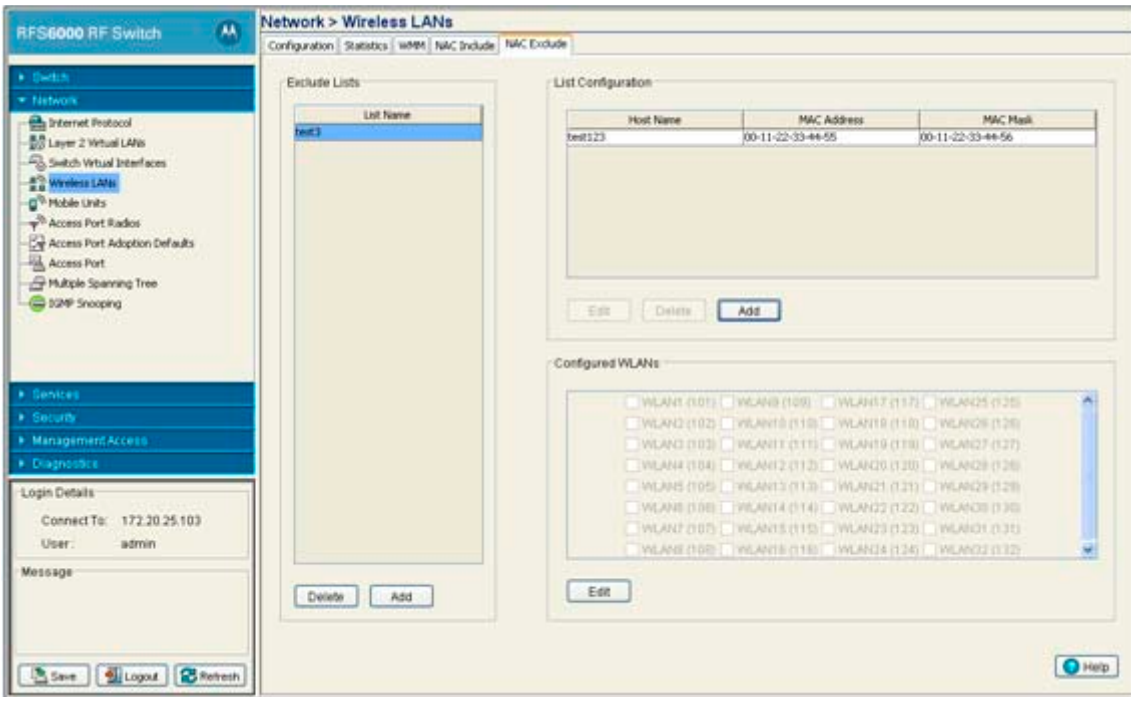
If a device's MAC address is not present in an exclusion list, it will go through the NAC server (LAN enforcer) and thereby a 802.1x host integrity check. For every WLAN configuration, there are two separate EAP servers (Radius and NAC).

Whenever a host entry is added or deleted from/to the list, the associated WLAN is updated and deauthenticated. The de-authenticated MU can be re-authenticated once it receives the de-authentication information from the WLAN.

For a NAC configuration example using the switch CLI, see *NAC Configuration Examples Using the Switch CLI on page 4-78*.

To view the attributes of a NAC exclusion list:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select the **NAC Exclude** tab to view and configure all the NAC include enabled devices.



The **Exclude Lists** field displays a list of devices that can be excluded from a WLAN.

3. Use the **Add** button to add a device that can be excluded on a WLAN. For more information, see *Adding an Exclude List to the WLAN on page 4-76*.

   The **List Configuration** field displays a list of MAC addresses that can be excluded from a WLAN. You can add more than one device to this list.

4. Use the **Add** button (within the **List Configuration field)** to add devices excluded from NAC compliance on a WLAN. You can create up to 32 lists (both include and exclude combined together) and 64 MAC

entries maximum per list. For more information, see *Configuring Devices on the Exclude List on page 4-76*.

5. The **Configured WLANs** field displays the available switch WLANs. Associate a list item in the Exclude Lists field with multiple WLANs.

   For information on mapping NAC Exclude list's items to WLANs, see *Mapping Exclude List Items to WLANs on page 4-77*.

6. To delete a device, select a device from the **Exclude List** and click the **Delete** button.
7. Use the **Edit** button to modify devices parameters.
8. To delete a list configuration for a device, select a row from the **List Configuration** field and click the **Delete** button.

4.5.5.1 Adding an Exclude List to the WLAN

To exclude a device from a WLAN:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select the **NAC Exclude** tab to view NAC exclude devices.
3. Click on the **Add** button in the **Exclude Lists** field.

4. Enter the name of the device that you wish to exclude for NAC authentication.
5. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to save and add the new configuration and close the dialog window.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.5.2 Configuring Devices on the Exclude List

To add more than one device for a particular type of device in the include list:

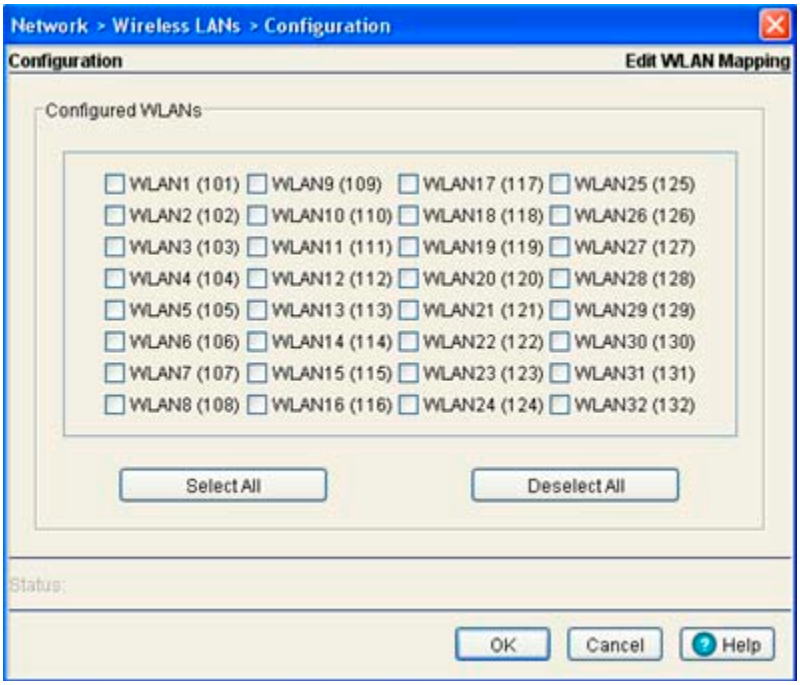
1. Select **Network > Wireless LANs** from the main menu tree.
2. Select the **NAC Exclude** tab to view and configure all the NAC exclude devices.
3. Click on the **Add** button in the **List Configuration** field.

4. The **List Name** displays the read-only name of the list for which you wish to add more devices.
5. Enter the **Host Name** for the device you wish to add for the selected exclude list.
6. Enter a valid **MAC Address** for the device you wish to add.
7. Optionally, enter the **MAC Mask** for the device you wish to add.
8. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to save and add the new configuration and close the dialog window.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.5.3 Mapping Exclude List Items to WLANs

To assign exclude list items to a one or more WLANs:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Select the **NAC Exclude** tab to view NAC excluded devices.
3. Select a item from the Exclude List's **List Name** field and click the **Edit** button (within the **Configured WLANs** field).



4. Map the selected list item with as many WLANs as needed (be selecting the WLAN's checkbox). Use the **Select All** button to associate each WLAN with the selected list item.
5. To remove the WLAN Mappings, select the **Deselect All** button to clear the mappings.
6. Refer to the **Status** field for a display of the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to save and add the new configuration and close the dialog window.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.5.6 NAC Configuration Examples Using the Switch CLI

The following are NAC include list, exclude list and WLAN configuration examples using the switch CLI interface:

4.5.6.1 Creating an Include List

Since few devices require NAC, Motorola recommends using the "bypass-nac-except-include-list" option. Refer to the commands below to create a NAC Include List:

1. Create a NAC include list.

   RF Switch (config-wireless) #client include-list Desktop

   RF Switch (config-wireless-client-list) #

NOTE: The instance changes from `(config-wireless)` to `(config-wireless-client-list)`.

2. Add a host entry to the include list. This adds a specified MAC entry/MAC range into the client's include list.

   RF Switch(config-wireless-client-list) #station pc1 AA:BB:CC:DD:EE:FF

   RF Switch(config-wireless-client-list) #

3. Associate the include list to a WLAN. This adds the client's include list into the WLAN.

   RF Switch(config-wireless-client-list) #wlan 1

   RF Switch(config-wireless-client-list) #

4.5.6.2 Creating an Exclude List

To create a NAC Exclude List:

1. Define the NAC include list.

   RF Switch(config-wireless) #client exclude-list Desktop

   RF Switch(config-wireless-client-list) #

2. Add a host entry into the exclude list.

   RF Switch(config-wireless-client-list) #station pc10 AB:BC:CD:DE:EF:FA

   RF Switch(config-wireless-client-list) #

3. Associate the exclude list to a WLAN.

   RF Switch(config-wireless-client-list) #wlan 1

   RF Switch(config-wireless-client-list) #

4.5.6.3 Configuring the WLAN for NAC

Many handheld devices are required to bypass NAC and a few laptops and desktops are required to be NAC validated.

1. Set the NAC mode for WLAN. A NAC validation is conducted for station entries in the include list. The station entries are authenticated using the Radius server.

   RF Switch(config-wireless) #wlan 1 nac-mode bypass-nac-except-include-list

   RF Switch (config-wireless) #

2. Configure the WLAN's NAC server settings.

   a. Configure the NAC Server's IP address.

      RF Switch(config-wireless) #wlan 1 nac-server primary 192.168.1.10

      RF Switch(config-wireless) #

   b. Configure the NAC Server's Radius Key.

      RF Switch(config-wireless) #wlan 1 nac-server primary radius-key my-secret

      RF Switch(config-wireless) #

NOTE: Configure the secondary NAC server for redundancy.

   c. Configure the secondary NAC server's IP address.

RF Switch(config-wireless) #wlan 1 nac-server secondary 192.168.1.20

RF Switch(config-wireless) #

d. Configure the secondary NAC Server's Radius Key.

RF Switch(config-wireless) #wlan 1 nac-server secondary radius-key my secret-2

RF Switch(config-wireless) #

3. MUs not NAC authenticated use Radius for authentication. To configure the WLAN's Radius settings:

a. Configure the Radius server's IP address.

RF Switch(config-wireless) #wlan 1 radius-server primary 192.168.1.30

RF Switch(config-wireless) #

b. Configure the server's Radius Key

RF Switch(config-wireless) #wlan 1 radius-server primary radius-key my-rad-secret

RF Switch(config-wireless)#

c. Configure the secondary Radius server's IP address.

RF Switch(config-wireless) #wlan 1 radius-server secondary 192.168.1.40

RF Switch(config-wireless) #

d. Configure the secondary server's Radius Key.

RF Switch (config-wireless) #wlan 1 radius-server secondary radius-key my-rad-secret-2

RF Switch (config-wireless) #

4. Configure the NAC server's timeout and re-transmit settings. The timeout parameter configures the duration for which the switch waits for a response from the Radius server before attempting a retry. This is a global setting for both the primary and secondary server.

   The re-transmit parameter defines the number of retries a switch attempts before dis-associating the MU.

   RF Switch(config-wireless) #wlan 1 nac-server timeout 30 retransmit 10

   RF Switch(config-wireless) #

5. Configure WLAN for EAP authentication and define the encryption type.

   RF Switch(config-wireless) #wlan 1 authentication-type eap

   RF Switch(config-wireless) #wlan 1 encryption-type wep128

   RF Switch(config-wireless) #wlan 1 ssid wlan-1

4.6 Viewing Associated MU Details

The **Mobile Units** screen displays read-only device information for MUs interoperating with the switch managed network. The **Mobile Units** screen consists of the following tabs:

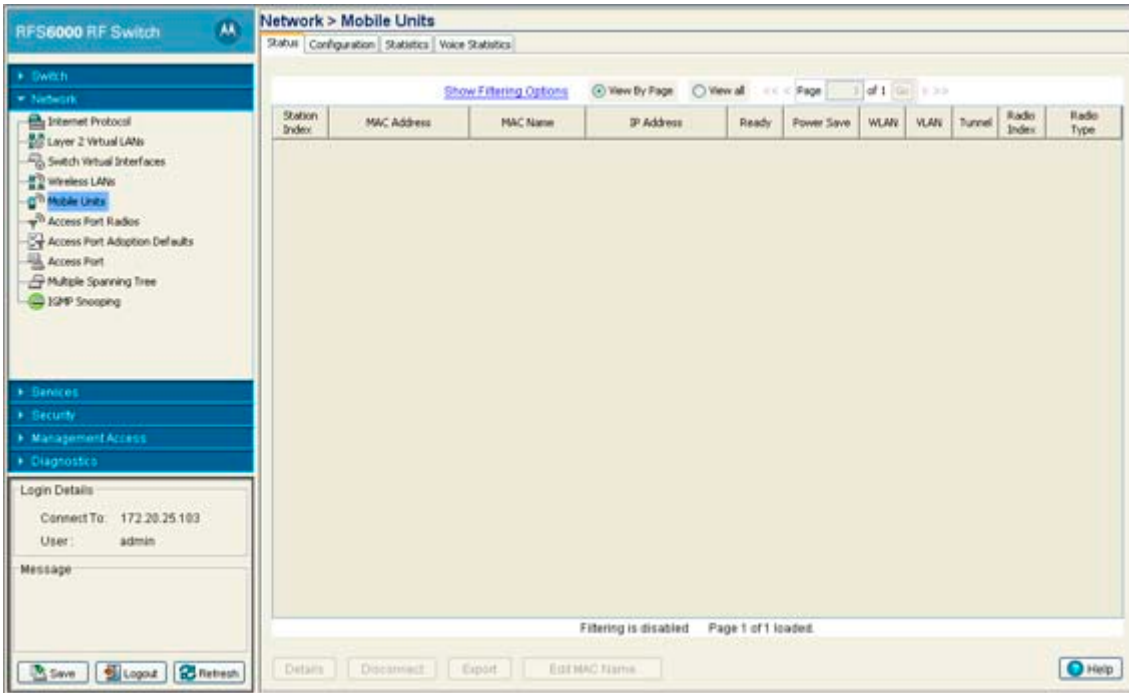
- *Viewing MU Status*
- *Configuring Mobile Units*
- *Viewing MU Statistics*
- *Viewing Voice Statistics*

NOTE: The *Motorola RF Management Software* is a recommended utility to plan the deployment of the switch and view its configuration once operational. Motorola RFMS can help optimize switch positioning and configuration in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Motorola Web site.

4.6.1 Viewing MU Status

To view MU Status is detail:

1. Select **Network** > **Mobile Units** from the main menu tree.
2. Click the **Status** tab.



The Status screen displays the following read-only device information for MUs interoperating within the switch managed network.

Station Index	Displays a numerical device recognition identifier for a specific MU.
MAC Address	Each MU has a unique *Media Access Control* (MAC) address through which it is identified. This address is burned into the ROM of the MU.

MAC Name	Displays the MAC name associated with each MU's MAC Address. The MAC Name is a user created name used to identify individual mobile unit MAC Addresses with a user friendly name.
IP Address	Displays the unique IP address for the MU. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
Ready	Displays whether the MU is ready for switch interoperation. Values are Yes and No.
Power Save	Displays the current (read-only) *Power-Save-Poll* (PSP) state of the MU. The Power Save field has two potential settings. PSP indicates the MU is operating in Power Save Protocol mode. In PSP, the MU runs enough power to check for beacons and is otherwise inactive. CAM indicates the MU is continuously aware of all radio traffic. CAM is recommended for MUs frequently transmitting with the switch's Access Ports for periods of two hours or greater.
WLAN	Displays the name of the WLAN the MU's associated AP is connect to.
VLAN	Displays the specific VLAN the target MU is mapped to.
Tunnel	Displays the tunnel the target MU is mapped to.
Radio Index	The Radio Index is a numerical device recognition identifier for MU radios. The index is helpful to differentiate device radios when a particular MU has more than one radio.
Radio Type	The Radio Type defines the radio used by the adopted MU. The switch supports 802.11b MUs and 802.11 a/b and 802.11 a/g dual-radio MUs. The radio also supports 802.11a only and 802.11g MUs.

3. Click the **Details** button to launch a screen with additional information about the selected MU. For more information, see *Viewing MU Details on page 4-82*
4. Highlight a MU from those listed and click the **Disconnect** button to remove the MU from the list of currently associated devices.

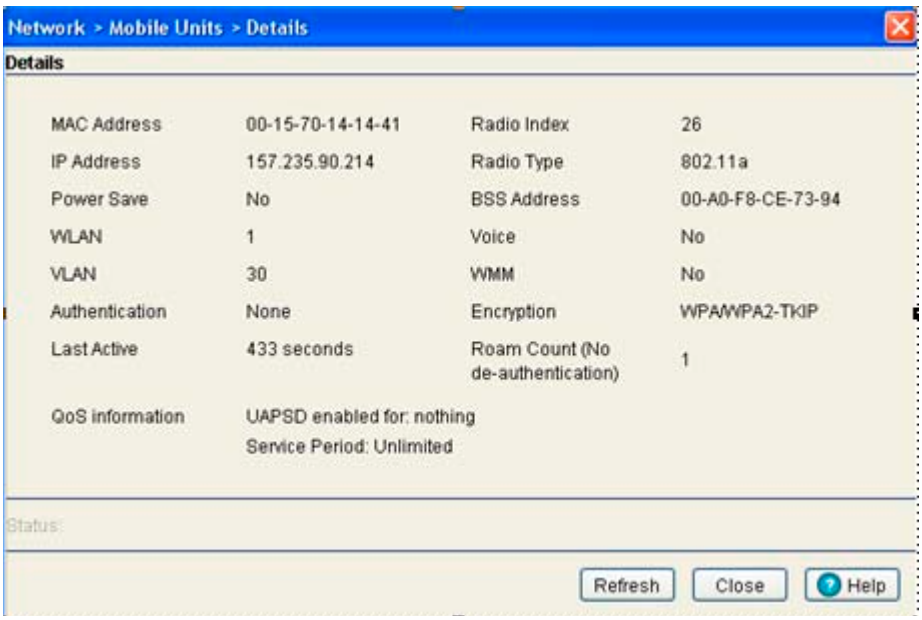
   Be aware that disconnected MUs will often become immediately re-connected to the switch. Ensure disconnected MUs are permanently removed from switch association.
5. Click the **Export** button to export the content of the table to a *Comma Separated Values* file (CSV).

4.6.1.1 Viewing MU Details

The **MUs Details** screen displays read-only MU transmit and receive statistics.

To view MU Details:

1. Select a **Network** > **Mobile Units** from the main menu tree.
2. Click the **Status** tab.
3. Select a MU from the table in the Status screen and click the **Details** button.



4. Refer to the following read-only MU's transmit and receive statistics:.

MAC Address	Displays the Hardware or Media Access Control (MAC) address for the MU.
IP Address	Displays the unique IP address for the MU. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
Power Save	Displays the current PSP state of the MU. This field has two potential settings. PSP indicates if the MU is operating in PSP mode. In PSP, the MU runs enough power to check for beacons, and is otherwise inactive. CAM indicates the MU is continuously aware of all radio traffic. CAM is recommended for MUs transmitting frequently.
WLAN	Displays of the WLAN the MU is currently associated with.
VLAN	Displays the VLAN parameter for the name of the VLAN the MU is currently mapped to.
Last Active	Displays the time the MU last interoperated with the switch.
QoS Information	Displays an indicator of the wireless device's battery life. Additionally, the service period for the selected MU is also displayed.
Radio Index	Displays is a numerical identifier used to associate a particular Radio with a set of statistics. The Index is helpful for distinguishing the a particular radio from other MU radios with similar configurations.
Radio Type	Displays the radio type used by the adopted MU. The switch supports 802.11b MUs as well as 802.11 a/b and 802.11 a/g dual-radio MUs. The radio also supports 802.11a only and 802.11g MUs.
Base Radio MAC	Displays the SSID of the Access Port when initially adopted by the switch.
BSS Address	Displays the MU's BSSID.

Voice	Displays whether or not the MU is a voice capable device. Traffic from a voice enabled MU is handled differently than traffic from MUs without this capability. MUs grouped to particular WLANs can be prioritized to transmit and receive voice traffic over data traffic.
WMM	Displays WMM usage status for the MU, including the Access Category currently in use. Use this information to assess whether the MU is using the correct WMM settings in relation to the operation of the switch.
Roam Count	Refer to the Roam Count value to assess the number of times the MU has roamed from the switch.

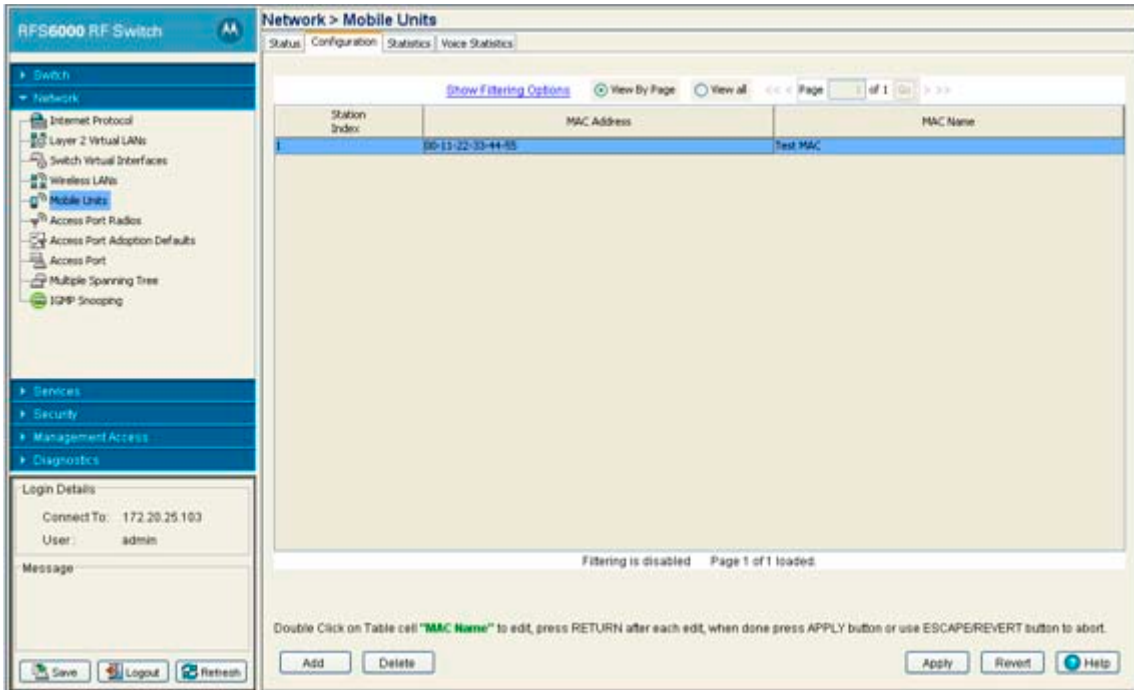
5. Click the **Refresh** button to update the MU Statistics to their latest values.
6. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

4.6.2 Configuring Mobile Units

The Mobile Units Configuration screen lets you view MAC Address to MAC Name associations as well as creating new MAC Address to MAC Name associations.

To configure Mobile Unit settings:

1. Select **Network** > **Mobile Units** from the main menu tree.
2. Click the **Configuration** tab.



3. The MU table displays the following information:

Station Index	The **Station Index** is a numerical device recognition identifier for a specific MU.

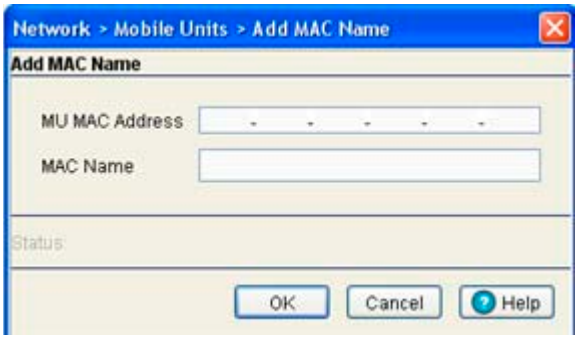
MAC Address	Each MU has a unique Media Access Control (**MAC**) address through which it is identified. This address is burned into the ROM of the MU.
MAC Name	The **MAC Name** is a user created name used to identify individual mobile unit MAC Addresses with a user friendly name. To edit an existing entry, double click the **MAC Name** and type in the new name.

4. When using clustering and the **Cluster GUI** feature is enabled a drop-down menu will be available to select which cluster members' MUs are displayed. To view MUs from all cluster members, select **All** from the drop-down menu. To view MUs from a specific cluster member, select that member's IP address from the drop-down menu.
5. To add a MAC address to MU association, click the **Add** button. For more information on adding an association, see *MAC Naming of Mobile Units*.
6. To remove a **MAC Name** association select the item from the table and click the **Delete** button.
7. If changes have been made to the MU table, click the **Apply** button to save the changes to the running config.

4.6.2.1 MAC Naming of Mobile Units

To configure Mobile Unit settings:

1. Select **Network** > **Mobile Units** from the main menu tree.
2. Click the **Configuration** tab and select **Add**.



3. Enter the MAC Address and MAC Name for the MU being added to the list:

MU MAC Address	Each MU has a unique Media Access Control (**MAC**) address through which it is identified. This address is burned into the ROM of the MU.
MAC Name	The **MAC Name** is a user created name used to identify individual mobile unit MAC Addresses with a user friendly name.

4. Click **OK** to use the changes to the running configuration and close the dialog.
5. Click **Cancel** to close the dialog without committing updates to the running configuration.

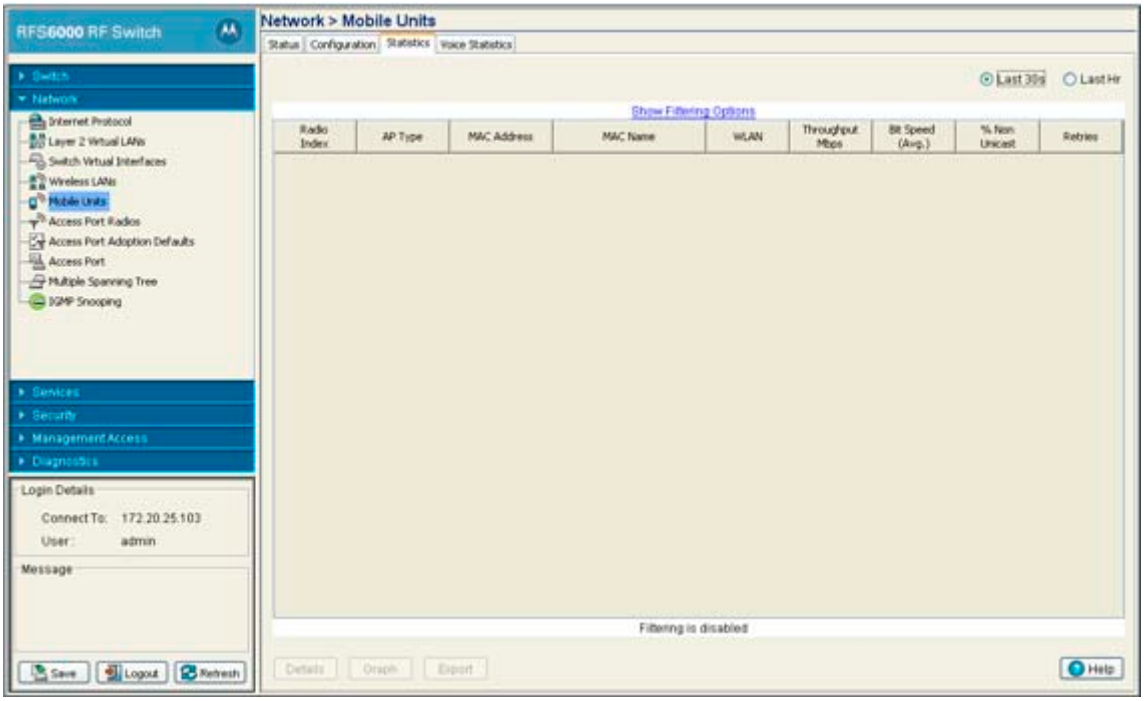
4.6.3 Viewing MU Statistics

The **Statistics** screen displays read-only statistics for each MU. Use this information to assess if configuration changes are required to improve network performance. If a more detailed set of MU statistics is required, select a MU from the table and click the **Details** button.

NOTE: The RFS6000 supports a maximum of 4096 MUs. The RFS7000 supports 8192 MUs.

To view MU statistics details:

1. Select **Network** > **Mobile Units** from the main menu tree.
2. Click the **Statistics** tab.



3. Select the **Last 30s** checkbox to display MU statistics gathered over the last 30 seconds. This option is helpful for assessing MU performance trends in real-time.
4. Select the **Last HR** checkbox to display MU statistics gathered over the last hour. This option is helpful for assessing performance trends over a measurable period.
5. Refer to following details as displayed within the **MU Statistics** table:

Radio Index	Displays a numerical identifier used to associate a particular Radio with a set of statistics. The Index is helpful for distinguishing the radio from other radios with a similar configuration.
AP Type	Displays the type of AP the MU is currently associated to. Use this information to discern whether the MU is optimally supported by this radio versus others detected.
MAC Address	Displays the Hardware or *Media Access Control* (MAC) address for the MU. The MAC address is hard coded at the factory and cannot be modified.

WLAN	Displays the name of the WLAN the MU is currently associated with. Use this information to determine if the MU/WLAN placement best suits the intended operation and MU coverage area.
Throughput Mbps	Displays the average throughput in Mbps between the selected MU and the Access Port. The Rx column displays the average throughput in Mbps for packets received on the selected MU from the Access Port. The Tx column displays the average throughput for packets sent on the selected MU from the Access Port.
Bit Speed (Avg.) Mpbs	Displays the average bit speed in Mbps for the selected MU. This includes all packets sent and received.
% Non Unicast	Displays the percentage of the total packets for the selected MU that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.

6. Click the **Details** button to launch a screen with additional information about the selected MU. For more information, see *Viewing MU Statistics in Detail on page 4-87*.
7. Click the **Graph** button to launch a graph with pictorial information about the selected MU in a graphical format. For more information, see *View a MU Statistics Graph on page 4-88*.
8. Click the **Export** button to export the content of the table to a *Comma Separated Values* file (CSV).

4.6.3.1 Viewing MU Statistics in Detail

The MU Statistics **Details** screen displays additional device address and performance information for the selected MU. Use the WMM information to assess if poor MU performance can be attributed to an inaccurate WMM setting for the type of data transmitted. To view the MU Statistics details:

1. Select a **Network** > **Mobile Units** from the main menu tree.
2. Click the **Statistics** tab.
3. Select a MU from the table displayed in the Statistics screen and click the **Details** button.

   The Details screen displays WLAN statistics for the selected WLAN, including:

   - *Information*
   - *Traffic*
   - *RF Status*
   - *Errors*

   Information in black represents the statistics from the last 30 seconds and information in blue represents statistics from the last hour. Use both sets of data to trend stats in real time versus a measurable period (1 hour).
4. Refer to the **Information** field for the following information:

MAC Address	Displays the Hardware or *Media Access Control* (MAC) address for the MU. This address is hard-coded at the factory and cannot be modified.
BSS Address	Displays the MU's BSSID.
IP Address	Displays the current IP address for the MU.

Voice	Displays whether the MU is a voice capable device. Traffic from voice enabled MUs is handled differently (higher priority) than traffic from MUs without this capability.
WLAN	Displays the name of the WLAN the MU is currently associated with.
WMM	Displays WMM usage status for the MU, including the access category currently in use. Use this information to assess whether the MU is using the correct WMM settings in relation to its intended data traffic type.

5. Refer to the **Traffic** field for the following information:

Pkts per second	Displays the average packets per second received by the MU. The Rx column displays the average packets per second received on the selected MU. The Tx column displays the average packets per second sent on the selected MU.
Throughput	Displays the average throughput in Mbps between the MU and the Access Port. The Rx column displays the average throughput in Mbps for packets received on the selected MU from the Access Port. The Tx column displays the average throughput for packets sent on the selected MU from the Access Port.
Avg. Bit Speed	Displays the average bit speed in Mbps on the selected MU. This includes all packets sent and received.
% Non-unicast pkts	Displays the percentage of the total packets for the MU that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.

6. Refer to the **RF Status** field for the following information:

Avg MU Signal	Displays the RF signal strength in dBm for the selected MU.
Avg MU Noise	Displays the RF noise for the selected MU.
Avg MU SNR	Displays the *Signal to Noise Ratio* (SNR) for the selected MU. The Signal to Noise Ratio is an indication of overall RF performance on the wireless network.

7. Refer to the **Errors** field for the following information:

Avg Num of Retries	Displays the average number of retries for the selected MU. Use this information to assess potential performance issues.
% Gave Up Pkts	Displays the percentage of packets the switch gave up on for the selected MU.
% of Undecryptable Pkts	Displays the percentage of undecryptable packets (packets that could not be processed) for the selected MU.

8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.6.3.2 View a MU Statistics Graph

The MU Statistics tab has an option for displaying detailed MU statistics for individual MUs in a graphical format. This information can be used for comparison purposes to chart MU and overall switch performance.

To view the MU Statistics in a graphical format:

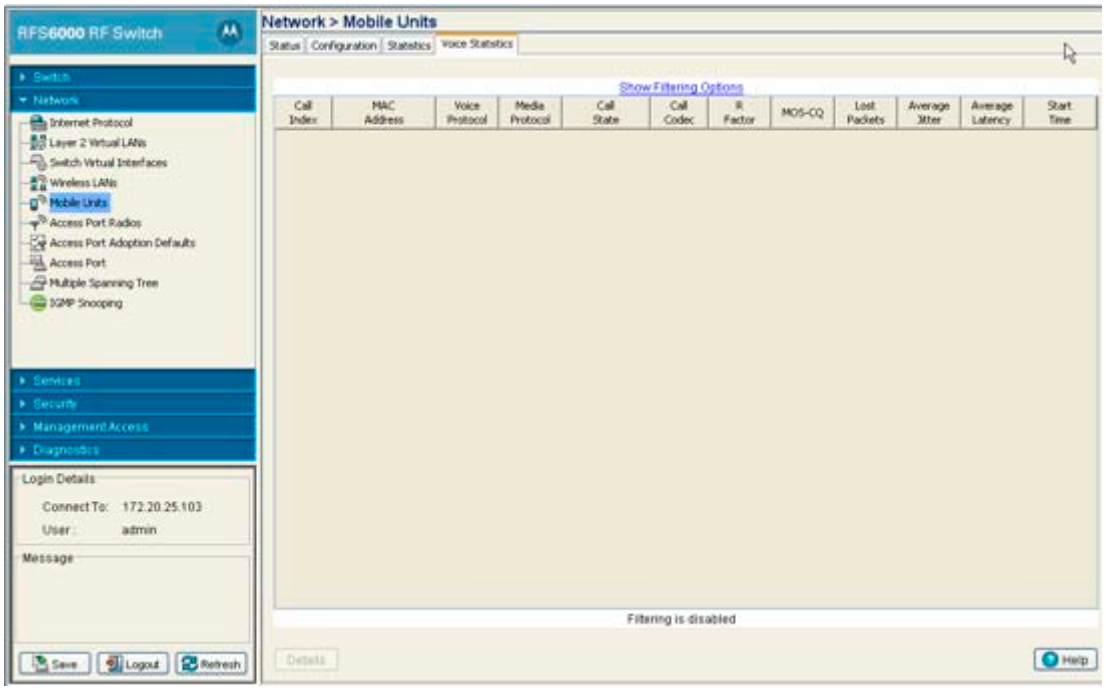
1. Select a **Network** > **Mobile Units** from the main menu tree.
2. Click the **Statistics** tab.
3. Select a MU from the table displayed in the Statistics screen and click the **Graph** button.
4. Select a checkbox to display that metric charted within the graph. Do not select more than four checkboxes at any one time.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **Close** to close the dialog without committing updates to the running configuration.

4.6.4 Viewing Voice Statistics

The **Voice Statistics** screen displays read-only voice data statistics for each MU. Use this information to assess if configuration changes are required to improve MU voice quality. If a more detailed set of voice statistics is required, select a call index from the table and click the **Details** button.

To view MU voice statistics details:

1. Select **Network** > **Mobile Units** from the main menu tree.
2. Click the **Voice Statistics** tab.



3. Refer to following details as displayed for voice data traffic with MUs:

Call Index	Displays a numerical identifier used to associate a particular voice call with a set of statistics. The Index is helpful for distinguishing the call from others with similar attributes.
MAC Address	Displays the MU MAC address of the device initiating the call.
Voice Protocol	Displays the voice protocol used for each call listed.

Media Control	Displays the protocol for the control of *Voice over IP* (VoIP) calls by external call-control elements known as *media gateway controllers* (MGCs) or *call agents* (CAs
Call State	Displays the call state of the MU's call session.
Call Codec	Displays the call codec. Codec complexity refers to the amount of processing required to perform compression. Codec complexity affects the number of calls, that can take place
R Factor	Displays the average call quality using the R Factor scale. The R Factor method rates voice quality on a scale of 0 to 120 with a higher score being better. If the R Factor score is lower than 70, it is likely users will not be satisfied with the voice quality of calls.
MOS-CQ	Displays the average call quality using the *Mean Opinion Score* (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 is likely that users will not be satisfied with the voice quality of calls.
Lost Packets	Displays the number of packets that did not make it to their destination during in the specified call index.
Average Jitter	Displays the average jitter time for calls on the displayed MUs. Jitter is delays on the network that can result in a lag in conversations. A jitter score higher than 150ms is likely to be noticed by end users during a call.
Average Latency	Displays the average latency in miliseconds for calls on the selected index.
Start Time	Displays when the call was originated.

4. Select a call index from those displayed and select the **Details** button for additional information.

4.7 Viewing Access Port Information

The **Access Ports** screen displays a high-level overview of the APs created for use within the switch managed network. Use this data as necessary to check all the APs that are active, their VLAN assignments, updates to a APs description as well as their current authentication and encryption schemes.

NOTE: The RFS6000 can support a maximum of 48 Access Ports. The RFS7000 can support a maximum of 256 Access Ports. However, port adoption per switch is determined by the number of licenses acquired.

NOTE: The *Motorola RF Management Software* is a recommended utility to plan the deployment of the switch and view its configuration once operational. Motorola RFMS can help optimize the positioning and configuration of a switch and Access Ports in respect to a WLAN's MU throughput requirements. For more information, refer to the Motorola Web site.

The Access Ports screen consists of the following tabs:

- *Configuring Access Port Radios*
- *Viewing AP Statistics*
- *Configuring WLAN Assignment*
- *Configuring WMM*

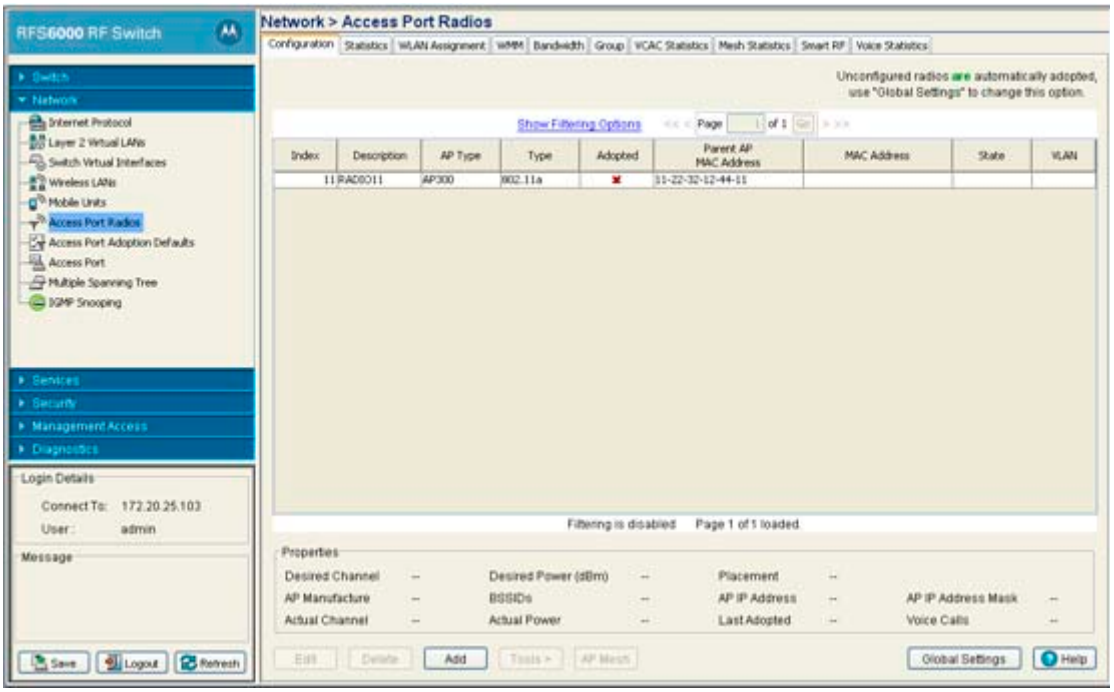
- *Configuring Access Point Radio Bandwidth*
- *Configuring Radio Groups for MU Load Balancing*
- *Viewing Active Calls (VCAC) Statistics*
- *Viewing Mesh Statistics*
- *Smart RF*
- *Voice Statistics*

4.7.1 Configuring Access Port Radios

Refer to the **Configuration** tab to view existing radio configurations available to the switch. After reviewing the radios listed, you have the option of editing a radio's properties, deleting a radio, adding a new radio, resetting a radio, scanning available channels or exporting a radio.

To view Access Port Radio configuration details:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Configuration** tab.



3. Refer to the table for the following information:

Index	Displays the numerical index (device identifier) used with the device radio. Use this index (along with the radio name) to differentiate the radio from other device radios.
Description	Displays a user assigned name for the radio.
AP Type	Displays the type of Access Port detected. The switches support Motorola AP 100, AP300 model Access Ports and AP-4131, AP-5131 and AP-7131 model Access Points.
Type	Use the Type to identify whether the radio is 802.11a radio or an 802.11bg radio.

Adopted	Displays the radio's adoption status. If the radio is adopted, a green check displays. If the radio is not adopted, a red X displays.
Parent AP MAC Address	Displays the Access Port's Ethernet MAC (the device MAC address that is printed on the casing of the unit). Please do not confuse this BSSID MAC with the Access Port's Ethernet MAC address.
MAC Address	The Base Radio MAC is the radio's first MAC address when it is adopted by the Switch.
State	Display the radio's current operational mode. If the radio is set as a Detector AP, the state is "Detector", otherwise the state is "Normal".
VLAN	Displays the name of the VLAN currently used with each Access Port radio.

4. Refer to the **Properties** field for the following

Desired Channel	When the radio's channel is configured statically, the Actual Channel and Desired Channel are the same. If using ACS (*Automatic Channel Selection*), the switch selects a channel for the radio. The Desired Channel displays "ACS" and the Actual channel displays the channel selected for the radio. When set to Random, the applet determines the channel's designation.
AP Manufacturer	Displays the kind of AP listed by each index.
Actual Channel	When the radio's channel is configured statically, the Actual Channel and Desired Channel are the same. If using ACS (Automatic Channel Selection), the switch selects a channel for the radio. The Desired channel displays "ACS" and the Actual Channel displays the channel selected for the radio.
Desired Power (dBm)	Displays the configured power setting in dBm for the selected radio. In most cases, the Desired Power and Actual Power are the same unless the desired power level would put the radio's output power outside the accepted regulatory compliance range.
BSSIDs	Displays the BSSIDs used by the displayed radio index.
Actual Power	Displays the current power level in dBm for the selected radio. In most cases, the Desired Power and Actual Power are the same unless the desired power level would put the radio's output power outside the accepted regulatory compliance range.
Placement	When the radio is adopted using the default configuration, the power for the radio can be defined as "Indoor" or "Outdoor." However, some countries have restrictions for the use of outdoor radios. If using a value of "Outdoor" verify it is in compliance with the country of operation's regulatory restrictions.
AP IP Address	Displays the AP's IP address.
Last Adopted	Displays the time this radio was last adopted by the switch.
AP IP Address Mask	Displays the net mask address associated with the selected Access Port IP Address.
Voice Calls	Displays the current number of active voice calls for the selected radio.

5. Click the **Edit** button to launch a screen used to configure radio specific parameters. For more information, see *Editing AP Settings on page 4-95*.

6. Click the **Delete** button to remove a radio. However, before a radio can be removed, the radio's BSS mapping must be removed.
7. Click the **Add** button to add a radio. The radio must be added before the radio can be adopted. For more information, see *Adding APs on page 4-101*.
8. Click the **Reset** button to reset an individual radio.
9. Click the **Tools >** button to displays a submneu with **Reset**, **Run ACS** and **Export** options.

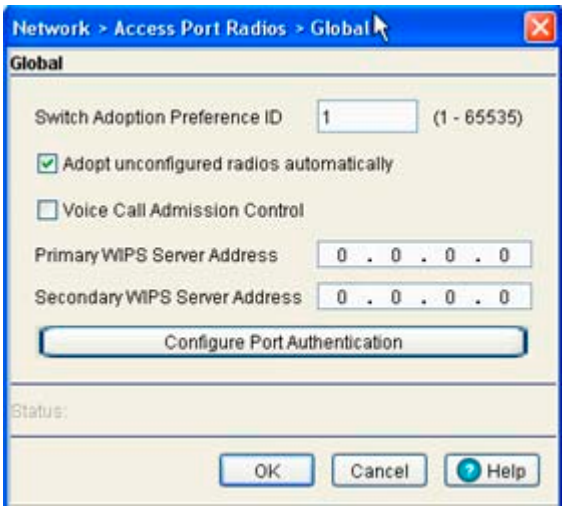
   Select the Reset option to reset the Access Port radio. Select the **Run ACS Now** option to scan all channels and discover which radios are adopted and on what channel. ACS then analyzes the radios' channels and moves the radio to the channel where it is least likely to have interference from the other radios. Use the **Export** option to move the contents of the table to a *Comma Separated Values* file (CSV).
10. When using clustering and the **Cluster GUI** feature is enabled, a drop-down menu will be available to select which cluster members' Access Port radios are displayed. To view Access Port radios from all cluster members, select All from the drop-down menu. To view Access Port radios from a specific cluster member, select that member's IP address from the drop-down menu.
11. Click the **Global Settings** button to display a screen with settings applying to all radios on the system. For more information, see *Configuring an AP's Global Settings on page 4-93*.

4.7.1.1 Configuring an AP's Global Settings

Use the **Global Settings** screen to define an adoption preference ID for the switch and enable an option to adopt non-configured radios. This can be helpful when you do not want to change an Access Port's configuration but require the Access Port be adopted.

To edit Global Radio configuration settings:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Configuration** tab.
3. Click the **Global Settings** button to display a screen containing global settings which apply to all radios on the switch.



4. Set an **Adoption Preference ID** value between 1 and 65535.

   To define a radio as preferred, the Access Port preference ID should be same as the adoption preference ID. The adoption preference ID is used for AP load-balancing. A switch will preferentially adopt Access Ports having the same adoption-preference-id as the switch itself.

   The Adoption Preference ID defines the switch preference ID. The value can be between 1 and 65535. To define radios as preferred, the Access Port preference ID should be same as the adoption preference ID. If the value is set to 0, the switch automatically changes the value to 1.

   In a layer 3 environment, the Access Port adoption process is somewhat unique, for more information, see
   Configuring Layer 3 Access Port Adoption on page 4-136.
5. To enable the automatic adoption of non-configured radios on the network, select the **Adopt unconfigured radios automatically** option. Default radio settings are applied to Access Ports when automatically adopted. Enable this option to allow adoption even when the Access Port is not configured. Default radio settings are applied to Access Ports adopted automatically.
6. To limit the number of voice enabled MUs which are associated, click the **Voice Call Admission Control** checkbox. Limiting voice MU traffic in a supported WLAN is a good idea to maintain data rates, voice quality and throughput. WMM admission control is a mechanism for limiting traffic on a given access category. Per the recommendation of the 802.11e specification, Motorola limits support of this feature to voice and video. The switch configures the AP to broadcast that admission control is configured by default on AP300s.
7. To use WIPS enter a **Primary WIPS Server Address** and **Secondary WIPS Server Address** into the corresponding fields.

NOTE: When using an AP-5131for use with WIPS and as a sensor you must first configure the WIPS server IP Addresses before converting the AP-5131 to a sensor.

8. Click the **Configure Port Authentication** button to open a new dialogue with port authentication configuration information.
9. Click **OK** to save the changes and return to the previous screen.

Port Authentication

To configure the port authentication settings on an Access Port:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Configuration** tab.
3. Click the **Global Settings** button.
4. Click the **Configure Port Authentication** button.
5. Enter the 802.1x **Username** assigned to the Access Port.
6. Enter the 802.1x **Password** (for the corresponding username) providing authorization for Access Port authorization adoption.

NOTE: The default user name and password for AP300 port authentication is a user name of **admin** and a password of **symbol**.

7. Check the **Use Default Values** option checkbox to set the Username and Password to factory default values. The Access Port can get disconnected if the 802.1x authenticator is not configured accordingly.

NOTE: 802.1x username and password information is only passed to adopted Access Ports when the Username and Password are set. Any AP adopted after this does not automatically receive a username and password.

NOTE: After setting the username and password to factory default settings, the system must be rebooted before the factory default settings are applied

8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

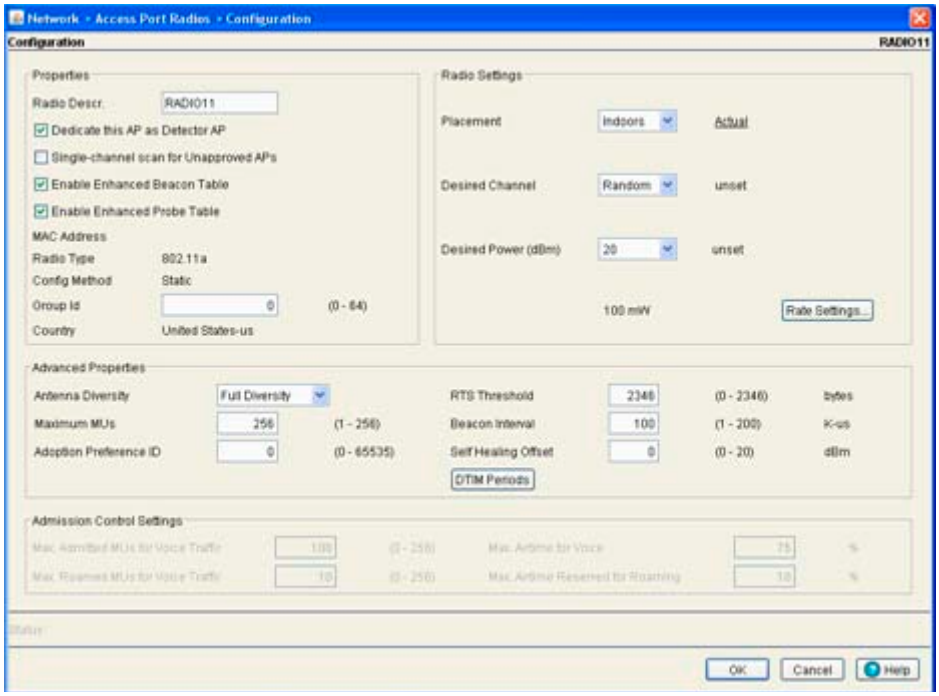
4.7.1.2 Editing AP Settings

The **Edit** screen provides a means of modifying the properties of an existing radio. This is often necessary when the radio's intended function has changed and its name needs modification or if the radio now needs to be defined as a detector radio. The Edit screen also enables you to modify placement, channel and power settings as well as a set of advanced properties in case its transmit and receive capabilities need to be adjusted.

NOTE: The screen display can vary slightly depending on whether the Access Port radio is an 802.11a or 802.11bg model.

To edit a radio's configuration:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Configuration** tab.
3. Select a radio to edit from the table.
4. Click the **Edit** button to display a screen containing settings for the selected radio.



5. The **Switch** field displays the IP address of the cluster member associated with each Access Port radio. When clustering is enabled on the switch and **Cluster GUI** is enabled the **Switch** field will be available on the Access Port Radio edit screen. For information on configuring enabling Cluster GUI, see *Managing Clustering Using the Web UI*.
6. In the **Radio Descr.** field, enter a brief description to differentiate the radio. The description is used to describe radios of the same type and can be used to locate a radio if there are any problems.
7. Select the **Dedicate this AP as Detector AP** option to use this radio as a detector port to identify rogue APs on the network.

   Setting this radio as a detector dedicates the radio to detect rogue APs on the network. Dedicated detectors do not connect to clients.
8. Select the **Single-channel scan for Unapproved APs** checkbox to enable the switch to scan for rogue devices using the radio's current channel of operation.
9. Select the **Enable Enhanced Beacon Table** checkbox to allow adopted Access Port or Access Point radios to scan for potentially unauthorized APs across all bands.

   This option utilizes radio bandwidth, but is an exhaustive means of scanning across all available channels and listening for AP beacon traffic. Once probe responses are received, a network device management application like Motorola RFMS or the *Wireless Intrusion Detection System* (WIDS) can locate the device and remove it if defined as unauthorized.
10. Select the **Enable Enhanced Probe Table** checkbox to enable an adopted Access Port or Access Point radio to forward the probes required to obtain MU RSSI information.

    RSSI data (as obtained by at least three detecting radios) can be used by the Motorola RFMS application to triangulate the location of a MU on a site map representative of the actual physical dimensions of the switch radio coverage area. Once located on a site map, intuitive decisions can be made regarding the MU's authorization within the switch managed network.

11.The following read only information is displayed:

MAC Address	The Base Radio MAC is the radio's first MAC address when it is adopted by the Switch.
Radio Type	Radio type identifies whether the radio is an 802.11an radio or a 802.11 bgn radio.
Config Method	The Config Method displays whether the radio has been configured using static or dynamic settings.

12.To add the radio to a Radio Group enter the **Group ID** for the radio group you wish to add it to. For more information on configuring Radio Groups see *Configuring Radio Groups for MU Load Balancing on page 4-114*.

Refer to the **Country** parameter to assess the country the AP radio has been deployed in. The radio must be configured to operate within the regulatory restrictions of the country it's deployed in.

13.From within the Radio Settings field, define the **Placement** of the Access Port as either **Indoors** or **Outdoors**.

An Access Port can be set for Indoors or Outdoors use depending on the model and the placement location. Power settings and channel selection options differ based on each country's regulatory rules and whether or not the unit is placed indoors or outdoors.

14.Select a channel for communications between the Access Port and its associated MUs within the **Desired Channel** field.

The selection of a channel determines the available power levels. The range of legally approved communication channels varies depending on the installation location and country. The selected channel can be a specific channel, "Random," or "ACS." Random assigns each radio a random channel. ACS (*Automatic Channel Selection*) allows the switch to systematically assign channels. Default is Random.

15.After first selecting a channel, select a power level in dBm for RF signal strength in the **Desired Power (dBm)** field.

The optimal power level for the specified channel is best determined by a site survey prior to installation. Available settings are determined according to the selected channel. Set a higher power level to ensure RF coverage in WLAN environments that have more electromagnetic interference or greater distances between the Access Port and MUs. Decrease the power level according to the proximity of other Access Ports. Overlapping RF coverage may cause lost packets and problems for roaming devices trying to connect to an Access Port. After setting a power level, channel and placement the RF output power for the Access Port is displayed in mW. The default is 20 dBm (802.11bg), 17 dBm (802.11a).

NOTE: After setting a power level, channel and placement, the RF output power for the Access Port displays in mW.

16.To configure optional rate settings, click the **Rate Settings** button to display a new dialogue containing rate setting information. Instructions on configuring rate settings is described in *Configuring Rate Settings on page 4-100*.

17. In most cases, the default settings for the **Advanced Properties** are sufficient. If needed, additional Advanced Properties can be modified for the following:

Antenna Diversity	Use the drop-down menu to configure the Antenna Diversity settings for Access Ports using external antennas. Options include: • *Full Diversity* - Utilizes both antennas to provide antenna diversity. • *Primary Only* - Enables only the primary antenna. • *Secondary Only* - Enables only the secondary antenna. Antenna Diversity should only be enabled if the Access Port has two matching external antennas. Default value is **Full Diversity**.
Maximum MUs	Sets the maximum number of MUs that can associate to a radio. The maximum number of MUs that can associate to a radio is 64.
Adoption Preference ID	Displays the preference ID of the switch.The value can be set between 1 and 65535. To define the radios as preferred, the Access Port preference ID should be same as adoption preference ID. The adoption preference ID is used for AP load-balancing. A switch will preferentially adopt APs which have the same adoption-preference-ID as the switch itself.
Short Preambles only	If using an 802.11bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This checkbox does not display if using an 802.11a radio.

RTS Threshold

Specify a *Request To Send* (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports.

RTS is a transmitting station's signal that requests a *Clear To Send* (CTS) response from a receiving station. This RTS/CTS procedure clears the air where many MUs 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.

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.

Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Ports. 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.

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. Default is 2346.

In 802.11b/g mixed RTS/CTS happens automatically. There is no way to disable RTS/CTS unless the network and all the devices used are 802.11g or 802.11a only. The proper co-existence of 802.11b and 802.11g is ensured thru RTS/CTS mechanism. On 802.11g radios CTS-to-self is enabled irrespective of whether or not 11b rates are enabled or disabled.

When ERP Protection is ON, the 11bg radio will perform a CTS-to-self before it transmits the frame.

Beacon Interval

Specify a beacon interval in units of 1,024 microseconds (K-us). This is a multiple of the DTIM value, for example, 100: 10. (See "DTIM Period," below). A beacon is a packet broadcast by the adopted Access Ports to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the radio-port 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 is 100 K-us.

Self Healing Offset	When an Access Port increases its power to compensate for a failure, power is increased to the country's regulatory maximum. Set the Self Healing Offset to reduce the country's regulatory maximum power if Access Ports are situated close to each other or if an Access Port uses an external antenna.
DTIM Periods	Select the **DTIM periods** button to specify a period for *Delivery Traffic Indication Messages* (DTIM) for BSS IDs 1-4. This is a divisor of the beacon interval (in milliseconds), for example, 10 : 100. (See "Beacon Interval," above). A DTIM is periodically included in the beacon frame transmitted from adopted Access Ports. 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 Port) 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. The default DTIM period is 10 beacons for BSS 1-4.

18. When the **Voice Call Admission Control** is enabled in the **Global Settings**, the **Admission Control Settings** section allows you to modify the following properties.

Max Admitted MUs for Voice Traffic	Specify the maximum number of MUs allowed to connect to the specified radio for voice traffic. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality.
Max Roamed MUs for Voice Traffic	Specify the maximum number of voice MUs that are allowed to roam to this radio. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality.
Max Airtime for Voice	Specify a maximum percentage out of the radio's total airtime that may be used for voice.
Max Airtime for Reserved Roaming	Specify a maximum percentage out of the radio's total airtime that may be used for voice MUs which roam from other APs.

19. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
20. If clustering is configured and the **Cluster GUI** feature is enabled the **Apply to Cluster** feature will be available. Click the **Apply to Cluster** button to apply the AP radio settings to all members in the cluster.

NOTE: When Cluster GUI is enabled and an Access Port configuration is deleted from one switch, it is not automatically deleted from other switches in the cluster.

21. Click **OK** to use the changes to the running configuration and close the dialog.
22. Click **Cancel** to close the dialog without committing updates to the running configuration.

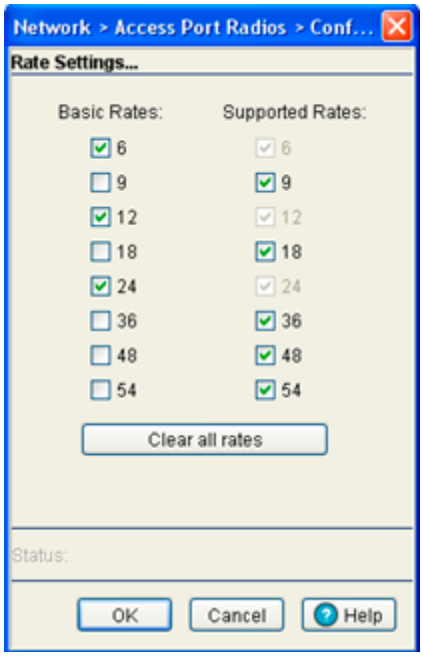
Configuring Rate Settings

Use the **Rate Settings** screen to define a set of basic and supported rates for the target radio. This allows the radio to sync with networks using varying data rates and allows the radio to default to a predefined set of data rates when higher data rates cannot be maintained.

To configure Rate Settings for a radio:

1. Click the **Rate Settings** button within the radio edit screen to launch a new screen with rate setting information.
2. Check the boxes next to all the **Basic Rates** you want supported.

   Basic Rates are used for management frames, broadcast traffic and multicast frames. If a rate is selected as a basic rate it is automatically selected as a supported rate.
3. Check the boxes next to all the **Supported Rates** you want supported.



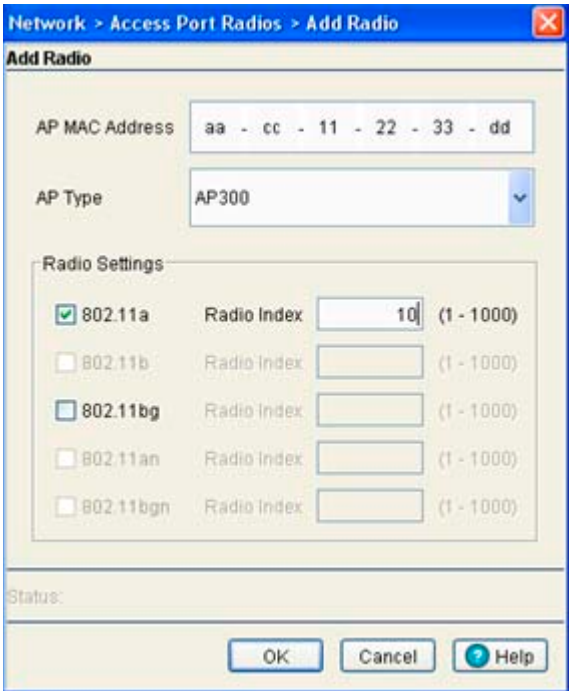
   Supported rates allow an 802.11 network to specify the data rate it supports. When a MU attempts to join the network, it checks the data rate used on the network. If a rate is selected as a basic rate, it is automatically selected as a supported rate. The basic default rates for an 802.11a radio differ from those 802.11b default rates, as an 802.11a radio can support a maximum data rate of 54Mbps, while an 802.11b radio can support a maximum data rate of 11Mbps.
4. Click the **Clear all rates** button to uncheck all of the Basic and Supported rates.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.7.1.3 Adding APs

The **Add Radio** screen provides a facility for creating a new (unique) radio index for inclusion within the Configuration screen. Use the Add screen to add the new radio's MAC address and define its radio type.

To add a Radio to the switch:

1. Select **Network** > **Access Port Radios** from the main menu.
2. Click the **Configuration** tab.
3. Click the **Add** button to display at screen containing settings for adding a radio



4. Enter the device **AP MAC Address** (the physical MAC address of the radio). Ensure this address is the actual hard-coded MAC address of the device.
5. Use the **AP Type** drop-down menu to define the radio type you would like to add. If adding an AP-4131, AP-5131 or AP-7131 model Access Point, the Access Port conversion will render the Access Point a "thin" Access Port.
6. From the **Radio Settings** section, select the radio type checkboxes corresponding to the type of AP radio used.Available radio types are dependant on the **AP Type** selected above.
7. Enter a numerical value in the **Radio Index** field for each selected radio.

   The Radio Index is a numerical value assigned to the radio as a unique identifier. For example: 1, 2, or 3. The index is helpful for differentiating radios of similar type and configuration.
8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. If clustering is configured and the **Cluster GUI** feature is enabled the **Apply to Cluster** feature will be available. Click the **Apply to Cluster** button to apply the AP radio settings to all members in the cluster.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

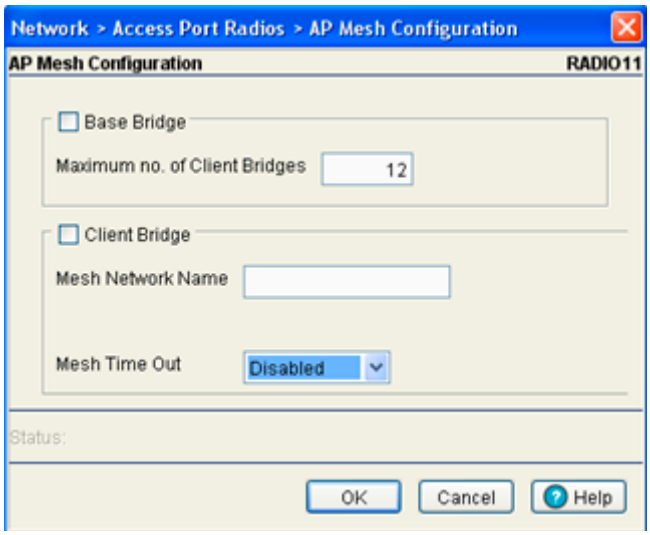
4.7.1.4 Defining the AP Radios Mesh Configuration

A separate mesh configuration can be set for each AP radio. Define mesh configurations as required when dedicating an AP radio as either a base or client bridge within a mesh configuration.

To define the selected AP radio's mesh configuration:

1. Select **Network** > **Access Port Radios** from the main menu.
2. Click the **Configuration** tab.
3. Select a target index from amongst those displayed.

4. Select the **AP Mesh** button at the bottom of the Configuration screen.



Base Bridge	Select the Base Bridge checkbox to allow the AP radio to accept client bridge connections from other access points in client bridge mode. The base bridge is the acceptor of mesh network data from those client bridges within the mesh network and never the initiator.
Maximum no. of Client Bridges	Define the client bridge load on this particular base bridge.
Client Bridge	Select the Client Bridge checkbox to enable the access point radio to initiate client bridge connections with other mesh network supported access point's using the same WLAN.

Mesh Network Name	If the Client Bridge checkbox has been selected, enter a Mesh Network Name to define the WLAN (ESS) the client bridge uses to establish a wireless link. Motorola recommends creating (and naming) a WLAN specifically for mesh networking support to differentiate the Mesh supported WLAN from non-Mesh supported WLANs.
Mesh Time Out	Define whether one of the radio's beacons uses an uplink connection. The Mesh Timeout value is not available on a single-radio AP, since the radio would have to stop beaconing and go into scan mode to determine if a base bridge uplink is lost. The following drop-down menu options are available: *Disabled* - When disabled, both radios are up at boot time and beaconing. If one radio (radio 1) does not have a mesh connection, the other radio (radio 2) is not affected. Radio 2 continues to beacon and associate MUs, but MU's can only communicate amongst themselves using the access point. Disabled is the default value. *Uplink detect* - The AP only boots up the radio configured as a client bridge. The AP boots up the second radio as soon as the first mesh connection is established. However, if the client bridge radio loses its uplink connection, the second radio shuts down immediately. Uplink detect is the recommended setting within a multi-hop mesh network. *Enabled* - If the mesh connection is down on one radio (radio 1), the other radio (radio 2) is brought down and stops beaconing after the timeout period. This allows the client bridge (radio 1) to roam without dropping the MU's associated to radio 2. The disadvantage is that radio 2 may beacon for the timeout period and have to drop associated MU's because radio 1 could not establish its uplink.

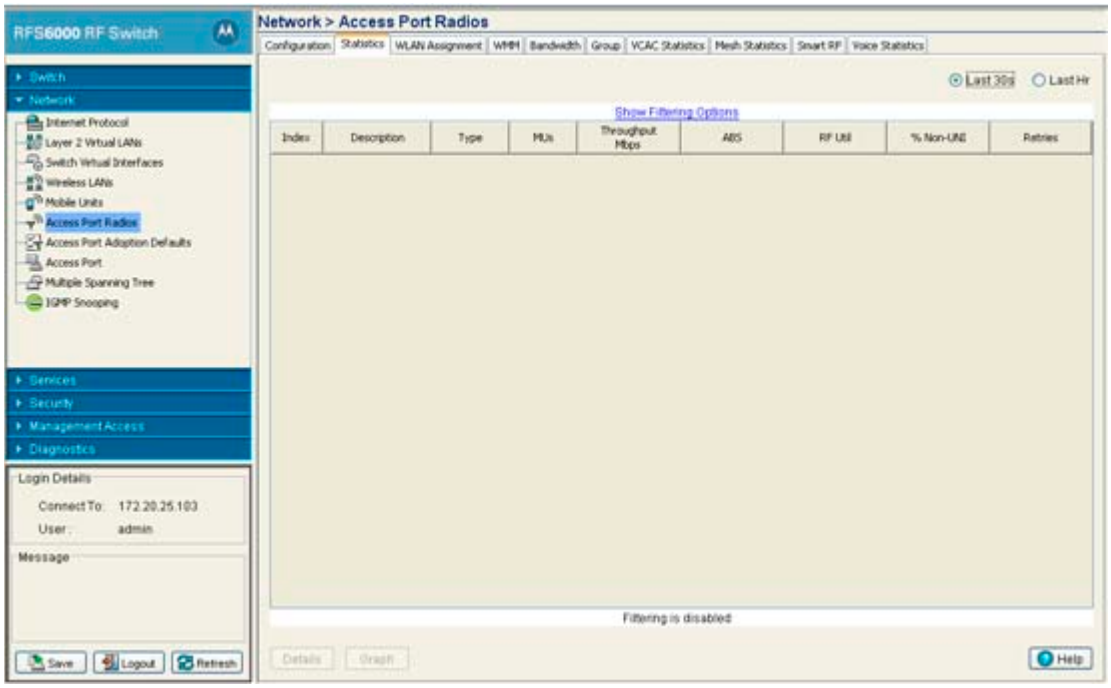
5. Select **OK** to save the changes to the AP's mesh configuration, or select **Cancel** to revert to the previously saved configuration.

4.7.2 Viewing AP Statistics

Refer to the **Statistics** tab for information and high-level performance data for individual radios. Performance information can be reviewed for either a 30 second or one hour interval. Use the Details button to display additional information for an individual radio.

To view Radio Statistics:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Statistics** tab.



3. To select the time frame for the radio statistics, select either **Last 30s** or **Last Hr** above the statistics table.
   - Select the Last 30s radio button to display statistics for the last 30 seconds for the radio.
   - Select the Last Hr radio button to display statistics from the last hour for the radio.
4. Refer to the table for the following information:

Index	Displays the numerical index (device identifier) used with the radio. Use this index (along with the radio name) to differentiate the radio from other device radios.
Description	Displays the name used with the radio. Use this name (along with the radio index) to differentiate the radio from other device radios.
Type	Identifies whether the radio is an 802.11a radio or an 802.11 bg radio.
MUs	Displays the number of MUs currently associated with the Access Port.
Throughput Mbps	Displays the average throughput in Mbps for the selected radio. The Rx column displays the average throughput in Mbps for packets received on the selected radio. The Tx column displays the average throughput for packets sent on the selected radio.
ABS	Displays the average bit speed in Mbps on the selected Access Port. This value includes packets both sent and received.
RF Util	Displays the percentage of the total packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.

% Non-UNI	Displays the percentage of packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the average number of retries for all MUs associated with the selected radio.

5. Select a radio from those displayed and click the **Details** button for additional radio information in rae data format. For more information, see *Viewing AP Statistics in Detail on page 4-106*.
6. Select a radio from those displayed and click the **Graph** button for additional radio performance information in graphical format. For more information, see *Viewing AP Statistics in Detail on page 4-106*.

4.7.2.1 Viewing AP Statistics in Detail

The **Details** screen provides additional (and more specific) traffic, performance and error information for the selected radio.

To view Radio Statistics Details:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Statistics** tab.
3. Select a radio from the table and click the **Details** button to display a screen with detailed statistics for that radio.

   Radio statistics details are split into four fields: **Information**, **Traffic**, **RF Status** and **Errors**. Information in black represents the statistics from the last 30 seconds and information in blue represents statistics from the last hour.
4. Refer to the **Information** field for the following information:

Description	Displays a brief description of the radio to help differentiate the radio from similar models.
MAC Address	Displays the Hardware or *Media Access Control* (MAC) address for the Access Port. Access Ports with dual radios will have a unique hardware address for each radio.
Num Associated Stations	Displays the number of MUs currently associated with the radio.
Radio Type	Displays the Access Port model.
Current Channel	Displays the channel the Access Port is currently passing traffic on. If the channel is displayed in red, it means the configured channel does not match the current channel. The configured channel in this case, is the value in parentheses. The AP may not be operating on the configured channel for 2 reasons: Uniform spreading is enabled or radar was encountered on the configured channel.

5. Refer to the **Traffic** field for the following information:

Pkts per second	Displays the average total packets per second that cross the selected radio. The Rx column displays the average total packets per second received on the selected radio. The Tx column displays the average total packets per second sent on the selected radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Throughput	Displays the average throughput in Mbps on the selected radio. The Rx column displays the average throughput in Mbps for packets received on the selected radio. The Tx column displays the average throughput for packets sent on the selected radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Avg Bit Speed	Displays the average bit speed in Mbps on the selected radio. This includes all packets that are sent and received. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Non-unicast Pkts	Displays the percentage of the total packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

6. Refer to the **RF Status** field for the following information:

Avg Station Signal	Displays the average RF signal strength in dBm for all MUs associated with the selected radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Avg Station Noise	Displays the average RF noise for all MUs associated with the selected radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Avg Station SNR	Displays the average *Signal to Noise Ratio* (SNR) for all MUs associated with the selected radio. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

7. Refer to the **Errors** field for the following information:

Avg Num of retries	Displays the average number of retries for all MUs associated with the selected radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
% Gave Up Pkts	Displays the percentage of packets the switch gave up on for all MUs associated with the selected radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
% of Undecryptable Pkts	Displays the percentage of undecryptable packets for all MUs associated with the selected radio. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

8. Click **Refresh** to update the content of the screen with the latest values.
9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

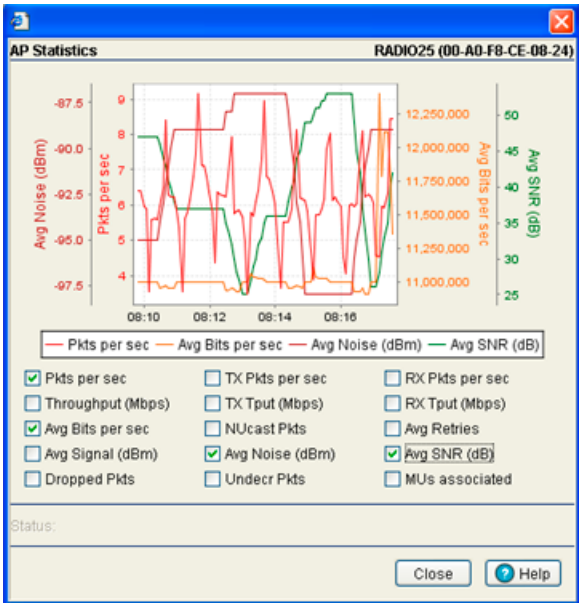
10.Click **Cancel** to close the dialog without committing updates to the running configuration.

4.7.2.2 Viewing AP Statistics in Graphical Format

The Access Port Radios Statistics tab has an option for displaying detailed Access Port radio statistics in a graph. This information can be used to chart associated switch radio performance and help diagnose radio performance issues.

To view the MU Statistics in a graphical format:

1. Select a **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Statistics** tab.
3. Select a radio index from the table displayed in the Statistics screen and click the **Graph** button.



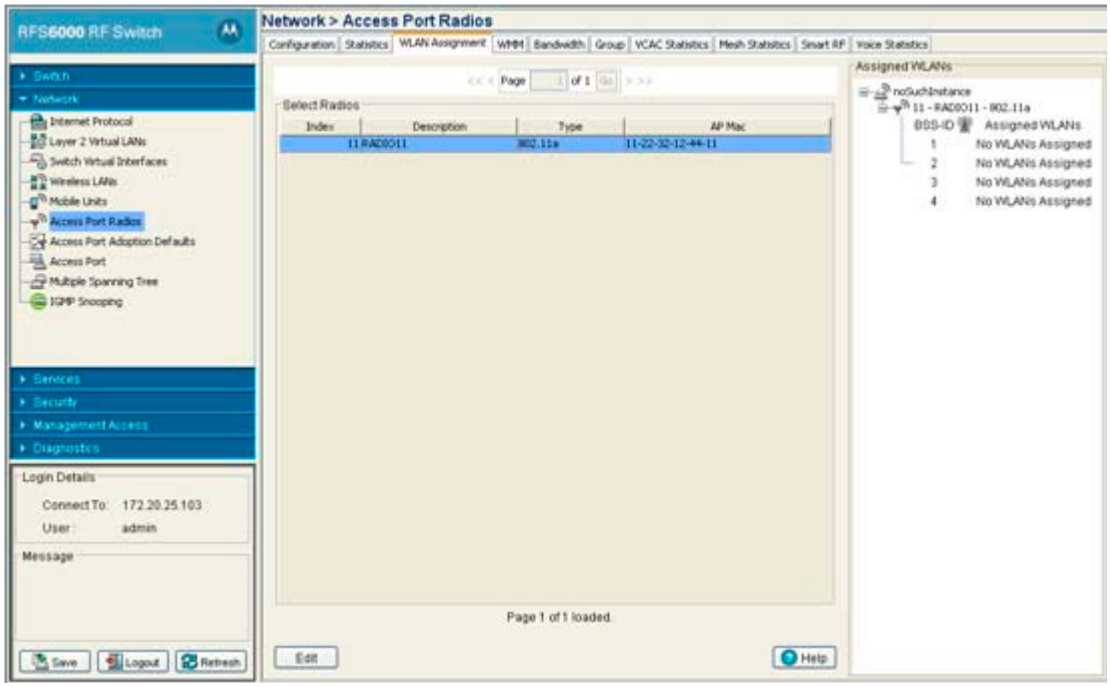
4. Select a checkbox to display that metric charted within the graph. Do not select more than four checkboxes at any one time.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **Close** to exit the Graph and return to the parent Access Port Radios Statistics screen.

4.7.3 Configuring WLAN Assignment

The **WLAN Assignment** tab displays a high-level description of the radio. It also displays the radios WLAN and BSSID assignments on a panel on the right-hand side of the screen.

To view existing WLAN Assignments:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **WLAN Assignment** tab.
3. Select a radio from the table to view WLAN assignment information.



The WLAN Assignment tab is divided into two fields; **Select Radios** and **Assigned WLANs**.

4. Refer to the **Select Radios** field for the following information**:**

Index	Displays the numerical index (device identifier) used with the radio. Use this index (along with the radio description) to differentiate the radio from other radios with similar configurations.
Description	Displays a description of the Radio. Modify the description as required to name the radio by its intended coverage area or function.
Type	Displays whether the radio is an 802.11a radio or an 802.11 bg radio.
AP Mac	Displays the MAC address of the port in AA-BB-CC-DD-EE-FF format.

The **Assigned WLANs** field displays the WLANs associated to each BSSID used by the radios within the radio table. There can be up to 16 WLANs associated with each BSS. Out of these, one WLAN must be the primary WLAN.

5. Select a WLAN Assignment (by index) and click the **Edit** button to modify its properties.For more information, see *Editing a WLAN Assignment on page 4-109*.
6. To remove an existing WLAN from the list available for WLAN assignment, select the WLAN and click the **Delete** button.

4.7.3.1 Editing a WLAN Assignment

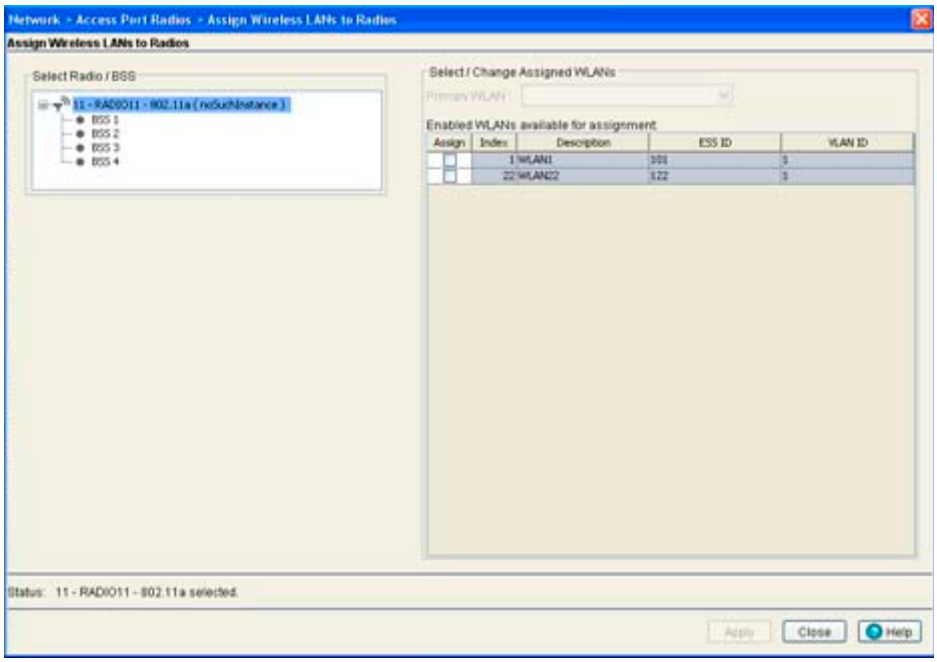
The properties of an existing WLAN assignment can be modified to meet the changing needs of your network,

To edit an exiting WLAN assignment:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **WLAN Assignment** tab.

3. Select a radio from the table and click the **Edit** button.

   The **Select Radio/BSS** field displays the WLANs associated to each of the BSSIDs used by the radios within the radio table. Use **Select/Change Assigned WLANs** field to edit the WLAN assignment.



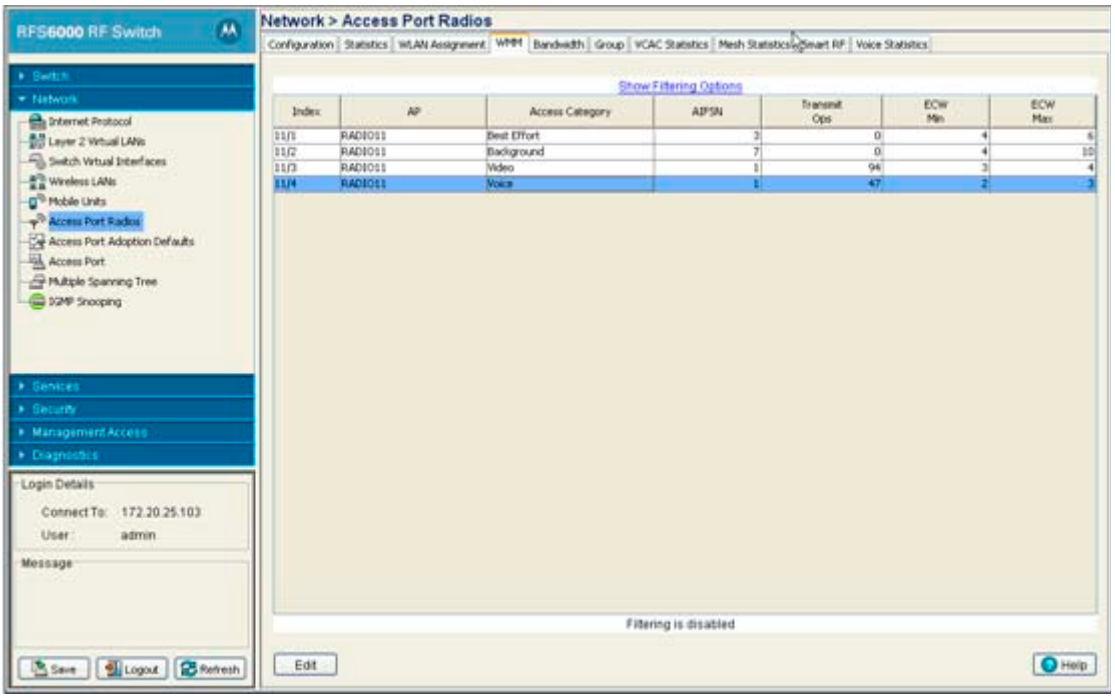
4. Select any of the WLANs from the table to unassign/disable it from the list of available WLANs.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click the **Apply** button to save the modified WLAN assignment.
7. Click **Close** to exit the screen without committing updates to the running configuration.

4.7.4 Configuring WMM

Use the **WMM** tab to review each radio's current index (numerical identifier), the Access Category that defines the data type (Video, Voice, Best Effort and Background) as well as the transmit intervals defined for the target access category.

To view existing WMM Settings:

1. Select **Network > Access Port Radios** from the main menu tree.
2. Click the **WMM** tab.



WMM information displays per radio with the following information:

Index	Displays the identifier assigned to each Radio index, each index is assigned a unique identifier such as (1/4, 1/3, etc.).
AP	Displays the name of the Access Port associated with the index. The Access Port name comes from the description field in the Radio Configuration screen.
Access Category	Displays the Access Category currently in use. There are four categories: Video, Voice, Best Effort and Background. Click the Edit button to change the current Access Category. Ensure the Access Category reflects the radio's intended network traffic.
AIFSN	Displays the current Arbitrary Inter-frame Space Number. Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will causes lower-priority traffic to wait longer before trying to access the medium.
Transmit Ops	Displays the maximum duration a device can transmit after obtaining a transmit opportunity.
ECW Min	Displays the ECW Max to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
ECW Max	Displays the ECW Min to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.

3. Use the Filter Options facility (by clicking the Show Filter Options link) to specify if information is filtered by Index (default setting), AP, Access Category, AIFSN, Transmit Ops, CW Min or CW Max. Select **Turn Filtering Off** to disable filtering.

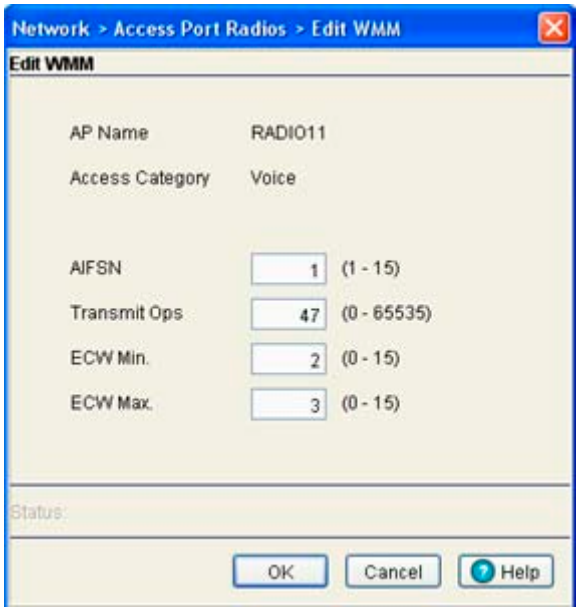
4. Select a radio and click the **Edit** button to modify its properties. For more information, see *Editing WMM Settings on page 4-112*.

4.7.4.1 Editing WMM Settings

Use the Edit screen to modify a WMM profile's properties (AIFSN, Tx Op, Cw Min and CW Max). Modifying these properties may be necessary as Access Categories are changed and transmit intervals need to be adjusted to compensate for larger data packets and contention windows. Use *Configuring WMM on page 4-110* to configure downstream traffic parameters. WLAN WMM configuration affects your upstream traffic parameters.

To edit existing WMM Settings:

1. Select **Network > Access Port Radios** from the main menu tree.
2. Click the **WMM** tab.
3. Select a radio from the table and click the **Edit** button to launch a screen displaying the WMM configuration for that radio.



4. Enter a number between 0 and 15 for the **AIFSN** value for the selected radio.

   The AIFSN value is the current Arbitrary Inter-frame Space Number. Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will causes lower-priority traffic to wait longer before trying to access the medium.

5. Enter a number between 0 and 65535 for the **Transmit Ops** value.

   The Transmit Ops value is the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set higher.

6. Enter a value between 0 and 15 for the Extended Contention Window minimum (**ECW Min**) value.

   The **ECW Min** is combined with the **ECW Max** to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority (video or voice) traffic.

7. Enter a value between 0 and 15 for the Extended Contention Window maximum (**ECW Max**) value.

   The **ECW Max** is combined with the **ECW Min** to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority (video or voice) traffic.

8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

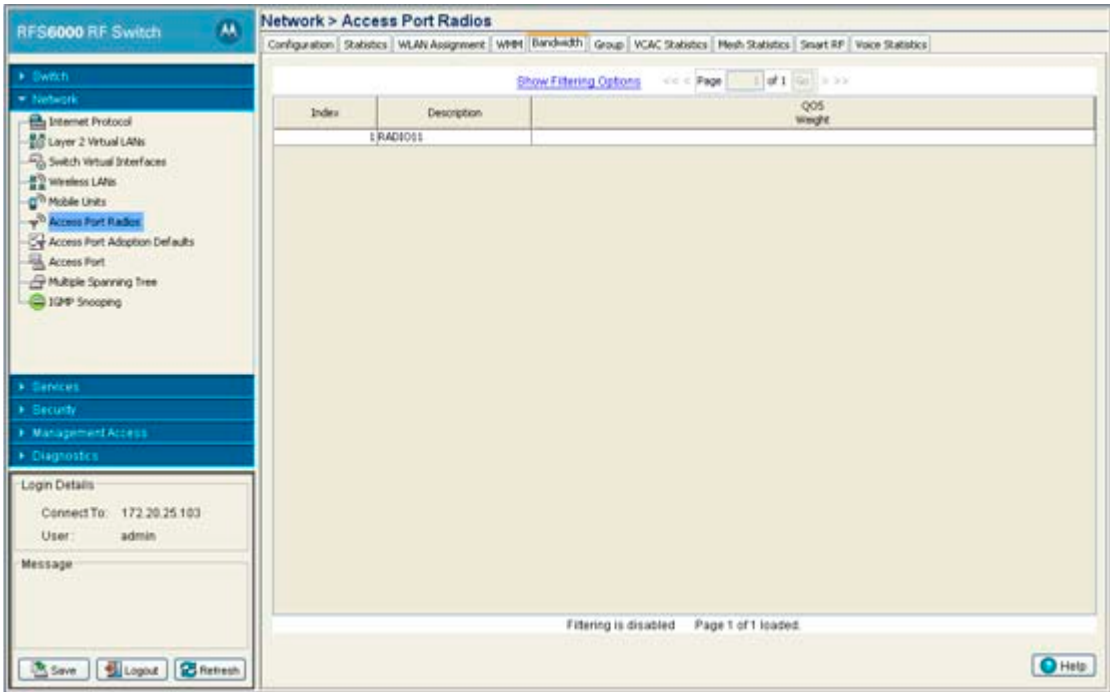
4.7.5 Configuring Access Point Radio Bandwidth

Refer to the **Bandwidth** tab to view the QoS weight associated with each radio when added to a WLAN. The weight represents the switch priority assigned to the traffic transmitted from the radio for the WLAN.

For information on revising the weight assigned to each radio in respect to its intended operation within its assigned WLAN, see *Editing the WLAN Configuration on page 4-26*.

To view existing radio bandwidth weight settings:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Bandwidth** tab.



Bandwidth information displays per radio with the following data:

Index — The Index is the numerical index (device identifier) used with the device radio. Use this index (along with the radio name) to differentiate the radio from other device radios.

Description	The displayed name is the name used with the device radio. Use this name (along with the radio index) to differentiate the radio from other device radios.
QoS Weight	Displays the Quality of Service weight for the AP. The default value for the weight is 1. AP QoS will be applied based on the QoS weight value with the higher values given priority.

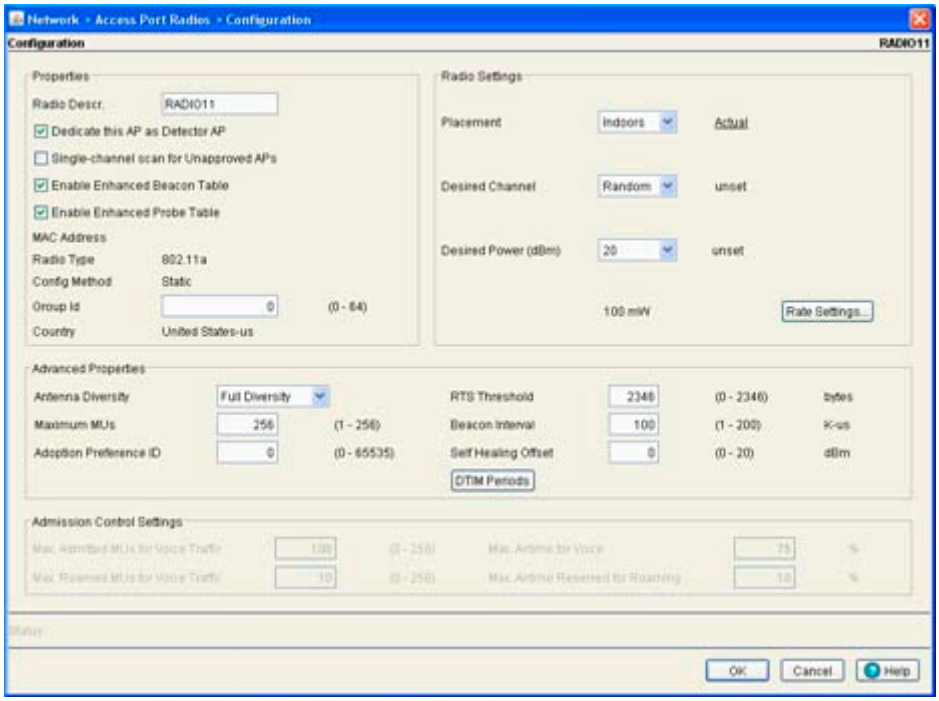
4.7.6 Configuring Radio Groups for MU Load Balancing

In order to do MU load balancing, radios must be grouped. Usually, two radios with similar characteristics and geographically close to each other can be grouped together.

By default, a radio is not in any group and the load balancing algorithm would not apply to it.

To configure a group of radios together:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Go to the **Configuration** tab.
3. Select a radio you wish to add to a group and click the **Edit** button.



4. Enter the **Group ID** for the group you wish to add the selected radio to.
5. Click **OK** to save the changes.
6. Repeat steps 3 through 5 for each radio you wish to add to groups.
7. When you have finished adding radios to groups, click the **Apply** button on the **Configuration** tab to save your changes.
8. To verify the radio groups click on the **Groups** tab to view configured radio groups. For more information on viewing radio groups refer to *Viewing Access Point Radio Groups on page 4-115*.

4.7.6.1 Viewing Access Point Radio Groups

Refer to the **Groups** tab to view the **Group ID** and **Index** associated with each radio when added to a WLAN.

To view existing radio group settings:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Group** tab.

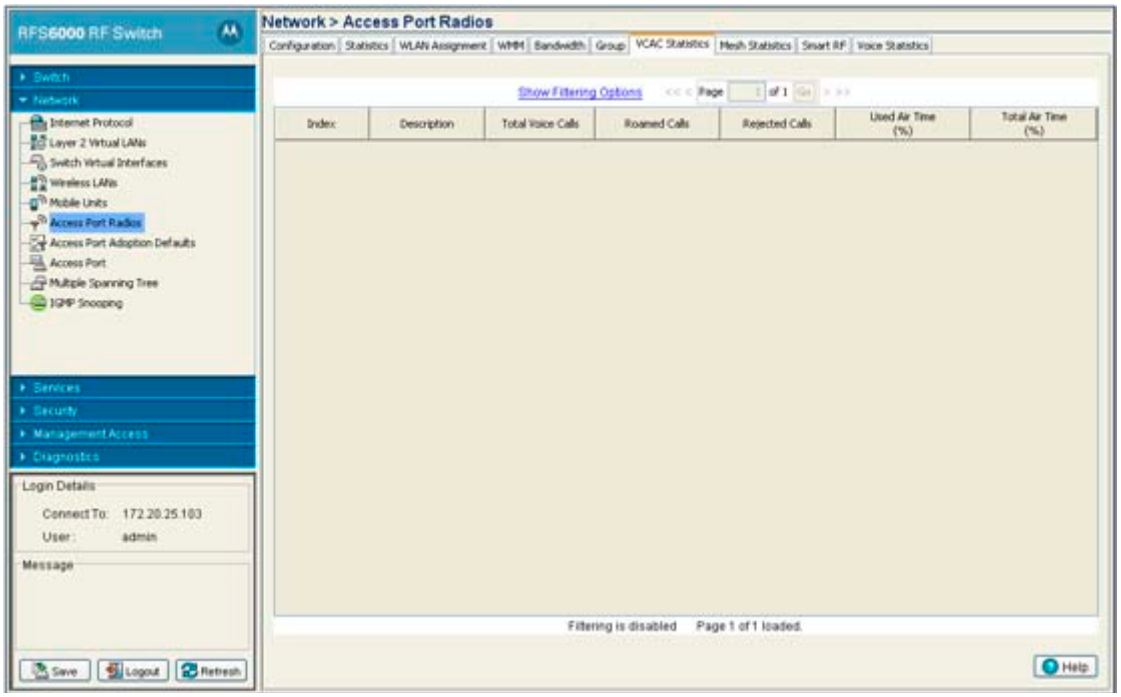
Group information displays per radio with the following data:

Group Id	Displays the Group Id associated with each adopted radio.
Radio Configured Index	The Index is the numerical index (device identifier) used with the device radio. Use this index (along with the radio name) to differentiate the radio from other device radios.

4.7.7 Viewing Active Calls (VCAC) Statistics

To view active call statistics:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **VCAC Statistics** tab.



3. The following statistics are displayed:

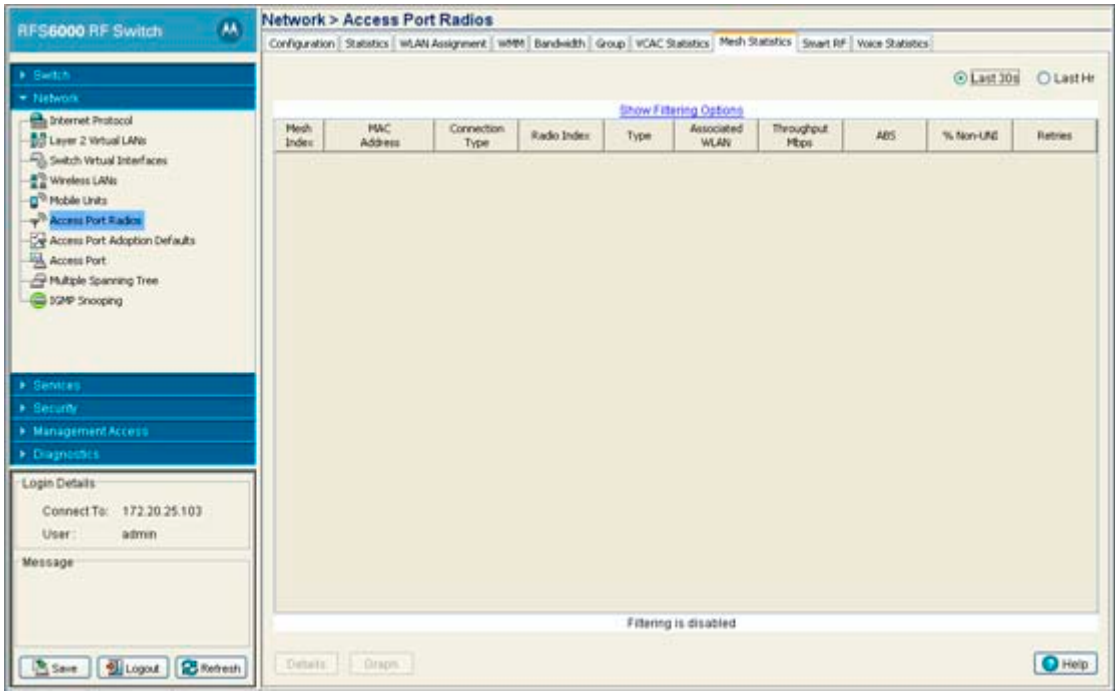
Index	Displays the numerical identifier assigned to each Access Port.
Description	Displays the names assigned to each of the APs. The AP name can be configured on the Access Port Radios Configuration page.
Total Voice Calls	Displays the total number of voice calls attempted for each Access Port.
Roamed Calls	Displays the total number of voice calls that were roamed from each Access Port.
Rejected Calls	Displays the total number of voice calls rejected by each Access Port. Calls may be rejected if the call doesn't meet the TPSEC Admission Control requirements for the AP or when an AP would not be able to provide the necessary QoS for the call.
Used Air Time (%)	Displays the total percentage of air time that each Access Port has dedicated to voice calls.
Total Air Time (%)	Displays the total percentage of air time allocated for TPSEC clients.

4.7.8 Viewing Mesh Statistics

To view Mesh Statistics:

1. Select **Network** > **Access Port Radios** from the main menu tree.

2. Click the **Mesh Statistics** tab.



3. The following statistics are displayed:

Mesh Index	Displays the numerical identifier assigned to each mesh member AP.
MAC Address	Displays the *Media Access Control* (MAC) address for each Access Port.
Connection Type	Displays the connection type for each Access Port.
Radio Index	The Radio Index is a numerical value assigned to the radio as a unique identifier. For example; 1, 2, or 3. The index is helpful for differentiating radios of similar type and configuration.
Type	Displays the radio type of the corresponding APs. Available type are: • *802.11a* • *802.11an* • *802.11b* • *802.11bg* • *802.11bgn*
Associated WLAN	Displays the WLAN that each Access Port is associated to.
Throughput Mbps	Throughput Mbps is the average throughput in Mbps on the selected Access Port.
ABS	Average Mbps is the average throughput in Mbps on the selected Access Port.
% Non-UNI	% Non-Uni is the percentage of the total packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the total number of retries for each Access Port.

4. Select a mesh index from amongst those displayed and select the **Details** button for additional (more granular) information on the mesh index selected.
5. Select a mesh index from those displayed and click the **Graph** button for additional radio performance information in graphical format.

4.7.9 Smart RF

When invoked by an administrator, Smart RF (or self-monitoring at run time) instructs radios to change to a specific channel and begin beaconing using their maximum available transmit power. Within a well planned deployment, any associated radio should be reachable by at least one other radio. The Smart RF feature 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.

Smart RF management is comprised of the following two phases:

- *Smart RF Calibration Phase*
- *Smart RF Monitoring Phase*

Smart RF is well suited for clustered environments. Smart RF interacts with a number of existing features, (such as radio detection, MU load balancing and self-healing).

4.7.9.1 Smart RF Calibration Phase

Smart RF calibration is initiated by an administrator during initial deployment or can be scheduled at a specified frequency or time of the day. Smart RF instructs adopted radios to scan legal channels and measure signal strength from associated radio and other device signals detected within the environment.

Smart RF conducts the following network management activities:

- Automatically calibrates associated radio's maximum power capability
- Automatically assigns certain radios to be detectors
- Automatically assign channels to radios to avoid channel overlap and interference from external RF sources
- Automatically calculates the transmit power of working radios
- Automatically configures self-healing parameters. Radio assume the roles of caretaker and caregiver. When a radio is down, it is referred to as the caretaker. Neighbor radios raising their transmit power to cover for the failed radio are referred to as caregivers. Smart RF calibration automatically chooses caregiver radios along with the power needed to cover.

4.7.9.2 Smart RF Monitoring Phase

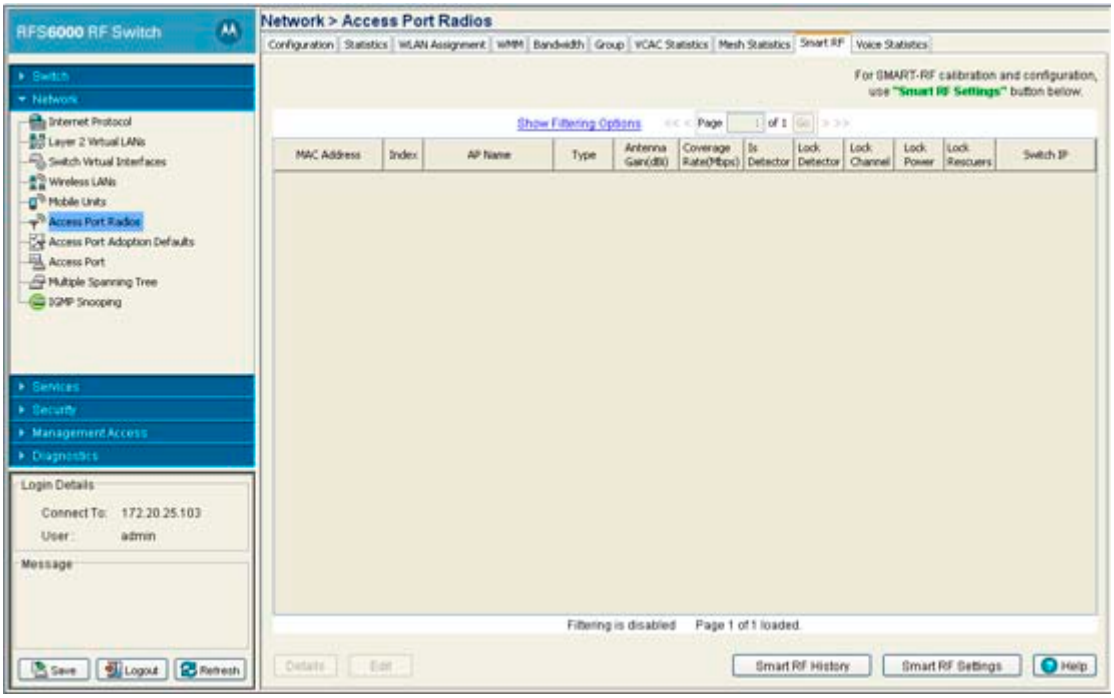
Smart RF monitoring occurs continuously. It includes the following monitoring activities:

- Self-healing to monitor whether a radio is down
- Interference monitoring using retry stats
- Defines coverage holes and discerns transmit rates and MU signal strength. When necessary, Smart RF increases MU power to maintain coverage
- Extensible to future smart-tuning. For example, distinguish between AP to AP interference and static interference

4.7.9.3 Viewing Smart RF Information

To view Smart RF information:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Smart RF** tab.

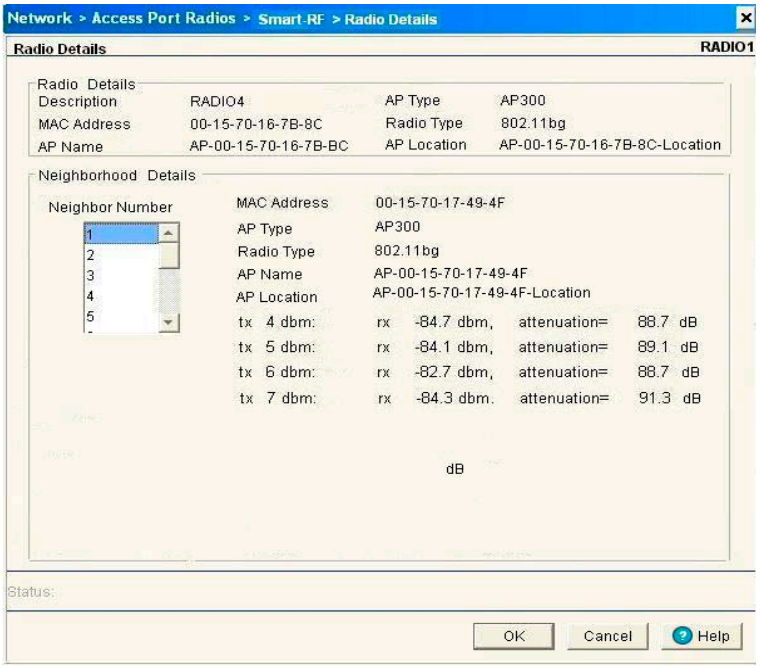


3. The following **Smart RF** details are displayed:

MAC Address	Displays the *Media Access Control (*MAC) Address of each of the APs in the table.
Index	Displays the numerical identifier assigned to each detector AP used in Smart RF calibration.
AP Name	Displays the names assigned to each of the APs. The AP name can be configured on the Access Port Radios Configuration page.
Type	Displays the radio type of the corresponding APs. Available type are: • *802.11a* • *802.11an* • *802.11b* • *802.11bg* • *802.11bgn*
Antenna Gain (dBi)	Displays the current antenna gain value in dBi for each Access Port.
Coverage Rate (Mbps)	Displays the current coverage rate for each Access Port based on the Smart RF settings.
Is Detector	Displays whether or not an Access Port is a detector or not.Detector status is determined through Smart RF based on coverage and location of other APs in the network.

Lock Detector	Displays whether or not each Access Port is locked in detector status.
Lock Channel	Displays whether or not each Access Port is locked to a specific channel.
Lock Power	Displays whether or not each Access Port is locked to a specific power level.
Lock Rescuers	Displays whether or not each Access Port is locked to group of rescuer APs.
Switch IP	Displays the IP address of the

4. To view the details of individual radio Smart RF information, select a radio from the list and click the **Details** button



5. The **Radio Details** section shows individual section displays the following information:

Description	Displays a description of the Radio. Modify the description as required to name the radio by its intended coverage area or function.
MAC Address	Displays the *Media Access Control* (MAC) Address of the selected AP.
AP Name	Displays the name assigned to the AP. The AP name can be configured on the Access Port Radios Configuration page.
AP Type	Displays the type of Access Port detected. The switches support Motorola AP 100, AP300 model Access Ports and AP-4131, AP-5131 and AP-7131 model Access Points.

Radio Type	Displays the radio type of the corresponding APs. Available type are: • *802.11a* • *802.11an* • *802.11b* • *802.11bg* • *802.11bgn*
AP Location	Displays the current location for the selected AP. The location can be configured on the Access Port Radios Configuration page.

6. The **Neighbor Details** section allows you to select detected neighbor radios and view the following information:

MAC Address	Displays the Media Access Control (MAC) Address of the selected AP.
AP Type	Displays the type of Access Port detected. The switches support Motorola AP 100, AP300 model Access Ports and AP-4131, AP-5131 and AP-7131 model Access Points.
Radio Type	Displays the radio type of the corresponding APs. Available type are: • *802.11a* • *802.11an* • *802.11b* • *802.11bg* • *802.11bgn*
AP Name	Displays the name assigned to the AP. The AP name can be configured on the Access Port Radios Configuration page.
AP Location	Displays the current location for the selected AP. The location can be configured on the Access Port Radios Configuration page.
tx/rx dbm	Displays the transmit, receive and attenuation information of the selected neighbor radio.

4.7.9.4 Editing Smart RF Radio Settings

To edit Smart RF radio settings:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Smart RF** tab.
3. Select a radio from the table and click the **Edit** button.

   The radio settings are divided into the following three sections:

- *Properties*
- *Radio Rescuer Settings*
- *Advanced Properties*

4. The **Properties** section displays the following information:

Description	Displays a description of the Radio. Modify the description as required to name the radio by its intended coverage area or function.
MAC Address	Displays the Media Access Control (MAC) Address of the selected AP.
AP Name	Displays the name assigned to the AP. The AP name can be configured on the Access Port Radios Configuration page.
AP Type	Displays the type of Access Port detected. The switches support Motorola AP 100, AP300 model Access Ports and AP-4131, AP-5131 and AP-7131 model Access Points.
Radio Type	Displays the radio type of the corresponding APs. Available type include: • *802.11a* • *802.11an* • *802.11b* • *802.11bg* • *802.11bgn*
AP Location	Displays the current location for the selected AP. The location can be configured on the Access Port Radios Configuration page.

5. The **Radio Rescuer Settings** section allows you to configure the following radio rescuer settings and information:

Available Radios	Displays a list of radios available to be used as rescuer radios.
Rescuer Radios	Displays a list of radios that have been configured as Rescuer Radios.
Add	Click the Add button to add a selected radio or radios from the Available Radios list into the Rescuer Radios list.
Remove	Click the **Remove** button to remove a selected radio or radios from the Recuer Radios list.
Rescuer MAC	Displays the Media Access Control (MAC) Address of the selected Rescuer Radio.
AP Name	Displays the configured AP Name for the selected Rescuer Radio.
AP Location	Displays the configured AP Location for the selected Rescuer Radio.The location can be configured on the Access Port Radios Configuration page.
Rescuer Power	Displays the current power level of the selected Rescuer Radio.
Rescuer Attenuation	Displays the current Attenuation power for the selected Rescuer Radio.

6. The **Advanced Properties** section contains the following configurable items:

Antenna Gain	Specify the desired antenna gain in dBi for the selected radio.
Coverage Rate	Specify the desired coverage rate for the selected radio from the drop-down menu options.
Lock Detector	Enable or disable radio detector mode lock for the selected radio.
Lock TX Power	Check this box to lock the TX power for the selected radio.

Lock Channel	Check this box to lock the channel for the selected radio.
Lock Rescuer	Check this box to lock the rescuer radio for the selected radio.

7. Click **OK** to use the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.7.9.5 Viewing Smart RF History

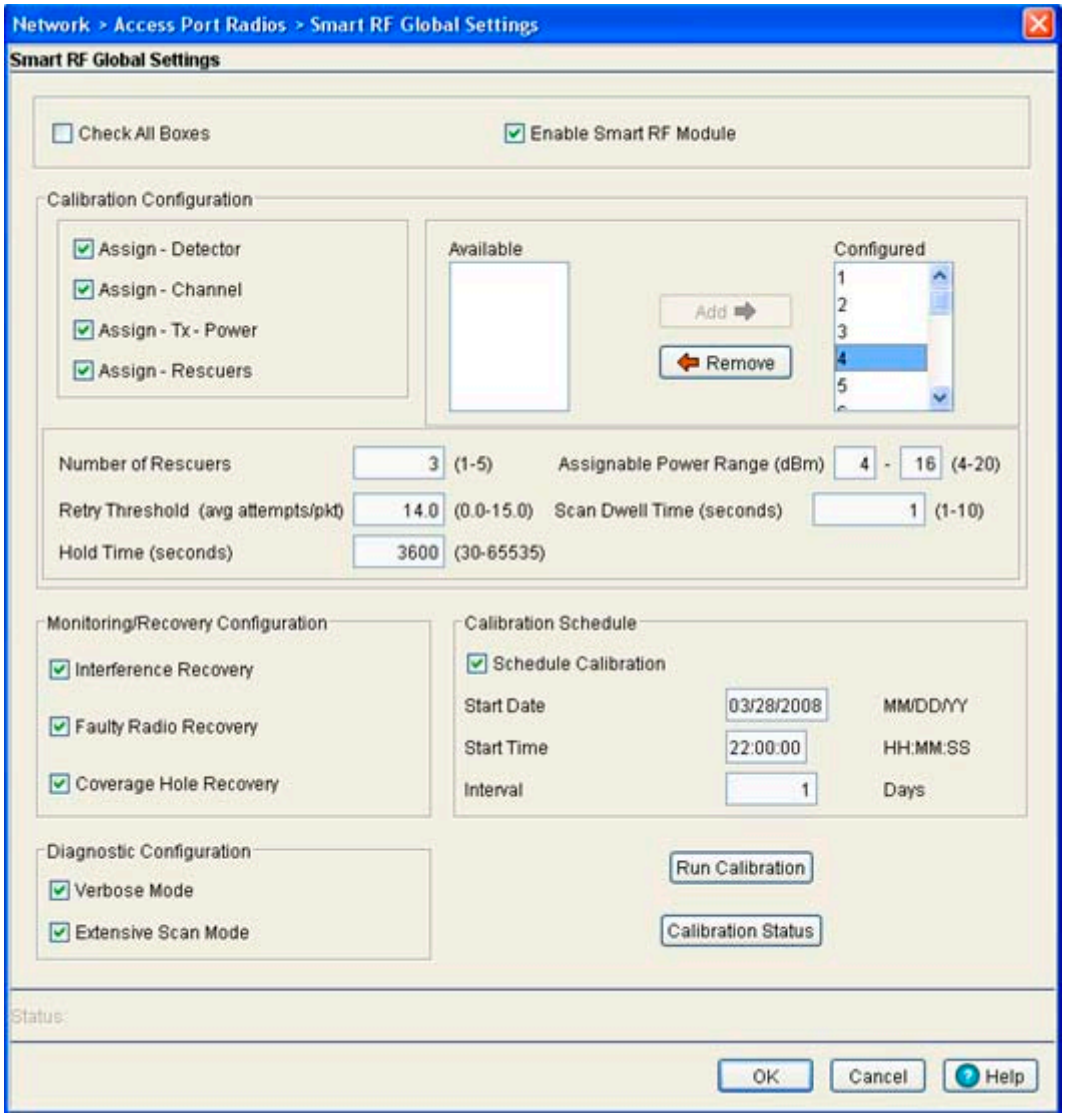
To view Smart RF history:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Smart RF** tab
3. Click the **Smart RF History** button.
4. The **Smart RF History** window displays the **Index** number and **Assignment History** of Smart RF activity.

4.7.9.6 Configuring Smart RF Settings

To configure Smart RF settings:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Smart RF** tab.
3. Click the **Smart RF Settings** button.



4. Click the **Check All Boxes** option in the Smart RF Global Settings dialogue to check every box in the configuration window. To uncheck all boxes click this box a second time.
5. Check the **Enable Smart RF Module** box to enable Smart RF functions on the switch.

   The remainder of the Smart RF Settings screen is divided into the following four sections:

   - *Calibration Configuration*
   - *Monitoring/Recovery Configuration*
   - *Diagnostic Configuration*
   - *Calibration Schedule*
6. The **Calibration Configuration** section contains the following RF calibration settings:

Assign - Detector	Check this box to enable automatic assignment of radio detectors.
Assign - Channel	Check this box to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources.

Assign - Tx Power	Check this box to enable automatic assignment of transmit power.
Assign - Rescuers	Check this box to enable automatic assignment of rescuers along with rescuing power.
Available	The Available box lists all available channels for Smart RF.
Configured	The Configured box lists all channels enabled for Smart RF.
Add	To add a channel to the configured list, select one or more channel from the Available box and click the Add button.
Remove	To remove a channel from the configured list, select one or more channels from the Available box and click the Remove button.
Number of Rescuers	Assign a number of radios to dedicate as rescuers. The valid range is between 1 and 5.
Retry Threshold (avg attempts/pkt)	Specify the retry threshold which is the average number of retries per packet to cause a radio to re-run channel selection.
Hold Time (seconds)	Specify the global hold time in seconds. The valid range is between 30 and 65535 seconds.
Assignable Power Range (dBm)	Specify a valid range for the power in dBm. The valid minimum is 4 and maximum is 20.
Scan Dwell Time (seconds)	Specify the RF Scan Dwell Time in seconds. The valid range is between 1 and 10 seconds.

7. The **Monitoring/Recovery Configuration** section contains the following configuration items:

Interference Recovery	Check this box to enable monitoring for interference and self-healing it by rescuer.
Faulty Radio Recovery	Check this box to enable monitoring for defective radio and self-healing by its rescuer.
Coverage Hole Recovery	Check this box to enable monitoring and recovering for coverage holes.

8. The **Diagnostic Configuration** section contains the following two configuration items:

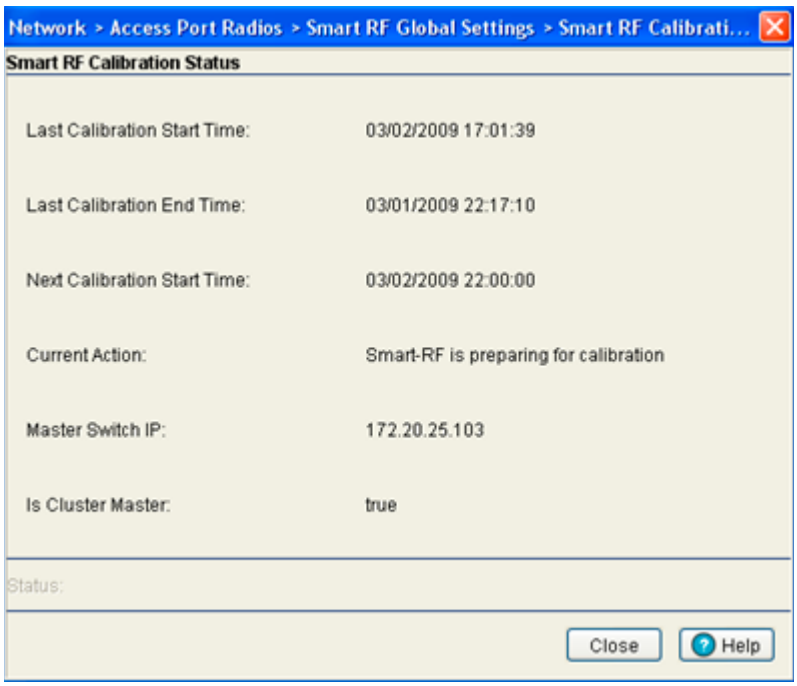
Verbose Mode	Check this box to enable verbose diagnostic information for Smart RF.
Extensive Scan Mode	Check this box to enable extensive scan mode when using Smart RF.

9. The **Calibration Schedule** contains the following calibration settings:

Schedule Calibration	Check this box to enable scheduled RF Calibration.
Start Date	If scheduled RF Calibration is enabled, enter a start date in MM/DD/YY format for the start date of scheduled calibration.

Start Time	If scheduled RF Calibration is enabled, enter a start time in HH:MM:SS format for the start time of scheduled calibration.
Interval	If scheduled RF Calibration is enabled, enter an interval in days for how long the scheduled calibration should continue after its start date.

10. Once the settings have been configured, click the **Run Calibration** button to start a Smart RF calibration.
11. Click the **Calibration Status** button to open a dialogue with the following calibration status information



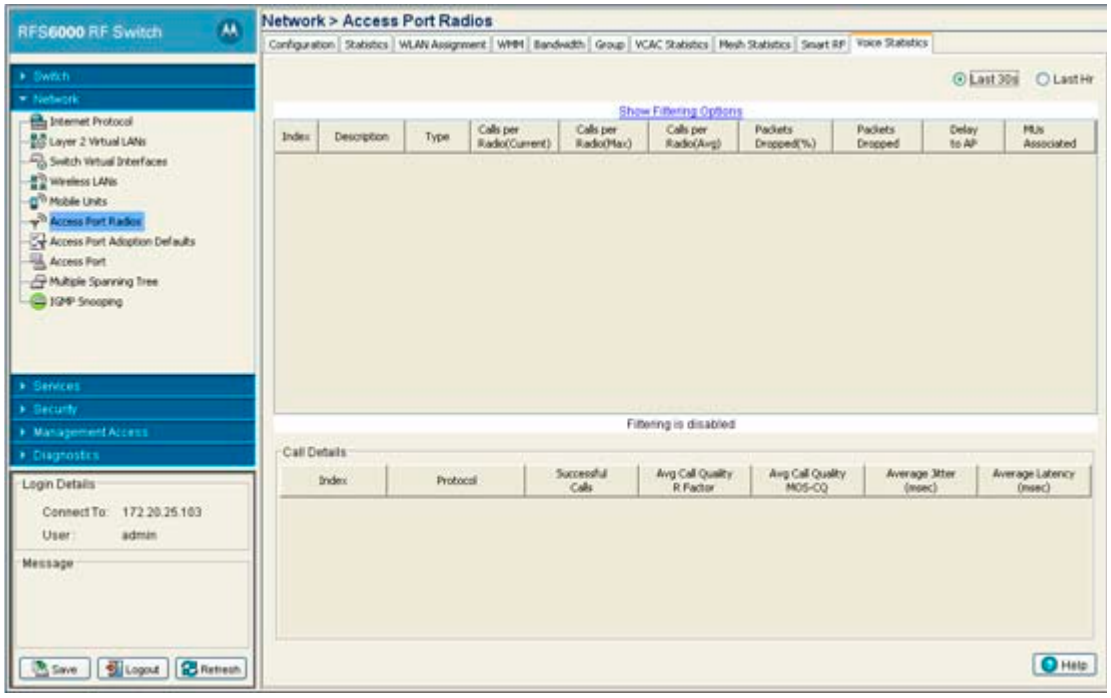
Last Calibration Start Time	Displays the date and time that the last Smart RF calibration began.
Last Calibration End Time	Displays the date and time that the last Smart RF calibration ended.
Next Calibration Start Time	Displays the date and time scheduled for the next Smart RF calibration.
Current Action	Displays what the Smart RF engine is currently doing. If there is a scan in process it will be displayed here.
Master Switch IP	Displays the IP address of the master switch in the cluster.
Is Cluster Master	Displays the cluster master status of the switch. If the switch is the master it will display **true**, otherwise it will display **false**.

12. Click **OK** to use the changes to the running configuration and close the dialog.
13. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.7.10 Voice Statistics

To view Voice Statistics:

1. Select **Network** > **Access Port Radios** from the main menu tree.
2. Click the **Voice Statistics** tab.



3. The following statistics are displayed:

Index	Displays the numerical identifier assigned to each Access Port.
Description	Displays the names assigned to each of the APs. The AP name can be configured on the Access Port Radios Configuration page.
Type	Displays the radio type of the corresponding APs. Available type are: • *802.11a* • *802.11an* • *802.11b* • *802.11bg* • *802.11bgn*
Calls per radio (Current)	Displays the current number of active voice calls for each Access Port.
Calls per radio (Max)	Displays the maximum number of concurrent voice calls that each Access Port has seen.
Calls per radio (Avg)	Displays an average number of calls active on each Access Port.
Airtime for Voice (%)	Displays the percentage of total airtime that each Access Port has dedicated to voice calls.

Packets Dropped (%)	Displays a percentage of the packets that each Access Port has dropped in comparison to the total number of packets.
Packets Dropped	Displays the total number of packets dropped by each Access Port.
Delay to AP	Displays the current delay time for each Access Port.
MUs Associated	Displays the total number of mobile units associated with each Access Port.

4. Selecting a radio from the table will display the following details of individual calls:

Index	Displays the numerical identifier assigned to each MU.
Protocol	Displays which voice protocol is being used for the selected call. Voice protocols include: • *SIP* • *TPSEC* • *Spectralink* • *H.323*
Successful Calls	Displays the number of successful calls for the displayed MUs.
Avg Call Quality R Factor	Displays the average call quality using the R Factor scale. The R Factor method rates voice quality on a scale of 0 to 120 with a higher score being better. If the R Factor score is lower than 70 it is likely users will not be satisfied with the voice quality of calls.
Avg Call Quality MOS-CQ	Displays the average call quality using the Mean Opinion Score (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 is likely that users will not be satisfied with the voice quality of calls.
Average Jitter (msec)	Displays the average jitter time for calls on the displayed MUs. Jitter is delays on the network that can result in a lag in conversations. A jitter score higher than 150ms is likely to be noticed by end users during a call.
Average Latency (msec)	Displays the average latency in miliseconds for calls on the selected MUs.

4.8 Viewing Access Port Adoption Defaults

Use the **Access Port Adoption Defaults** screen to configure the current radio adoption configurations, assigning WLANs and security schemes and to review each radio type, as well as the Access Category that defines which data type (Video, Voice, Best Effort and Background) the radio has been configured to process. It has the following tabs: In a layer 3 environment, the Access Port adoption process is somewhat unique, for more information, see *Configuring Layer 3 Access Port Adoption on page 4-136*.

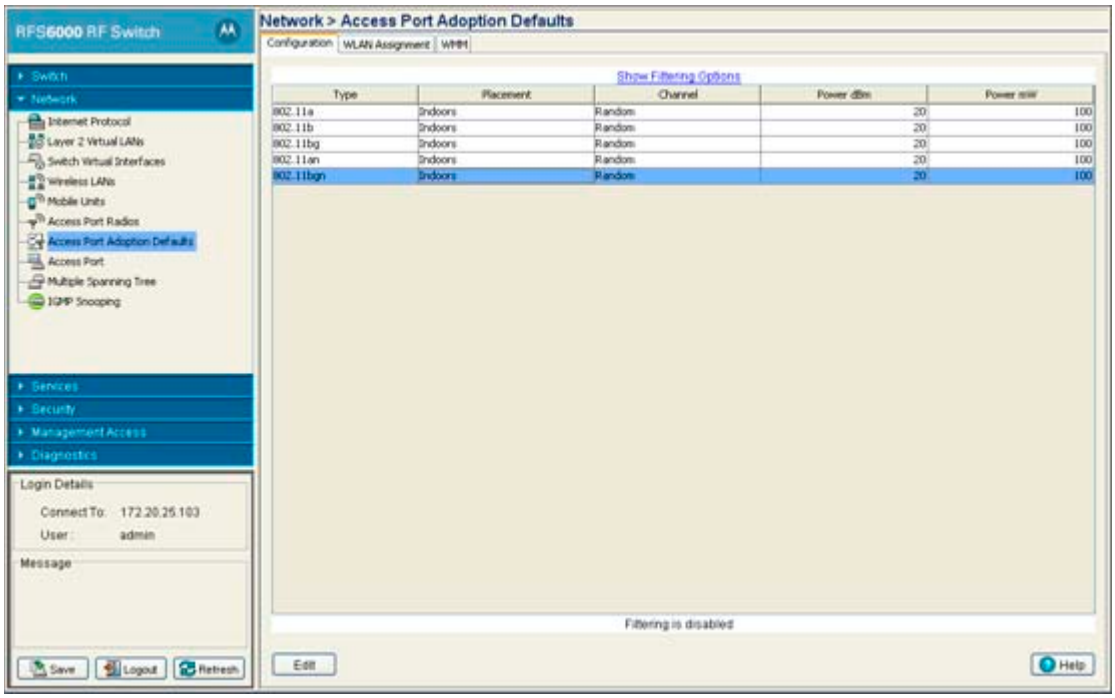
- *Configuring AP Adoption Defaults*
- *Configuring Layer 3 Access Port Adoption*
- *Configuring WLAN Assignment*
- *Configuring WMM*

4.8.1 Configuring AP Adoption Defaults

The **Configuration** tab displays the current radio adoption configuration including radio type, placement, channel setting and power settings. Many of these settings can be modified (as well as radio's current rate settings) by selecting a radio and clicking the **Edit** button. These settings are the default configurations when the radios are set to auto-adopt.

To view existing Radio Configuration information:

1. Select **Network** > **Access Port Adoption Defaults** from the main menu tree.
2. Click the **Configuration** tab.



3. Refer to the following information as displayed within the **Configuration** tab:

Type	Displays whether the radio is an 802.11a radio or an 802.11 bg model radio
Placement	Displays the default placement when an radio auto-adopts and takes on the default settings. Options include Indoor or Outdoor. Default is Indoor.
Channel	Displays the default channel when an radio auto-adopts and takes on the default settings. This value can be a specific channel, Random, or ACS. Random assigns each radio a random channel. ACS (Automatic Channel Selection) allows the switch to systematically assign the channel. Default is random.
Power dBm	Displays the default power when an radio auto-adopts and takes on the default settings. Defaults are 20 dBM for 802.11bg) and 17 dBm for 802.11a.
Power mW	Displays the default transmit power in mW (derived from the Power dBm setting). Defaults are 100 mW for 802.11bg and 50 mW for 802.11a.

4. To modify a radio's adoption defaults, select a radio and click the **Edit** button. For more information, see *Editing Default Access Port Adoption Settings on page 4-130*.

CAUTION: An Access Port is required to have a DHCP provided IP address before attempting layer 3 adoption, otherwise it will not work. Additionally, the Access Port must be able to find the IP addresses of the switches on the network.

To locate switch IP addresses on the network:

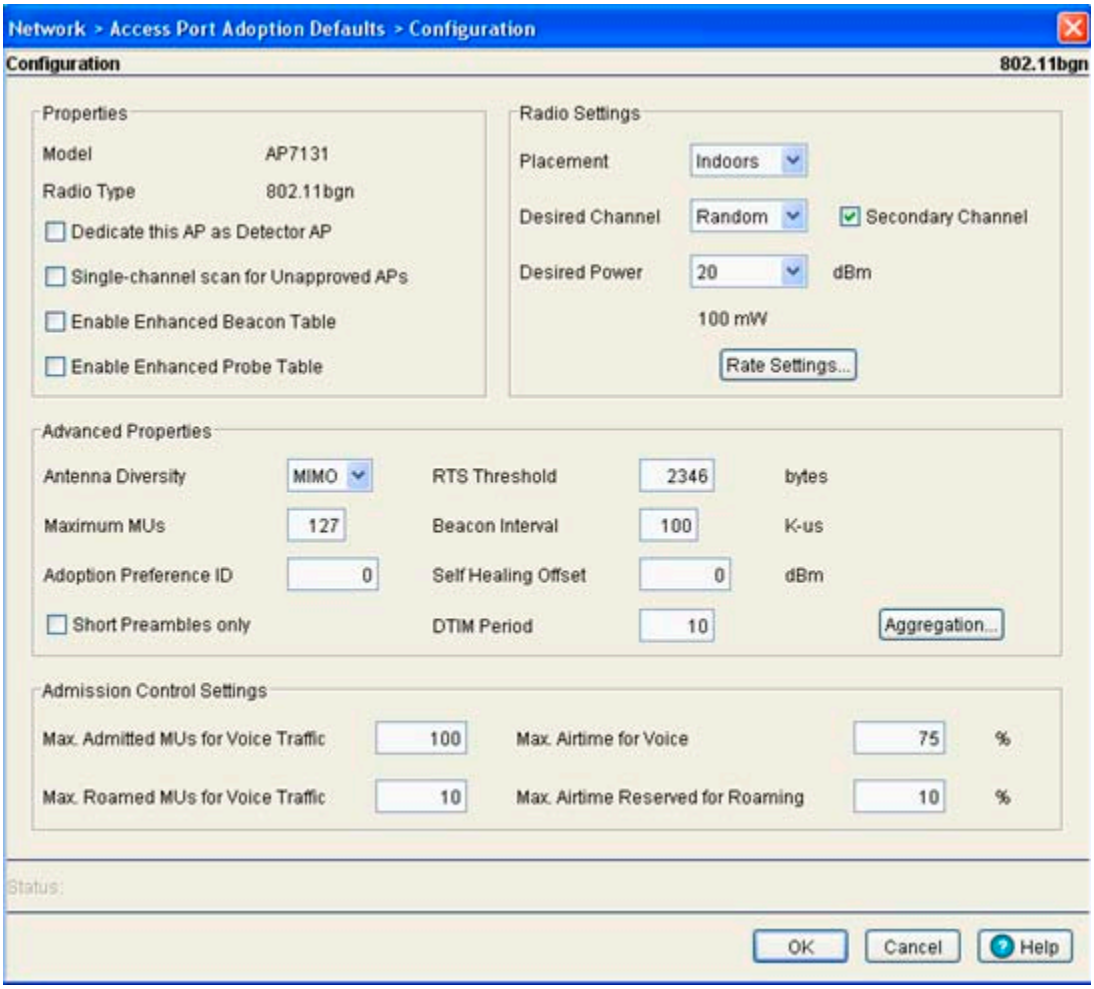
- Configure DHCP option 189 to specify each switch IP address.
- Configure a DNS Server to resolve an existing name into the IP of the switch. The Access Port has to get DNS server information as part of its DHCP information. The default DNS name requested by an AP300 is "Symbol-CAPWAP-Address". However, since the default name is configurable, it can be set as a factory default to whatever value is needed.

4.8.1.1 Editing Default Access Port Adoption Settings

Use the **Edit** screen to dedicate a target radio as a detector radio, as well as change the radios settings (placement, power and channel) and advanced properties (antenna setting, maximum associations, adoption preference etc.).

To edit radio adoption configuration settings:

1. Select **Network Setup** > **Access Port Adoption Defaults** from the main menu tree.
2. Click the **Configuration** tab.
3. Select a radio from the table.
4. Click the **Edit** button to display a screen to change the radio adoption default values for the currently selected radio type (either 802.11a or 802.11bg).



The **Properties** field displays the **Model** family for the selected Access Port. The **Model** is read only and cannot be modified. The **Radio Type** displays the radio type (802.11a or 802.11bg). This value is read only and cannot be modified

5. To use this radio as a detector to identify rogue APs on your network, check the box titled **Dedicate this AP as Detector AP.** Setting this radio as a detector will dedicate this radio to detecting rogue APs on the network. Dedicated detectors do not connect to by clients.
6. Select the **Single-channel scan for Unapproved APs** checkbox to enable the switch to detect rogue devices using its only its current channel of operation.
7. Select the **Enable Enhanced Beacon Table** checkbox to allow the AP to receive beacons and association information.
8. Select the **Enable Enhanced Probe Table** checkbox to allow an AP to forward MU probe requests to the switch.
9. Within the Radio Settings field, configure the **Placement** of the radio as either **Indoors** or **Outdoors**. The setting will affect the selection channel and power levels. Default is Indoor.
10. Select a channel for communications between the Access Port and MUs in the **Desired Channel** field.

    The selection of a channel determines the available power levels. The range of legally approved communication channels varies depending on the installation location and country. The selected channel

can be a specific channel, *Random*, or *ACS*. Random assigns each radio a random channel. ACS (Automatic Channel Selection) allows the switch to systematically assign channels. Default is Random.

11. After first selecting a channel, select a power level in dBm for RF signal strength in the **Desired Power (dBm)** field.

    The optimal power level for the specified channel is best determined by a site survey prior to installation. Available settings are determined according to the selected channel. Set a higher power level to ensure RF coverage in WLAN environments that have more electromagnetic interference or greater distances between the Access Port and MUs. Decrease the power level according to the proximity of other Access Ports. Overlapping RF coverage may cause lost packets and difficulty for roaming devices trying to engage a Access Port. After setting a power level, channel and placement the RF output power for the Access Port is displayed in mW. Default is 20 dBm (802.11bg), 17 dBm (802.11a)**)**

NOTE: After setting a power level, channel and placement the RF output power for the Access Port is displayed below in mW.

12. To configure optional rate settings, click the **Rate Settings** button to display a new dialogue containing rate setting information. Instructions on configuring rate settings are described in *Configuring Rate Settings on page 4-100*.

13. In most cases, the default settings for the **Advanced Properties** section are sufficient for most users. If needed, additional radio settings can be modified for the following properties:

Antenna Diversity	Use the drop-down menu to configure the Antenna Diversity settings for Access Ports using external antennas. Options include: • *Full Diversity* - Utilizes both antennas to provide antenna diversity. • *Primary Only* - Enables only the primary antenna. • *Secondary Only* - Enables only the secondary antenna. Antenna Diversity should only be enabled if the Access Port has two matching external antennas. Default value is **Full Diversity**.
Maximum MUs	Sets the maximum number of MUs that can associate to a radio. The maximum number of stations that can associate to a radio are 256.
Adoption Preference ID	The Adoption Preference ID defines the preference ID of the switch.The value can be set between 1 and 65535. To make the radios preferred, the Access Port preference ID should be same as adoption preference ID. The adoption preference id is used for RP load-balancing. A switch will preferentially adopt Access Ports which have the same adoption-preference-id as the switch itself.
Short Preambles only	If using an 802.11 bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This checkbox does not display if using an 802.11a radio.

RTS Threshold

Specify a *Request To Send* (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports.

RTS is a transmitting station's signal that requests a *Clear To Send* (CTS) response from a receiving station. This RTS/CTS procedure clears the air where many MUs (or nodes) 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.

Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and simply sends (without RTS/CTS) any data frames that are smaller than the threshold.

Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Ports. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of the 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.

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. Default is 2346.

In 802.11b/g mixed RTS/CTS happens automatically. There is no way to disable RTS/CTS unless the network and all the devices used are 802.11g or 802.11a only. The proper co-existence of 802.11b and 802.11g is ensured thru RTS/CTS mechanism. On 802.11g radios CTS-to-self is enabled irrespective of whether or not 11b rates are enabled or disabled.

When ERP Protection is ON, the 11bg radio will perform a CTS-to-self before it transmits the frame.

Beacon Interval

Specify a beacon interval in units of 1,000 microseconds (K-us). This is a multiple of the DTIM value, for example, 100: 10. (See "DTIM Period," below). A beacon is a packet broadcast by the adopted Access Ports to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the radio-port 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. Default is 100 K-us.

DTIM Period	Specify a period for the *Delivery Traffic Indication Message* (DTIM). This is a divisor of the beacon interval (in milliseconds), for example, 10 : 100. (See "Beacon Interval," above). A DTIM is periodically included in the beacon frame transmitted from adopted Access Ports. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates that broadcast and multicast frames (buffered at the Access Port) 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. The default DTIM period is 2 beacons.
Self Healing Offset	When an Access Port increases its power to compensate for a failed Access Port, power is increased to the country's regulatory maximum. Set the Self Healing Offset to reduce the country's regulatory maximum power if Access Ports are situated close to each other or if Access Ports s use external antennas. For additional information on determining the offset value, see the documentation shipped with the Access Port.

14. In the **Max Admitted MUs for Voice Traffic** field, specify the maximum number of MUs allowed to connect to the specified radio for voice traffic. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality. Admission control is only available for TSPEC enabled voice clients.
15. In the **Max Roamed MUs for Voice Traffic** field, specify the maximum number of voice MUs that are allowed to roam to this radio. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality. Admission control is only available for TSPEC enabled voice clients.
16. In the **Max Airtime for Voice** field, specify a maximum percentage out of the radio's total airtime that may be used for voice.
17. In the **Max Airtime for Reserved for Roaming** field, specify a maximum percentage out of the radio's total airtime that may be used for voice MUs which roam from other APs.
18. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
19. Click **OK** to use the changes to the running configuration and close the dialog.
20. Click **Cancel** to close the dialog without committing updates to the running configuration.

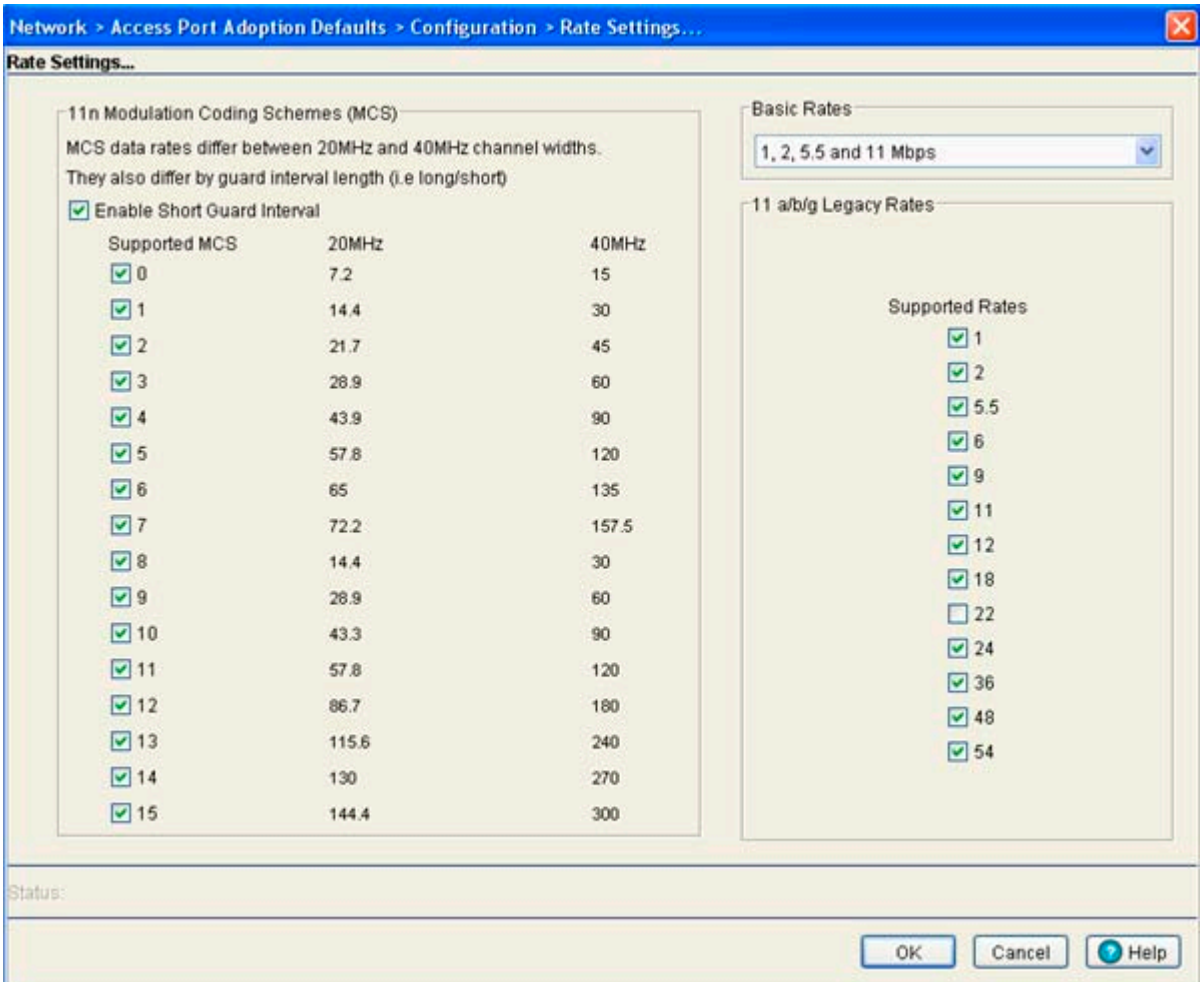
Configuring Rate Settings

Use the **Rate Settings** screen to define a set of basic and supported rates for the target radio. This allows the radio to sync with networks using varying data rates and allows the radio to default to a predefined set of data rates when higher data rates cannot be maintained.

To configure a radio's rate settings:

1. Click the **Rate Settings** button in the radio edit screen to launch a screen wherein rate settings can be defined for the radio.
2. Check the boxes next to all **Basic Rates** you want supported by this radio.

   Basic Rates are used for management frames, broadcast traffic and multicast frames. If a rate is selected as a basic rate it is automatically selected as a supported rate.
3. Check the boxes next to all **Supported Rates** you want supported by this radio.



Supported Rates allow an 802.11 network to specify the data rate it supports. When a station attempts to join the network, it checks the data rate used on the network. If a rate is selected as a basic rate it is automatically selected as a supported rate.

4. Click the **Clear all rates** button to uncheck all of the Basic and Supported rates.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.8.2 Configuring Layer 3 Access Port Adoption

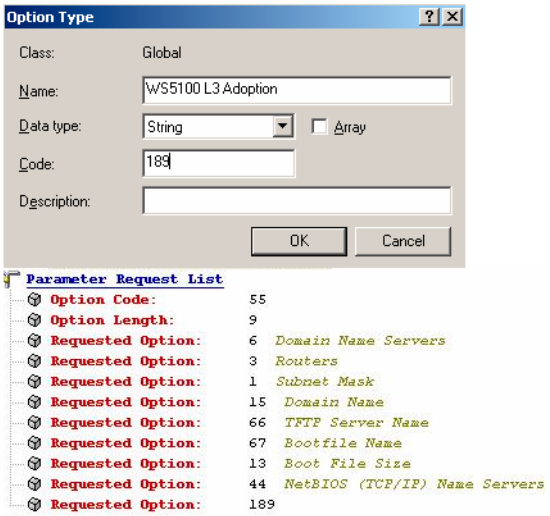
The configuration activity required for adopting Access Ports in a layer 3 environment is unique. In a layer 3 environment, switch discovery is attempted in the following ways:

- *On the local VLAN*
- *Through the DHCP Server*

Initially, the Access Port attempts to find its wireless switch by broadcasting a Hello packet on its local VLAN. During this activity:

1. All switches on the VLAN that receive this Hello packet respond with a parent packet.
2. If no response is received, the Access Port attempts to discover its switch by first obtaining an IP address from a DHCP (or DNS) server and checking the options field within the DHCP response.

   The options field (Option 189) contains a list of switch IP addresses available for the Access Port.



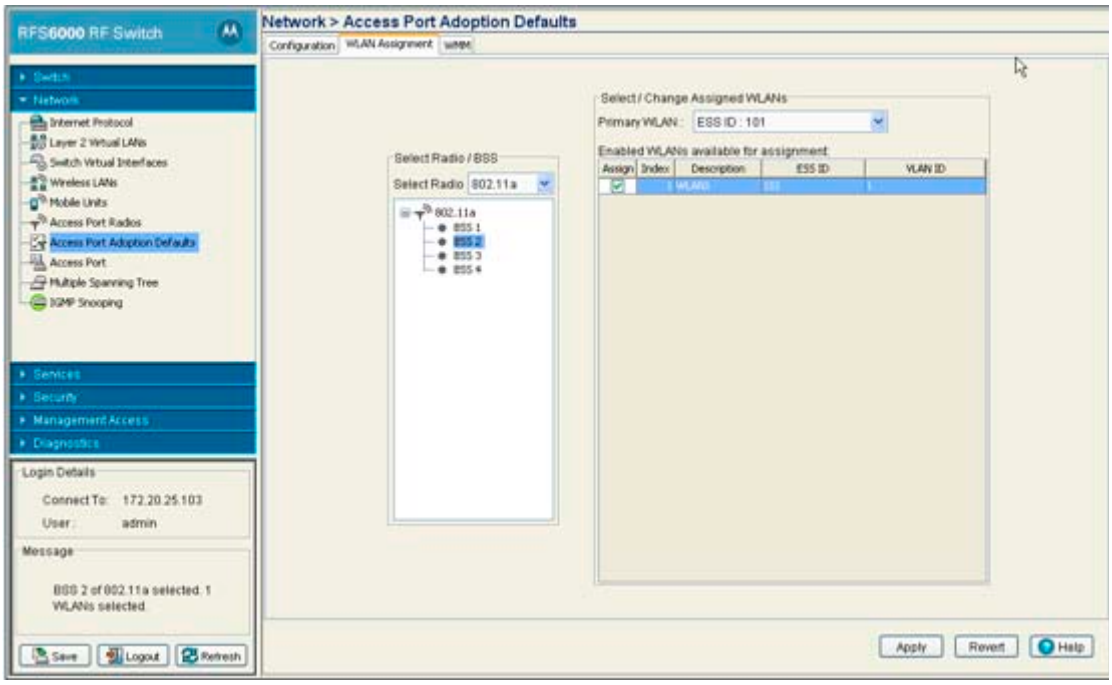
3. The system administrator now programs these options into the DHCP server.
4. If the Access Port finds the list, it sends a unidirectional Hello packet (encapsulated in a UDP/IP frame) to each switch on the list.
5. Each switch that receives such a packet responds with a Parent response.

4.8.3 Configuring WLAN Assignment

Use the **WLAN Assignment** tab to assign WLANs and security schemes.

To view existing WLAN Assignments:

1. Select **Network** > **Access Port Adoption Defaults** from the main menu tree.
2. Click the **WLAN Assignment** tab.



The Assigned WLANs tab displays two fields: **Select Radios/BSS** and **Select/Change Assigned WLANs**.

3. With the **Select Radios/BSS** field, select the radio type to configure (802.11a or 802.11bg) from the **Select Radio** drop-down menu.
4. Select the desired BSS from the **BSS list** or select a **Radio** (802.11a or 802.11bg) to modify.
5. Refer to the **Select/Change Assigned WLAN** field for the following information:

Primary WLAN	If a specific BSS was selected from the **Select Radio/BSS** area, choose one of the selected WLANs from the drop-down menu as the primary WLAN for the BSS. If the radio was selected, the applet will automatically assign one WLAN to each BSS in order, and that WLAN will be set as the **Primary WLAN** for the BSS. If the number of WLANs selected is greater than the number of BSSIDs, the remaining WLANs are included with the last BSS.
Assign	Assign the WLAN(s) to the selected BSS or Radio.
Index	Displays (in ascending order) the numerical index assigned to each SSID. Use the index (along with the WLANs name) as a means of identifying WLANs once assigned to different radio BSSIDs. A BSSID cannot support two WLANs with the same numerical index.
Description	Use the WLAN description (along with the WLANs index) as a means of identifying WLANs assigned to different radio BSSIDs. A BSSID cannot support two WLANs with the same description.
ESS ID	Displays the assigned SSID uniquely distributed between the WLANs assigned to the BSSIDs.
VLAN ID	Displays the VLAN ID of VLANs assigned to WLANs. By default, all WLANs are assigned to VLAN 1.

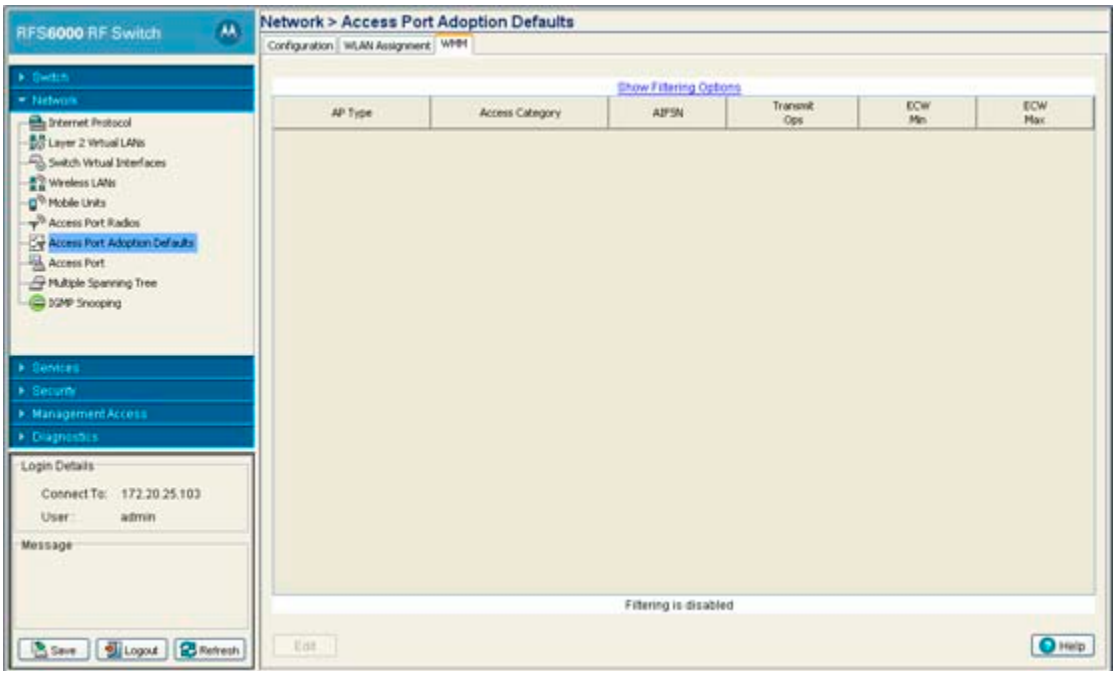
6. Click **Apply** to save the changes made within the screen.
7. Click **Revert** to cancel the changes made and revert back to the last saved configuration.

4.8.4 Configuring WMM

Use the **WMM** tab to review each radio type, as well as the Access Category that defines the data (Video, Voice, Best Effort and Background) the radio has been configured to process. Additionally, the WMM tab displays the transmit intervals defined for the target access category.

To view existing WMM Settings:

1. Select **Network Setup** > **Radio Adoption Defaults** from the main menu tree.
2. Click the **WMM** tab.



3. Refer to the WMM table for the following information:

AP Type	Displays whether the radio is an 802.11a radio or an 802.11bg radio. This value is read-only and cannot be modified.
Access Category	Displays the Access Category currently in use. There are four categories: Video, Voice, Best Effort and Background. Click the Edit button to change the current Access Category. Ensure the Access Category reflects the radios intended network traffic.
AIFSN	Displays the current *Arbitrary Inter-frame Space Number* (AIFSN). Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before trying to access the medium.
Transmit Ops	Displays the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set higher.

ECW Min	The ECW Min is combined with the ECW Max to define the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
ECW Max	The ECW Max is combined with the ECW Min to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.

4. To modify the properties of WMM Adoption Settings, select a radio and click the Edit button. For more information, see *Editing Access Port Adoption WMM Settings on page 4-139*.

4.8.4.1 Editing Access Port Adoption WMM Settings

Use the **Edit** screen to modify a WMM profile's properties (AIFSN, Transmit Ops, Cw Min and CW Max). Modifying these properties may be necessary as Access Categories are changed and transmit intervals need adjustment to compensate for larger data packets and contention windows.Use *Configuring WMM on page 4-110* to configure downstream traffic parameters. WLAN WMM configuration affects your upstream traffic parameters.

To edit the existing WMM settings:

1. Select **Network Setup** > **Radio Adoption Defaults** from the main menu tree.
2. Click the **WMM** tab.
3. Select a radio from the table and click the **Edit** button.

   The **AP Type** identifies whether the radio is an 802.11a radio or an 802.11 bg radio. This value is read-only and cannot be modified. There are four editable access categories: Video, Voice, Best Effort and Background.
4. Enter a number between 0 and 15 for the **AIFSN** value for the selected radio.

   The AIFSN value is the current *Arbitrary Inter-frame Space Number*. Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before trying to access the medium.
5. Enter a number between 0 and 65535 for the **Transmit Ops** value.

   The Transmit Ops value is the maximum duration a device can transmit after obtaining a transmit opportunity. For Higher-priority traffic categories, this value should be set higher.
6. Enter a value between 0 and 15 for the **Contention Window minimum** value.

   The CW Minimum is combined with the CW Maximum to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
7. Enter a value between 0 and 15 for the **Contention Window maximum** value.

   The CW Maximum is combined with the CW Minimum to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.9 Configuring Access Ports

Use the **Access Port** screen to view device hardware address and software version information for adopted and unadopted Access Ports. For more information, refer to the following Access Port configuration sections:

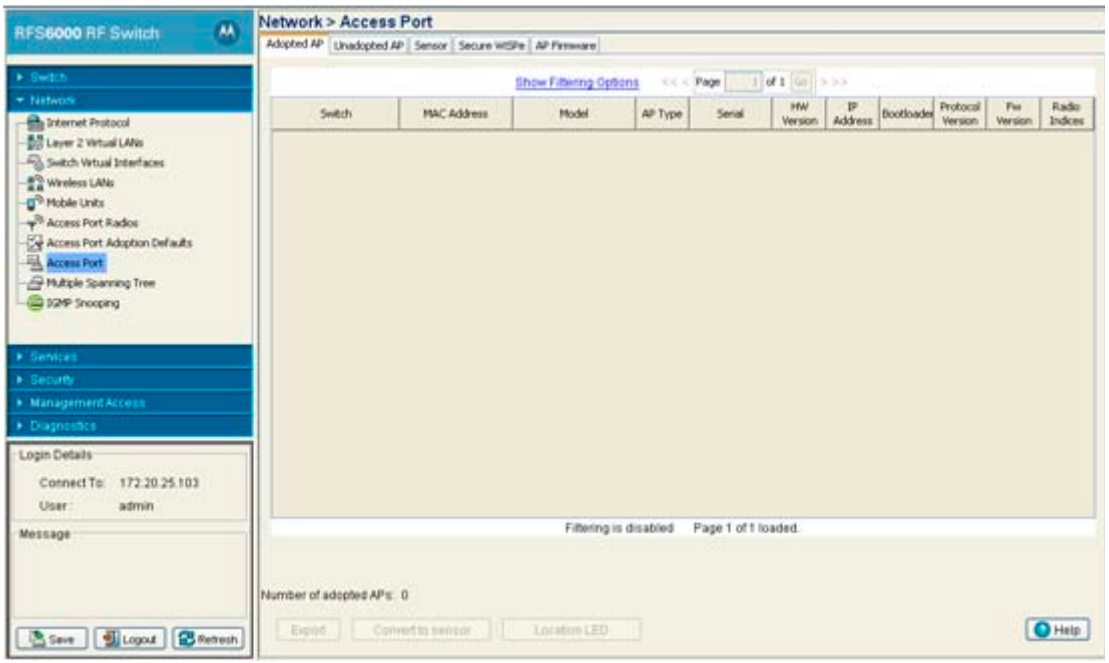
- *Viewing Adopted Access Ports*
- *Viewing Unadopted Access Ports*
- *Viewing Sensor Information*
- *Configuring Secure WiSPe*
- *Configuring Adaptive AP Firmware*

4.9.1 Viewing Adopted Access Ports

Use the **Adopted AP** tab for gathering device hardware address and software version information for the Access Port. Use this information to determine whether the Access Port's version supports the optimal feature set available for the network.

To view existing adopted Access Port information:

1. Select **Network** > **Access Port** from the main menu tree.
2. Click the **Adopted AP** tab.



3. Refer to the **Adopted AP** screen for the following information:

Switch	The **Switch** field displays the IP address of the cluster member associated with each AP. When clustering is enabled on the switch and Cluster GUI is enabled the **Switch** field will be available on the AP configuration screen. For information on configuring enabling Cluster GUI, see *Managing Clustering Using the Web UI*.
MAC Address	Displays the radio's first MAC address when it is adopted by the switch.

Model	Displays the model number of the Access Port.
AP Type	Displays the Access Port type.
Serial	Displays the serial number of the Access Port, and is used for switch management purposes. It is read-only and cannot be modified.
HW Version	Displays the hardware version of the Access Port. This information can be helpful when troubleshooting problems with the Access Port.
IP Address	Displays the IP address of the adopted Access Port.
Bootloader	Displays the software version the Access Port boots from. This information can be helpful when troubleshooting problems.
Protocol Version	Displays the version of the interface protocol between the Access Port and the switch. This information can be helpful when troubleshooting problems with the Access Port.
Fw Version	Displays the Access Port firmware version at run time. Use this information to assess whether the software requires an upgrade for better compatibility with the switch.
Radio Indices	Displays the indices of the radios belonging to the selected Access Port. These indices are equivalent to a numerical device recognition identifier (index) for the radio.
Number of Adopted APs	The Number of Adopted APs is the total number of Access Ports currently adopted by the switch.

4. When using clustering and the **Cluster GUI** feature is enabled, a pulldown menu will be availble to select which cluster members' APs are displayed. To view APs from all cluster members, select **All** from the pulldown menu. To view APs radios from a specific cluster member, select that member's IP address from the drop-down menu.
5. Click the **Export** button to export the contents of the table to a Comma Separated Values file (CSV).
6. Click the **Convert to Sensor** button to convert the selected adopted AP300 to a sensor that can be used with the *Wireless Intrusion Detection System* (WIDS) application.

NOTE: Both Access Ports and standalone Access Points can be converted to sensors. When converting an AP300 Access Port to a sensor both the 802.11a and 802.11bg radios are converted to sensors. When using a standalone Access Point, such as the AP5131, one radio can be converted into a sensor and the other radio can function as standard radio.

NOTE: When converting APs to sensors the default sensor configuration will be sent to each AP. If a static IP is configured in the default sensor configuration, all sensors will receive the same IP address and cause an IP address conflict. It is recommended not to set a static IP for the default sensor configuration and to update individual sensors if they require static IPs.

WIDS uses sensors to collect data transmitted by 802.11a and 802.11b/g compliant devices and sends the data to a centralized server for analysis and correlation. Sensors are passive devices that function primarily in listen-only mode. A single sensor can monitor multiple APs.

Once the sensor collects wireless LAN data, the centralized server analyzes the 802.11 frames and extracts meaningful data points to determine key attributes, such as:

- *Wireless device associations*

- *Use of encryption and authentication*
- *Vendor identification of all devices*
- *Total data transferred*

Preprocessing data centrally ensures a reduced reliance on network bandwidth to perform wireless network management.

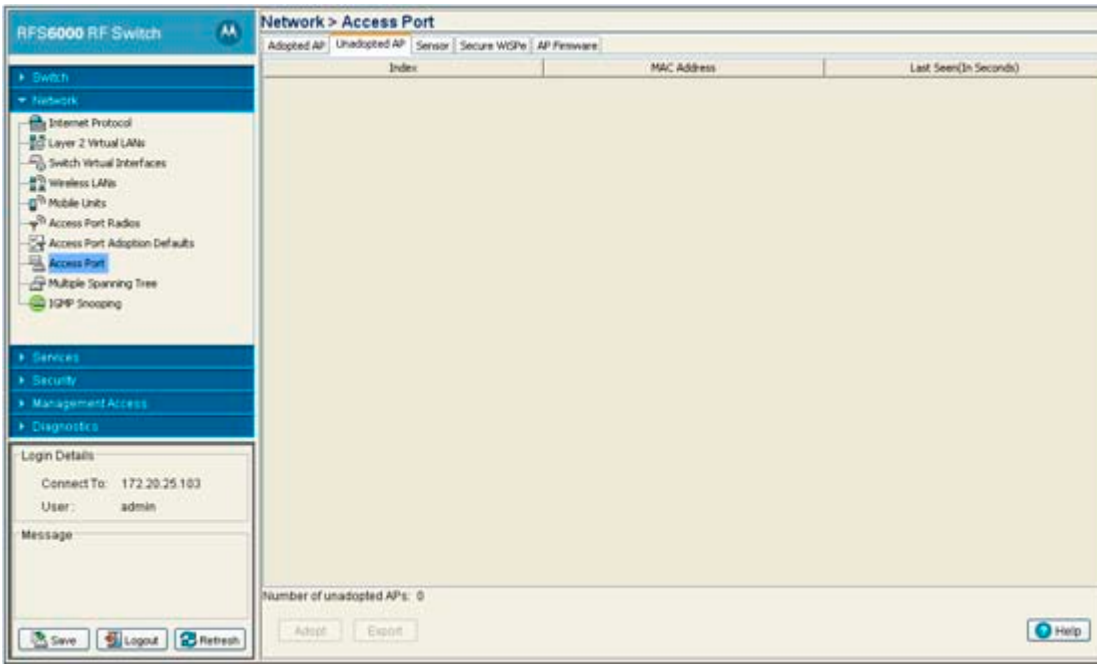
7. Click the **Location LED** button to flash the LEDs on the AP to assist in locating and identifying a selected AP within an installation.

4.9.2 Viewing Unadopted Access Ports

Use the **Unadopted AP** tab for gathering device hardware address and software version information for the Access Port.

To view existing Radio Configuration information:

1. Select **Network** > **Access Port** from the main menu tree.
2. Click the **Unadopted AP** tab.



The **Unadopted AP** tab displays the following information:

Index	Displays a numerical identifier used to associate a particular Access Port with a set of statistics and can help differentiate the Access Port from other Access Ports with similar attributes.
MAC Address	Displays the unique Hardware or *Media Access Control* (MAC) address for the Access Port. Access ports with dual radios will have a unique MAC address for each radio. The MAC address is hard coded at the factory and cannot be modified.

Last Seen (In Seconds)	Displays the time the Access Port was last seen (observed within the switch managed network). This value is expressed in seconds. Use this value to assess if the Access Port is no longer in communications with the switch.
Number of Unadopted APs	Displays the total number of Access Ports (at the bottom of the screen) that have been recognized, but not adopted by the switch.

3. Select an available index and click the **Adopt** button to display a screen wherein the properties of a new radio can be added for adoption to the switch. When displayed, the screen prompts for the MAC address and type of radio. Complete the fields and click the **OK** button to add the radio.
4. Click the **Export** button to export the contents of the table to a Comma Separated Values file (CSV).

CAUTION: An Access Port is required to have a DHCP provided IP address before attempting layer 3 adoption, otherwise it will not work. Additionally, the Access Port must be able to find the IP addresses of the switches on the network. To locate switch IP addresses on the network:

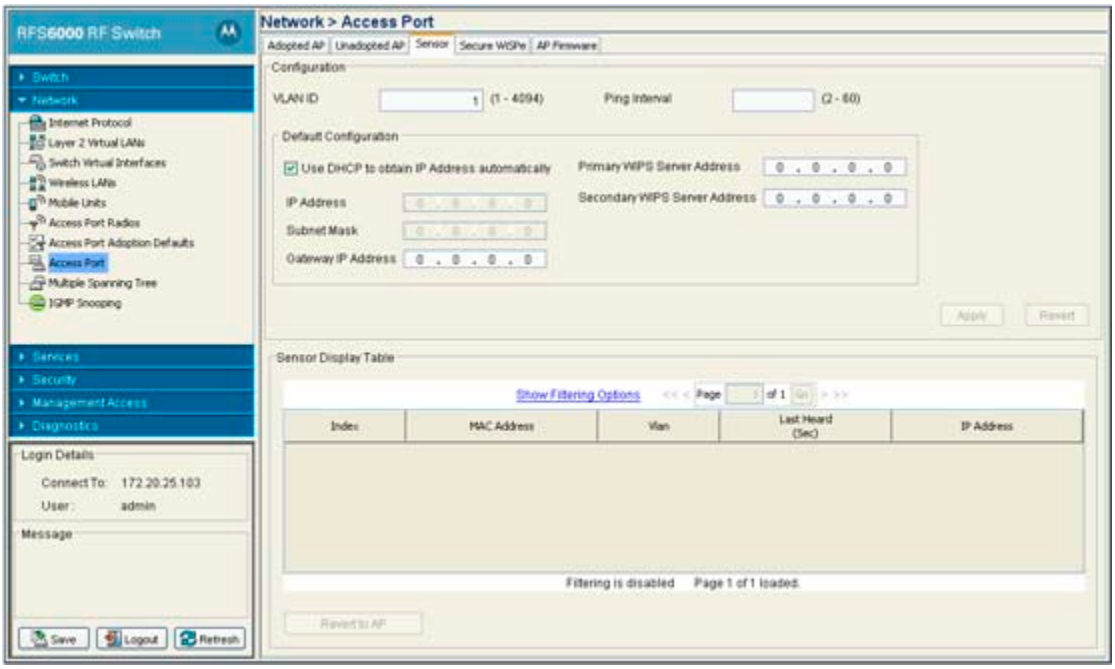
- Configure DHCP option 189 to specify each switch IP address.
- Configure a DNS Server to resolve an existing name into the IP of the switch. The Access Port has to get DNS server information as part of its DHCP information. The default DNS name requested by an AP300 is “Symbol-CAPWAP-Address”. However, since the default name is configurable, it can be set as a factory default to whatever value is needed.

4.9.3 Viewing Sensor Information

Use the **Sensor** tab to view information on AP300s configured as sensors and if needed revert them to Access Ports.

To view existing Sensor information:

1. Select **Network** > **Access Port** from the main menu tree.
2. Click the **Sensor** tab.



3. Refer to the **Configuration** field to define the following information:

VLAN ID	Enter a global default VLAN ID for all radios configured as sensors.
Ping Interval	Define the ping interval (in seconds) the switch uses to contact the radios defined as sensors.
Use DHCP to obtain IP address automatically	Select this option to allow the switch's DHCP managed services to assign an IP address to a WIPS sensor.
Subnet Mask	Assign a subnet mask to the WIPS Server.
Gateway IP Address	Assign a gateway address to the WIPS Server.
Primary WIPS Server Address	Define the first choice IP address where the switch managed network will attempt to obtain rogue device information from a WIPS Server.
Secondary WIPS Server Address	Define an alternate (second choice) IP address where the switch managed network will attempt to obtain rogue device information from a WIPS Server.

4. Specify the global default **VLAN ID** for all sensors and click the **Apply** button.

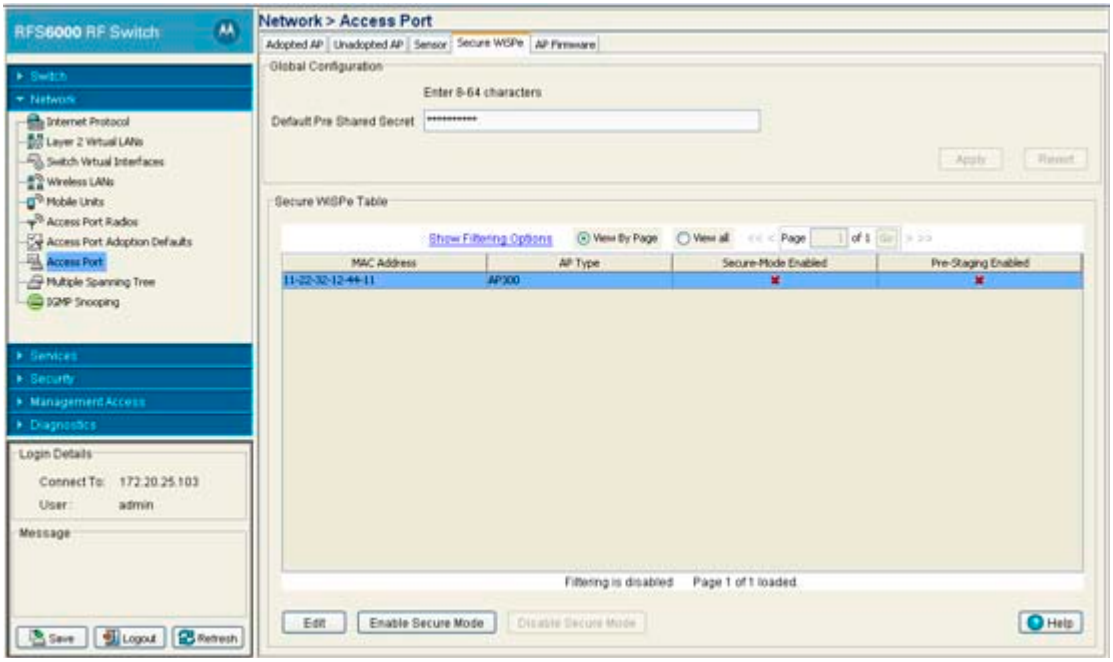
   The **Sensor Display Table** displays the following information:

Index	Displays the numeric value assigned to each sensor AP.
MAC Address	Displays the Media Access Control (MAC) address for each sensor AP.
VLAN	Displays the VLAN that each sensor AP is associated with.
Last Heard (sec)	Displays the number of seconds since the switch last received packets from each sensor AP.
IP Address	Displays the current IP address for each sensor AP.
Revert to AP	Select a sensor AP from the table and click the Revert to AP button to return to convert the AP back to a standard Access Port.

4.9.4 Configuring Secure WiSPe

To configure Secure WiSPe:

1. Select **Network** > **Access Port** from the main menu tree.
2. Click the **Secure WiSPe** tab.



3. Enter a **Default Pre-Shared Secret** used for Secure WiSPe authentication. The shared secret must be between 8 and 64 characters.
4. The **Secure WiSPe Table** displays the following information on each configured AP:

MAC Address	Displays the MAC Addresses for each of the Access Ports.
AP Type	The AP Type displays the Access Port model (AP100, AP300, AP-5131 or AP-7131).
Secure Mode Enabled	Indicates if Secure Mode is enabled for each of the listed Access Ports. A green checkmark indicates Secure Mode is enabled and a red X indicates that Secure Mode is disabled.
Pre-Staging Enabled	Indicates if Pre-Staging Mode is enabled for each of the listed Access Ports. A green checkmark indicates Pre-Staging is enabled and a red X indicates that Pre-Staging is disabled.

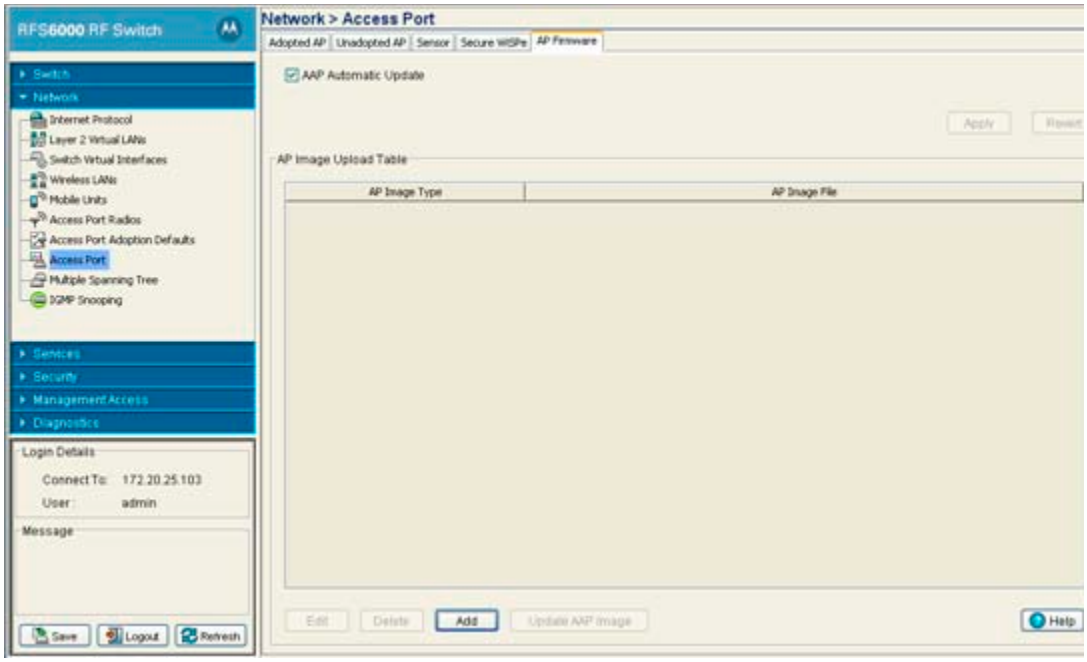
5. To edit the Secure WiSPe settings for an AP, select an AP from the **Secure WiSPe Table** and click the **Edit** button.
6. To enable Secure Mode click the **Enable Secure Mode** button to enable secure-mode to a set of APs. The AP's MAC Address and mode will be saved in the running configuration. If secure-mode is set to enable, it means that WISP-e transactions for this AP will be secured.
7. To disable Secure Mode click the **Disable Secure Mode** button to disable secure-mode to a set of APs. The AP's MAC Address and mode will be saved in the running configuration. If secure-mode is set to disable, it means that WISP-e transactions for this AP will not be secured.
8. When using clustering and the **Cluster GUI** feature is enabled, a drop-down menu is available to select which cluster members' APs are displayed. To view APs from all cluster members, select **All** from the drop-down menu. To view APs radios from a specific cluster member, select that member's IP address from the drop-down menu.

4.9.5 Configuring Adaptive AP Firmware

Refer to the **AP Firmware** tab to view the Access Port and Adaptive AP firmware image associated with each adopted Access Port or Adaptive AP. The screen allows you to update the firmware image for Adaptive APs that associate with the switch.

To view AP firmware information:

1. Select **Network** > **Access Port** from the main menu tree.
2. Click the **AP Firmware** tab.



1. Enable or disable Adaptive AP Automatic Update (AAP Automatic Update).

AAP Automatic Update	Check this box to enable automatic updates of Access Port or Adaptive AP firmware when an Access Port or Adaptive AP associates with the switch. The AP image file used for automatic update are specified in the **AP Image Upload Table** below.

2. View the firmware information displayed per Adaptive AP type with the following data:

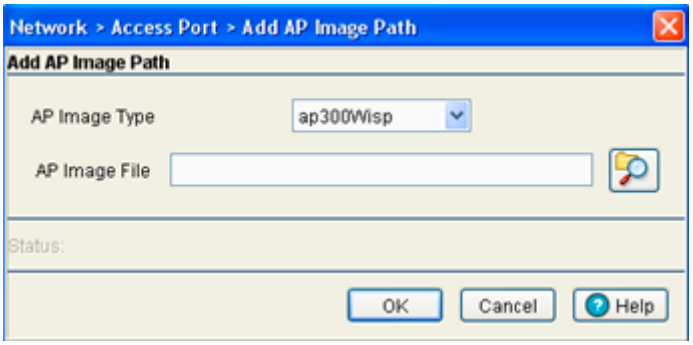
AP Image Type	The AP image type is the model of Access Port or Adaptive AP which the firmware is used with. Available image types are: • *ap300Wisp* • *ap300Wispe* • *ap300IpsSensor* • *ap100* • *ap4131* • *ap4131Revert* • *ap5131* • *ap5181* • *ap7131* • *ap7181*
AP Image File	Displays the filename of the image file associated with the **AP Image Type**.

3. To add a new AP firmware image, click the **Add** button. For information on adding a new AP firmware refer to *Adding a New AP Firmware Image on page 4-147*.
4. To edit the details of an AP firmware image, highlight an AP image type and click the **Edit** button. For information on adding a new AP firmware refer to *Editing an Existing AP Firmware Image on page 4-148*.
5. To delete an existing AP firmware image, highlight an AP image type and click the **Delete** button.

4.9.5.1 Adding a New AP Firmware Image

To add AP Firmware Image settings:

1. Select **Network Setup** > **Access Port** from the main menu tree.
2. Click the **AP Firmware** tab.
3. Click the **Add** button to display a screen to configure the **AP Image Type** and **AP Image File**.



4. Specify the **AP Image Type**.
5. Specify the **AP Image File**. You can browse the switch file systems using the browser icon. AP images must be on the flash, system, nvram or usb file systems in order for them to be selected.
6. Click the **OK** button to save the changes and return to the **AP Firmware** tab.

4.9.5.2 Editing an Existing AP Firmware Image

To modify the AP Firmware Image settings:

1. Select **Network Setup** > **Access Port** from the main menu tree.
2. Click the **AP Firmware** tab.
3. Select an **AP Image Type** from the **AP Image Upload** table.
4. Click the **Edit** button to display a screen to change the **AP Image Type** or **AP Image File**.
5. Modify the **AP Image Type** as necessary.
6. Modify the **AP Image File** as necessary. You can browse the switch file systems using the browser icon. AP images must be on the flash, system, nvram or usb file systems in order for them to be selected.
7. Click the **OK** button to save the changes and return to the **AP Firmware** tab.

4.10 Multiple Spanning Tree

Multiple Spanning Tree Protocol (MSTP) provides a VLAN-aware protocol and algorithm to create and maintain a loop-free network. It allows the configuration of multiple spanning tree instances. This ensures a loop-free topology for 1 or more VLANs. It allows the network administrator to provide a different path for each group of VLANs to better utilize redundancy.

MSTP allows rapid convergence similar to *Rapid Spanning Tree Protocol* (RSTP). RSPT is an independent protocol and MSTP does not use RSTP. Since MSTP allows VLANs to be grouped in an instance, each instance can have its own spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding links for data traffic, load balancing and therefore, reduces the number of spanning-tree instances required to support a large number of VLANs.

Using MSTP, the network can be divided into regions. All switches within a region use the same VLAN to instance mapping. The entire network runs a spanning tree instance called the *Common Spanning Tree* instance (CST) that interconnects regions as well as legacy (STP and RSTP) bridges. The regions run on a local instance for each configured MSTP instance.

The network-wide spanning tree for instance 0 is known as the *Common Spanning Tree* (CST). A spanning tree for any other instance, which is local to a region, is known as an *Internal Spanning Tree* (IST). The *Common and Internal Spanning Tree* (CIST) (which consists of the CST as well as all ISTs across regions) interconnects all bridges in the network.

The following definitions describe the STP instances that define an MSTP configuration:

- *Common Spanning Tree (CST)* – MSTP runs a single spanning tree instance (called the *Common Spanning Tree*) that interconnects all the bridges in a network. This instance treats each region as a single bridge. In all other ways, it operates exactly like *Rapid Spanning Tree* (RSTP).
- *Common and Internal Spanning Trees (CIST)* – CIST contains all of the ISTs and bridges not formally configured into a region. This instance interoperates with bridges running legacy STP and RSTP implementations.
- *Multiple Spanning Tree Instance (MSTI)* – The MSTI is identified by an *MSTP identifier* (MSTPid) value from 1 to 15. This defines an individual instance of a spanning tree. One or more VLANs can be assigned to an MSTI. A VLAN cannot be assigned to multiple MSTIs. The multiple spanning tree instance 0 is always present. VLANs not explicitly assigned to an instance are assigned to instance 0.
- *MSTP Region* – These are clusters of bridges that run multiple instances of the MSTP protocol. Multiple bridges detect they are in the same region by exchanging their configuration digest (which is dependent

on the VLAN to instance mapping), region name and revision-level. If you need to have two bridges in the same region, the two bridges must have identical VLAN to instance mappings, region names and revision-levels.

To configure the switch for MSTP support, configure the region name and the revision on each switch being configured. This region name is unique to each region. Then create one or more instances and assign IDs. VLANs are then assigned to instances. These instances must be configured on switches that interoperate with the same VLAN assignments. Port cost, priority and global parameters can then be configured for individual ports and instances.

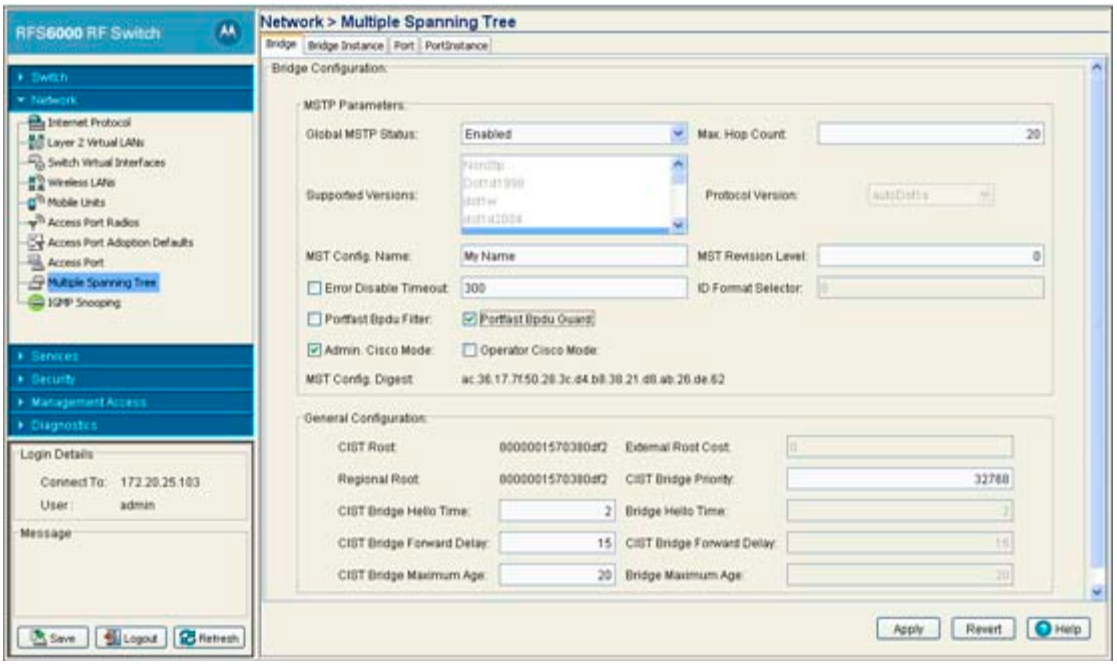
The Multiple Spanning Tree option contains separate tabs for the following activities:

- *Configuring a Bridge*
- *Viewing and Configuring Bridge Instance Details*
- *Configuring a Port*
- *Viewing and Configuring Port Instance Details*

4.10.1 Configuring a Bridge

Use the **Bridge** tab to configure the Bridge. This window displays bridge configuration details for the switch

To configure the MSTP bridge:



To configure the MSTP bridge:

1. Select **Network** > **Multiple Spanning Tree** from the main menu tree.
2. Select the **Bridge** tab (should be the displayed tab by default).
3. Refer to the MSTP Parameter field to view or set the following:

Global MSTP Status Use the drop-down menu to define MSTP status. The default is Enabled.

Max Hop Count	Displays the maximum allowed hops for a BPDU (*Bridge Protocol Data Unit)* in an MSTP region. This value is used by all the MSTP instances.
Supported Versions	Displays the different versions of STP supported.
Protocol Version	Displays the current protocol version in use. Available MSTP protocol versions are: • *forceNonStp* • *forceLegacyDot1d* • *forceDot1w* • *autoDot1s* • *unknown*
MST Config. Name	Enter a name for the MST region. This is used when configuring multiple regions within the network. Each switch running MSTP is configured with a unique MST region name. This helps when keeping track of MSTP configuration changes. Increment this number with each configuration change. The revision-level specifies the revision-level of the current configuration.
MST Revision Level	Assign a MST revision level number to the MSTP region to which the device belongs. Each switch running is configured with a unique MSTP name and revision number. This helps when keeping track of MSTP configuration changes. Increment this number with each configuration change. The revision level specifies the revision level of the current configuration.
Error Disable Timeout	Select this option to enable an error disable-timeout facility. The error disable-timeout is used to set a timeout value for ports disabled resulting from a BPDU guard. The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port.
ID Format Selector	Displays the ID format currently in use.
Portfast Bdpu Filter	Select this checkbox to enable BPDU filter for all portfast enabled ports.The Spanning Tree Protocol sends BPDUs from all the ports. Enabling the BPDU filter feature ensures PortFast enabled ports do not transmit or receive any BPDUs.
PortFast Bdpu Guard	Select this checkbox to enable BPDU guard for all portfast enabled ports. When the BPDU Guard feature is set for bridge, all portfast-enabled ports of the bridge that have BPDU set to default shutdown the port on receiving a BPDU. Hence no BPDUs are processed.
Admin Cisco Mode	Select this checkbox to enable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP.
Operator Cisco Mode	Displays whether Cisco's version of MSTP is running. This is not a configurable parameter.
MST Config Digest	Displays the Configuration Digest derived from the MSTP Configuration table.

4. Refer to the **General Configuration** field for the following

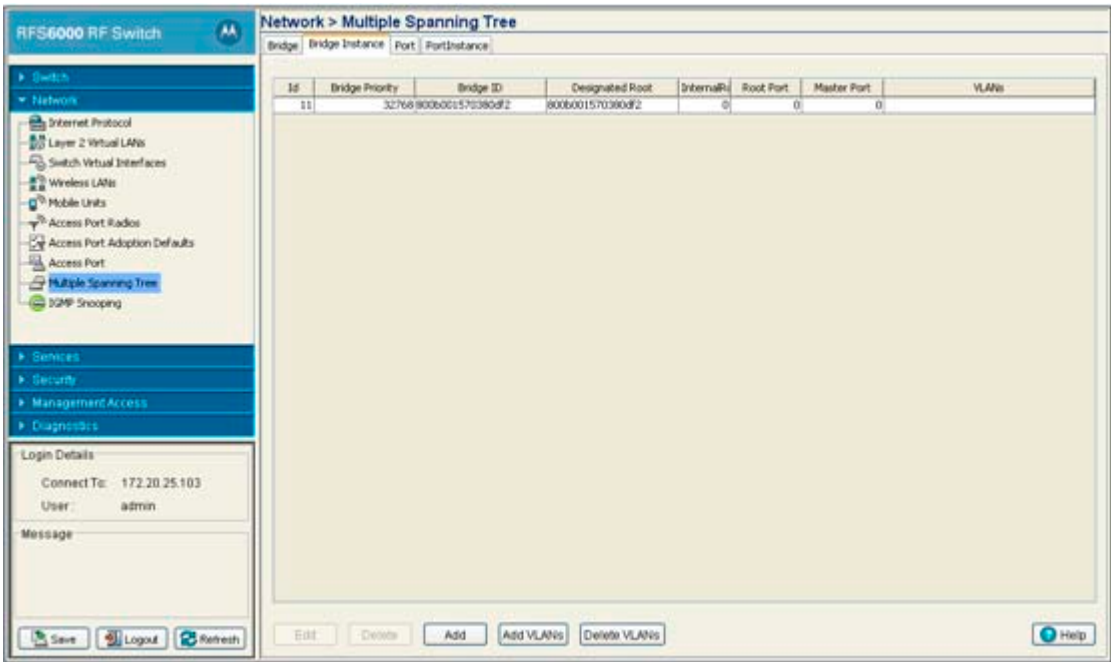
CIST Root	This displays the CIST (Common and Internal Spanning Tree) root bridge's bridge identifier. The bridge identifier consists of a priority value followed by the MAC address.The lower the path cost, the greater the likelihood of the bridge becoming the root.
External Root Cost	Displays the root cost of the CIST root.
Regional Root	This displays the regional roots MAC address.

CIST Bridge Priority	Set the bridge priority for the common instance. The value entered, determines the likelihood this bridge is selected as the root. The lower the priority the greater the likelihood of the bridge becoming a root.
CIST Bridge HelloTime	Set the CIST Hello Time (in seconds). After the defined interval all bridges in a bridged LAN exchange BPDUs. The hello time is the time interval (in seconds) the device waits between BPDU transmissions. A very low value leads to excessive traffic on the network, whereas a higher value delays the detection of a topology change. This value is used by all instances.
Bridge Hello Time	Displays the configured Hello Time. If this is the root bridge, the value is equal to the configured Hello Time.
CIST Bridge Forward Delay	Enter the CIST bridge forward delay value received from the root bridge. If this is the root bridge, the value will be equal to the Configured Forward Delay. The forward delay value is the maximum time (in seconds) the root device waits before changing states (from a listening state to a learning state to a forwarding state). This delay is required, as every device must receive information about topology changes before forwarding frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops may result.
CIST Bridge Forward Delay	Displays the configured forward delay period.
CIST Bridge Maximum Age	Enter the CIST bridge maximum age received from the root bridge. The max-age is the maximum time (in seconds) for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The max-age should be greater than twice the value of hello time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so a frame generated by root can be propagated to the leaf nodes without exceeding the maxage.
Bridge Maximum Age	Displays the BPDU maximum age value. If this is the root bridge, the value will be equal to the Configured Max Age.

4.10.2 Viewing and Configuring Bridge Instance Details

The Bride Instance tab displays the number of MSTP instance created and VLANS associated with it. To view and configure the MSTP bridge instance:

1. Select **Network** > **Multiple Spanning Tree** from the main menu tree.
2. Select the **Bridge Instance** tab.



The Bridge Instance tab displays the following:

ID	Displays the ID of the MSTP instance.
Bridge Priority	Displays the bridge priority for the associated instance. The Bridge Priority is assigned to an individual bridge based on whether it is selected as the root bridge. The lower the priority, the greater likelihood the bridge becoming the root for this instance.
Bridge ID	Bridge ID Displays the bridge id of the bridge for this instance.
Designated Root	Displays the ID of the root bridge that sent the BPDU received on this port.
Internal Root Cost	Displays the configured path cost on a link connected to this port within the internal MSTP region.
Root Port	Root Port Displays the Port ID of the root port for this instance.
Master Port	Master Port Displays the Port ID of the master port, if any, for this instance.
VLANs	VLANs Displays the list of VLANs included in this MSTP instance.

3. Select an ID and click the **Delete** button to remove from the list.

4.10.2.1 Creating a Bridge Instance

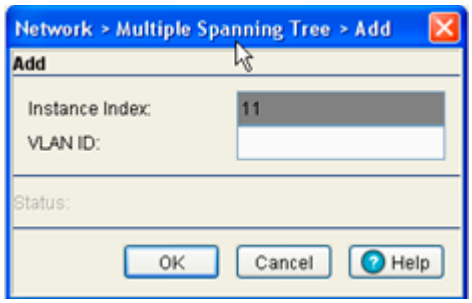
To create a VLAN instance and associate it with a bridge as a numerical identifier:

1. Select **Network** > **Multiple Spanning Tree** from the main menu tree.
2. Select the **Bridge Instance** tab.
3. Click the **Add** button.

4. Enter a value between 1 and 15 as the Instance ID.
5. Click **OK** to save and commit the changes.
6. The Bridge Instance tab with now display the new instance ID.
7. Click **Cancel** to disregard the new Bridge Instance ID.

4.10.2.2 Associating VLANs to a Bridge Instance

1. Select **Network** > **Multiple Spanning Tree** from the main menu tree.
2. Select the **Bridge Instance** tab.
3. Select an ID from the table within the Bridge Instance tab and click on the **Add VLAN**s button.



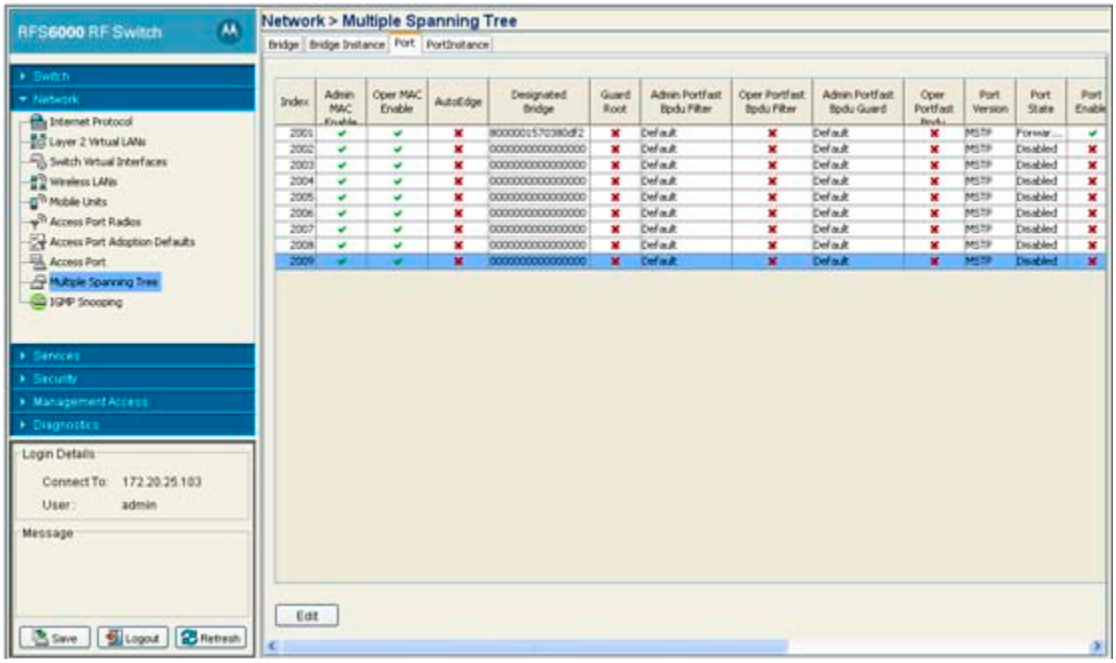
4. Enter a VLAN ID between 1 to 4094 in the VLAN ID field. This VLAN ID is associated with the Instance index. You can add multiple VLANs to an instance.
5. Click **OK** to save and commit the new configuration.
6. Click **Cancel** to disregard the changes.

4.10.3 Configuring a Port

Use the **Port** tab to view and configure MSTP port parameters, including enabling/disabling the spanning tree algorithm on one or more ports (displaying the designated bridge and port/root information).

To view and configure MSTP port details:

1. Select **Network** > **Multiple Spanning Tree** from the main menu tree.
2. Select the **Port** tab.



The **Port** tab displays the following information (ensure you scroll to the right to view the numerous port variables described):

Index	Displays the port index.
Admin MAC Enable	Displays the status of the Admin MAC. Change the status using the **Edit** button. A green check mark indicates the Admin MAC Enable status is active/enabled.
Oper MAC Enable	This field displays the status of the Oper MAC Enable. You can change the status using the **Edit** button. A green check mark indicates the Oper MAC Enable status is active/enabled.
AutoEdge	AutoEdge Displays whether the port can automatically detect whether it is an edge port edge port.
Designated Bridge	Displays the ID of the bridge sent the best BPDU received on this port.
Guard Root	Displays whether the listed port index enforces root bridge placement. The guard root 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.
AdminPort PortFast BPDU Filter	Displays the portfast BPDU filter for the admin port. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter ensures PortFastenabled admin ports do not transmit or receive BPDUs.
OperPort PortFast Bpdu Filter	Displays a portfast BPDU filter for the oper port. Enabling the BPDU Filter feature ensures PortFastenabled oper ports do not transmit or receive BPDUs.

AdminPort PortFast Bpdu Guard
Displays the whether BPDU Guard is currently enabled for this port.
When set for a bridge, all portfast-enabled ports having the bpdu-guard set to default shut down the port on receiving the BPDU. When this occurs, the BPDU is not processed.

OperPort PortFast Bpdu Guard
Displays the whether BPDU Guard is currently enabled for this port.
When the OperPort PortFast BPDU Guard feature is set for a bridge, all portfast-enabled ports that have the bpdu-guard set to default shut down the port on receiving a BPDU. When this occurs, the BPDU is not processed.

Port Version
Displays the port version associated with this instance. It can be either of the following:

- *STP*
- *RSTP*
- *MSTP*

Port State
Port State Displays the MSTP state for this port. A port must be enabled to be able to forward.

Port Enable
Displays the enable/disable MSTP designation of each port. A green check mark indicates the Oper MAC Enable status is active/enabled.

Port Path Cost
Port Path Cost Displays the path cost for the specified port index. The default path cost depends on the speed of the interface.

Speed	**Default path cost**
<=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*

Port Designated Cost
Displays the port cost for each port on the switch. The cost helps determine the role of the port 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.

Designated Port
Defines the port connection used to send and receive packets. By having only one designated port per segment, all looping issues should be resolved. Once the designated port has been selected, any other ports that connect to that segment become non-designated ports and block traffic from taking the defined path.

Forward Transitions
Forward Transitions Displays the number of MSTP state transitions to the forwarding state that have occurred on this port.

Protocol Migration
The switch can interoperate with legacy 802.1d bridges running STP / RSTP. If the port receives a legacy
802.1D configuration BPDU, it only sends 802.1D BPDUs over its port from that point on. Enable this option to restart detection of whether the port is connected to an MSTP capable bridge or a legacy 802.1 bridge.

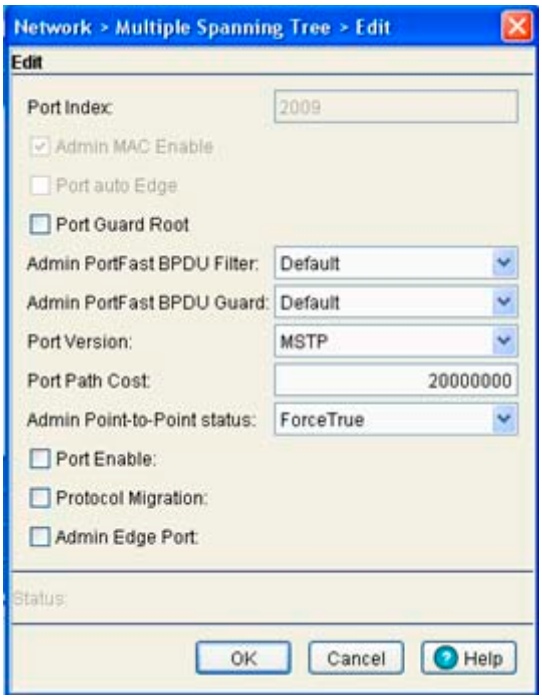
Admin Edge Port	A green checkmark defines the listed index enabled as an Admin Edge Port, and a red "X" defines the listed index as not being an Admin Edge Port. Enable it only on ports that connect to a single location.
Oper Edge Port	Oper Edge Port Displays whether the port is currently an edge port.
Admin Point-to-Point	Displays the point-to-point status as ForceTrue or ForceFalse. ForceTrue indicates this port should be treated as connected to a point-to-point link. ForceFalse indicates this port should be treated as having a shared connection.
Oper Point-to-Point	Displays whether the listed port index is configured to connect to another port through a point-to-point link. A green checkmark indicates the port as supporting point-to-point, and a red "X" indicates the port as having point-to-point disabled.

3. Select an Id and click the **Edit** button to revise the selected MSTP port configuration.

4.10.3.1 Editing a MSTP Port Configuration

To edit and reconfigure MSTP Port parameters.

1. Select a row from the port table and click the **Edit** button.



The following MSTP Port parameters can be reconfigured.

Port Index	Displays the read-only Port Index.
Admin MAC Enable	Displays the status of the Admin MAC Enable. A green check mark indicates the status as enabled.
Port auto Edge	Select the checkbox to use the port as an edge port.

Port Guard Root	Port Guard Root Select this checkbox to enable guard root for this 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.
PortFast BPDU Filter	Enable this option to change the status of the *Port Fast BPDU Filter*.
Port FastBPDU Guard	Enable this option to change the status of the *Port Fast BPDU Guard*.
Port Version	Select a value to reconfigure the port version.
Port Path Cost	Port Path Cost Displays the path cost for the specified port index. The default path cost depends on the speed of the interface.

Speed	**Default path cost**
<=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*

Admin Point-to-Point status	Define the point-to-point status as ForceTrue or ForceFalse. ForceTrue indicates this port should be treated as connected to a point-to-point link. ForceFalse indicates 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 switch or workstation is a point-to-point link.
Port Enable	Select this checkbox to use this port for the forwarding of packets on the switch.
Port Migration	The switch can interoperate with legacy 802.1d bridges running STP / RSTP. If the port receives a legacy 802.1D configuration BPDU, it only sends 802.1D BPDUs over its port from that point on. Enable this option to restart detection of whether the port is connected to an MSTP capable bridge or a legacy 802.1 bridge.
Admin Edge Port	Select the checkbox to define this port as an admin edge port.

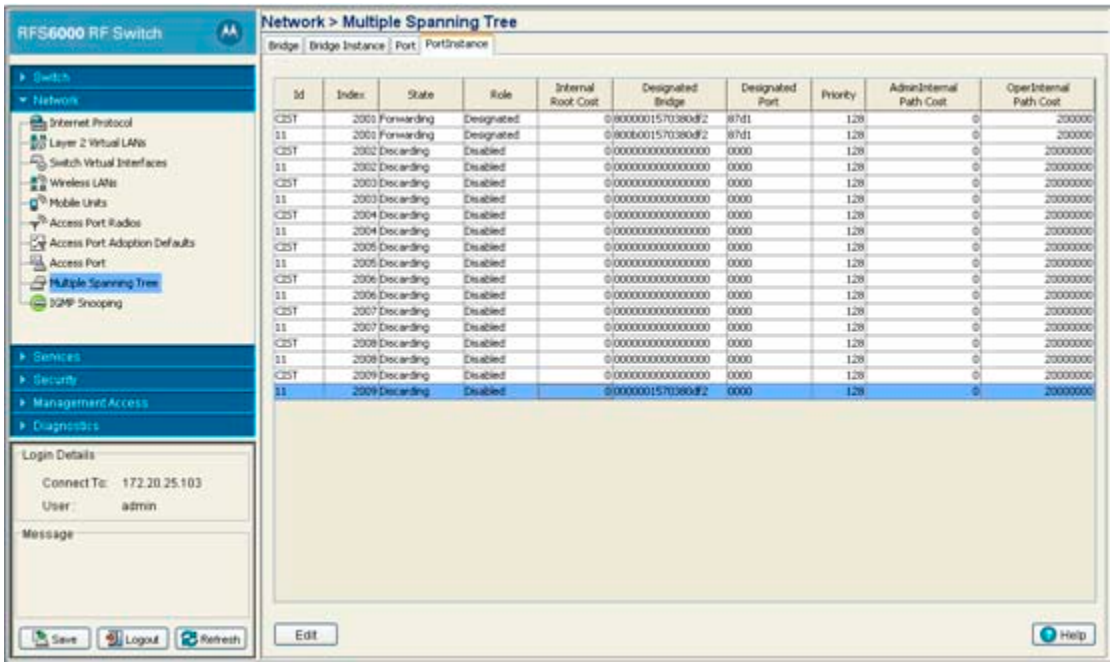
2. Click on **OK** button to save and commit the new configuration.
3. Click **Cancel** to disregard the changes and revert back to the previous configuration.

4.10.4 Viewing and Configuring Port Instance Details

Use the **Port Instance** tab to view and configure MST parameters per port per instance, including Port Priority and Admin Internal Path Cost.

To view and configure the MSTP bridge instance:

1. Select **Network** > **Multiple Spanning Tree** from the main menu tree.
2. Select the **PortInstance** tab.



The Port Instance table displays the following:

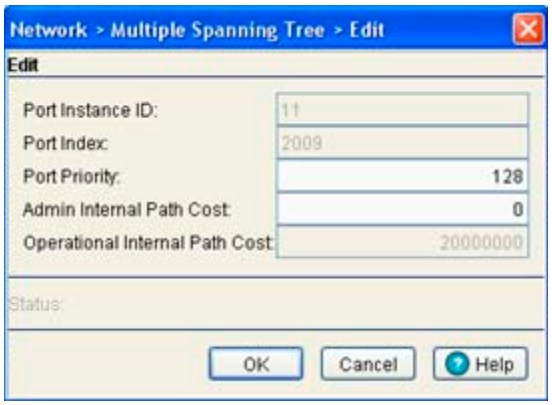
ID	Displays the instance ID.
Index	Displays the port index.
State	Displays the MSTP state for the port for that instance.
Role	Displays the MSTP state of the port.
Internal Root Cost	Displays the Internal Root Cost of a path associated with an interface. The lower the path cost, the greater likelihood of the interface becoming the root.
Designated Bridge	Displays the ID of the bridge that sent the best BPDU.
Designated Port	Designated Port Displays the ID of the port that is the designated port for that instance.
Priority	Displays the port priority set for that port and instance.
AdminInternal Path Cost	Displays the configured Admin Internal Path Cost of a port. A value of 0 indicates that the user has not configured a path cost.
OperInternal Path Cost	Displays the Operational Path Cost of a port. This displays the default cost if AdminInternal Path Cost is 0.

3. If necessary, select a CIST Index from the table and click on **Edit** button to change the port priority and internal path cost value. For additional information, see *Editing a Port Instance Configuration on page 4-159*.

4.10.4.1 Editing a Port Instance Configuration

To edit and reconfigure Port Instance parameters.

1. Select a row from the port table and click the **Edit** button.



Most of the MSTP Port Instance parameters can be reconfigured, as indicated below.

Port Instance ID	Read only indicator of the instance ID used as a basis for other modifications.
Port Index	Read only indicator of the port index used as a basis for other modifications.
Port Priority	If necessary, change the port priority value for the bridge. The lower the priority, a greater likelihood of the port becoming a designated port.
Admin Internal Path Cost	Displays the configured Admin Internal Path Cost of a port. A value of 0 indicates that the user has not configured a path cost.
Operational Internal Path Cost	Displays the Operational Path Cost of a port. This displays the default cost if AdminInternal Path Cost is 0.

4.11 Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) is used by both IP hosts and multicast routers. IP hosts use IGMP to report their multicast group memberships to any immediate-neighboring multicast router. Routers use the query message on its interface to solicit multicast group membership information from clients.

IGMP snooping is the process of listening to IGMP traffic. IGMP snooping allows the switch to listen in on an IGMP conversation between hosts and routers by processing layer 3 packets IGMP packets sent in a multicast network.

The goal of IGMP is to learn multicast router ports and snoop IGMP join requests/reports to build a portal list to forward multicast packet to interested hosts only on that Portal, thus optimizing the flooding of multicast packets.

IGMP snooping allows the switch to manage multicast traffic based on groups of IGMP hosts on a per-portal basis. IGMP snooping keeps track of hosts interested in a multicast group and on the portal it is associated and forwards multicast packets to portal on which the host is connected.

In the case of IP multicast traffic, an IGMP supported switch provides the benefit of conserving bandwidth on those network segments where no node has expressed interest in receiving packets addressed to the group address. This is in contrast to normal switch behavior, where multicast traffic is typically forwarded on all interfaces.

IGMP basically operates as follows:

- One router periodically broadcasts IGMP query messages onto a link
- Hosts respond to the query messages by sending IGMP report messages indicating their group memberships
- All routers receive the report messages and note the memberships of hosts on the link
- If a router doesn't receive a report message for a particular group for a period of time, the router assumes there are no more members of the group on the link

The IGMP Snooping screen is partitioned into two tabs supporting the following activities:

- *IGMP Snooping Configuration*
- *IGMP Snoop Querier Configuration*

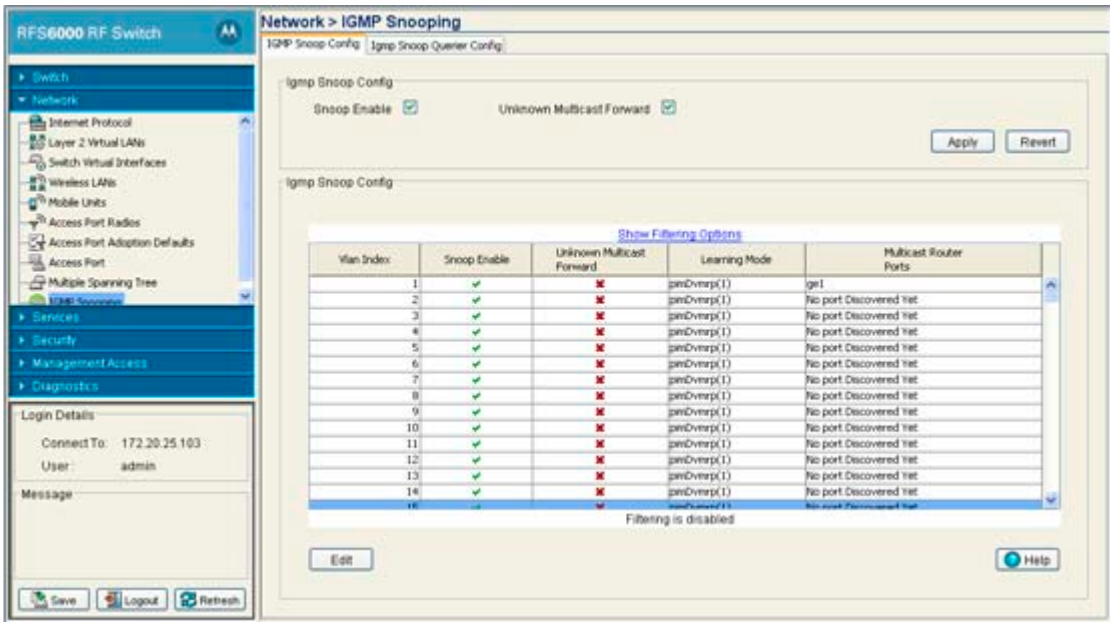
4.11.1 IGMP Snooping Configuration

To view and configure IGMP snooping:

1. Select **Network** > **IGMP Snooping** from the main menu tree.
2. Select the **IGMP Snoop Config** tab.
3. Optionally select the **Snoop Enable** option.

   When IGMP snooping is enabled, the switch analyses all the IGMP packets between hosts connected to the switch and multicast routers. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP leave, it removes the host's port from the table entry. When enabled, a green checkmark displays as opposed to a red “X” designating the snoop as disabled.
4. Optionally select the **Unknown Multicast Forward** option.

   This will allow the broadcast of multicast traffic to all the ports in a broadcast domain (LANs), regardless of whether the hosts were interested in that traffic or not.

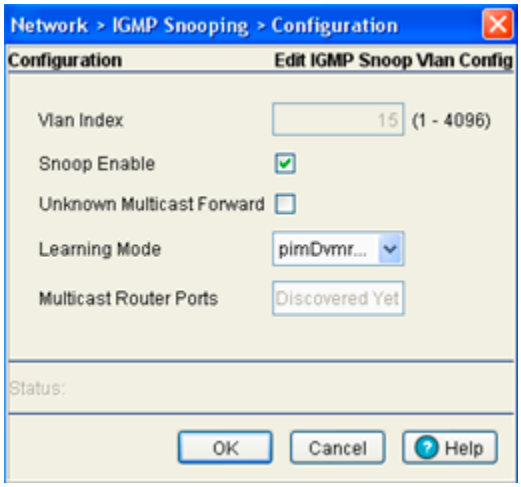


5. Select **Apply** to save the changes to the Snoop Enable and Unknown Multicast Forward options.

6. Review to the following to discern whether an existing snoop configuration requires revision.

Vlan Index	Lists the VLAN interfaces upon which snooping and unknown multicast forward is enabled or disabled
Snoop Enable	Displays whether IGMP snooping is enabled/disabled on the VLAN Index listed.
Unknown Multicast Forward	Displays whether unknown multicast traffic is enabled/disabled on the VLAN Index listed.
Learning Mode	Displays the learning mode the switch uses to listen to messages to detect router ports with IGMP snooping. Modes include: *pimDvmrp(1)* - Protocol Independent Multicast and Distance Vector *static* - Static entry
Mulitcast Router Ports	Displays the name of the multicast router port discovered as part of the snooping process. If no port has been detected, a *No port Discovered Yet* message displays.

7. Optionally, select a VLAN Index from amongst those listed, and select **Edit** to revise the Snoop Enable, Unknown Multicast Forward, Learning Mode and Multicast Router Ports.



8. Select **OK** to save the edits to the IGMP configuration. Selecting Cancel reverts the IGMP snooping configuration to its previous settings.

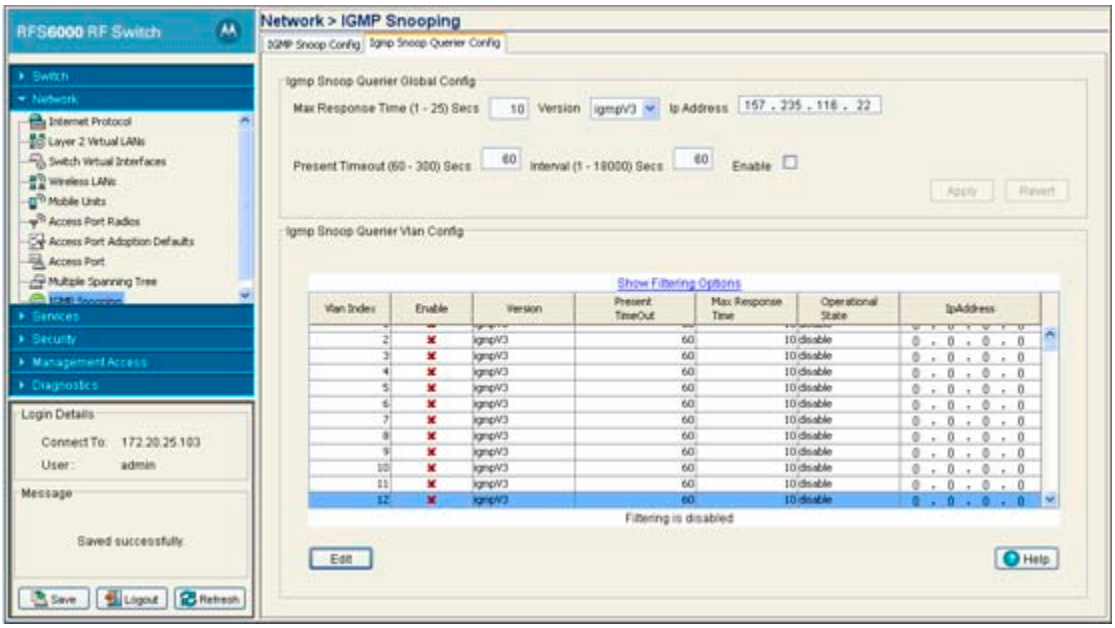
4.11.2 IGMP Snoop Querier Configuration

The IGMP snoop querier functionality is used in absence of a multicast router in networks where there is a multicast streaming server and multicast listener hosts, but no IGMP querier. For IGMP snooping to work, periodic IGMP general queries are required so multicast group memberships are refreshed by interested clients by replying to IGMP reports for the IGMP queries received. This feature can also be enabled under circumstances where the user wants to accommodate a query loss due to a multicast router being down or a query loss in the network. The present timeout is used to detect query loss and activate the switch querier. Switch topology changes are roaming clients. Joining or going away is handled by proxy querying (which is part of IGMP snoop functionality not the querier. On wired side, all multicast packets are flooded, so there is no need for a proxy query or detecting such changes.

NOTE: IGMP snooping does not detect link layer topology. The only thing it can detect is that a query loss has happened and activates the IGMP querier if enabled in the configuration.

To view and potentially modify an IGMP snooping querier configuration:

1. Select **Network** > **IGMP Snooping** from the main menu tree.
2. Select the **IGMP Snoop Querier Config** tab.

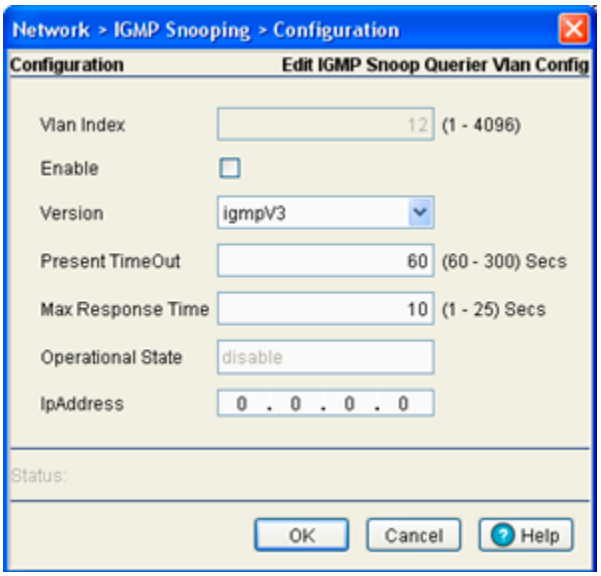


3. Refer to the **Igmp Snoop Querier Global Config** field and define the following values, once enabled these values display within the Igmp Snoop Querier Vlan Config field:

Max Response Time (1 - 25) Secs	Defines the maximum response time for the switch to receive a report. If the switch does not receive a report, it discards this port. If it receives a response from a wireless client it updates it's IGMP snoop table with the reported multicast group membership. In case of IGMP reports from wired ports, it simply forwards to multicast router ports, as IGMP snooping is conducted only for wireless clients and all wired ports are flooded for multicast packets.
Version	Define the igmpV1, igmpV2 or igmpV3 version from the drop-down menu.
Ip Address	Displays the configured querier IP address on the switch used while generating the general IGMP query.
Present Timeout (60 -300) Secs	The snooping switch does not rely on IGMP group leave announcements to determine when entries should be removed from the forwarding table. It implements a last membership query mechanism (such as the router-side functionality of the IGMP protocol as described in the IGMP and MLD specifications) on all its non-router ports. Define a timeout value as required between 60 - 300 seconds. Hosts that have silently opted out without sending a leave message are discarded if they do not respond with join/reports on the next query interval.

Interval (1 - 18000) Secs	Configures the interval for group specific IGMP queries sent by the switch. Valid range is 1 to 18000 seconds.
Enable	Select this option to enable the Apply/Revert buttons in order to save an updated configuration. Once a parameter has been enabled, the red "X" in the enabled column of the Igmp Snoop Querier Vlan Config table displays a green checkmark, designating the configuration as enabled.

4. Select **Apply** to save the changes to the Igmp Snoop Querier Global Config options.
5. Optionally, select a VLAN Index from amongst those listed, and select **Edit** to revise the following parameters:



Enable	Select the enable checkbox to use this IGMP snoop querier configuration with the VLAN listed. Once a parameter has been enabled, the red "X" in the enabled column of the Igmp Snoop Querier Vlan Config table displays a green checkmark, designating the configuration as enabled.
Version	Define the igmpV1, igmpV2 or igmpV3 version from the drop-down menu.
Present TimeOut	The snooping switch does not rely on IGMP group leave announcements to determine when entries should be removed from the forwarding table. It implements a last membership query mechanism (such as the router-side functionality of the IGMP protocol as described in the IGMP and MLD specifications) on all its non-router ports. Define a timeout value as required between 60 - 300 seconds. Hosts that have silently opted out without sending a leave message are discarded if they do not respond with join/reports on the next query interval.
Max Response Time	Defines the maximum response time for the switch to receive a report. If the switch does not receive a report, it discards this port. If it receives a response from a wireless client it updates it's IGMP snoop table with the reported multicast group membership. In case of IGMP reports from wired ports, it simply forwards to multicast router ports, as IGMP snooping is conducted only for wireless clients and all wired ports are flooded for multicast packets. Define a value between 1 - 25 seconds.

Operational State	Displays whether a particular configuration has been enabled/disabled. Once a parameter has been enabled, the red "X" in the enabled column of the Igmp Snoop Querier Vlan Config table displays a green checkmark, designating the configuration as enabled.
IpAddress	Displays the configured querier IP address on the switch used while generating the general IGMP query.

6. Select **OK** to save the edits to the configuration. Selecting **Cancel** reverts the configuration to its previous settings.

5

Switch Services

This chapter describes the Services main menu information available for the following switch configuration activities.:

- *Displaying the Services Interface*
- *DHCP Server Settings*
- *Configuring Secure NTP*
- *Configuring Switch Redundancy and Clustering*
- *Layer 3 Mobility*
- *Configuring Self Healing*
- *Configuring Switch Discovery*
- *Locationing*

5.1 Displaying the Services Interface

Refer to the **Services** main menu interface to review a summary describing the availability of several central features within the Services main menu item.

NOTE: When the switch's configuration is successfully updated (using the Web UI), the effected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the effected screen's Status field. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To display a **Services Summary:**

1. Select **Services** from the main menu tree.

2. Refer to the **Services Summary** field for the following information relating to configurable values within the Services main menu item.

DHCP Servers	Displays whether DHCP is enabled and the current configuration. For information on configuring DHCP Server support, see *DHCP Server Settings on page 5-3*.
NTP Time Management	Displays whether time management is currently enabled or disabled. *Network Time Protocol* (NTP) manages time and/or network clock synchronization within the switch managed network. NTP is a client/server implementation.
Redundancy Service	Displays whether Redundancy is currently enabled or disabled. One or more switches can be configured as members of a redundancy group to significantly reduce the chance of a disruption in service to WLANs and associated MUs in the event of failure of a switch or intermediate network failure. For more information, see *Configuring Switch Redundancy and Clustering on page 5-34*.

Layer 3 Mobility	Displays whether Layer 3 Mobility is currently enabled or disabled. Layer 3 mobility is a mechanism which enables a MU to maintain the same Layer 3 address while roaming throughout a multi-VLAN network. This enables the transparent routing of IP datagrams to MUs during their movement, so data sessions can be initiated while they roam (in for voice applications in particular). Layer 3 mobility enables TCP/UDP sessions to be maintained in spite of roaming among different IP subnets. For more information on configuring Layer 3 Mobility, see *Layer 3 Mobility on page 5-48*.
GRE Tunnels	Displays the number of GRE tunnels currently in service on the switch managed network.
Self Healing	Displays whether Self Healing is currently enabled. Self healing enables radios to take action when one or more radios fail. To enable the feature, the user must specify radio neighbors that would self heal if a neighbor goes down. The neighbor radios do not have to be of the same type. An 11bg radio can be the neighbor of a 11a radio and either of them can self heal when one fails. For information on configuring self healing, see *Configuring Self Healing on page 5-53*.

5.2 DHCP Server Settings

The DHCP Server Settings section contains the following activities:

- *Configuring the Switch DHCP Server*
- *Viewing the Attributes of Existing Host Pools*
- *Configuring Excluded IP Address Information*
- *Configuring the DHCP Server Relay*
- *Viewing DDNS Bindings*
- *Viewing DHCP Bindings*
- *Reviewing DHCP Dynamic Bindings*
- *Configuring the DHCP User Class*
- *Configuring DHCP Pool Class*

5.2.1 Configuring the Switch DHCP Server

The switch contains an internal *Dynamic Host Configuration Protocol* (DHCP) Server. DHCP can provide the dynamic assignment of IP addresses automatically. 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 IP address, network mask and gateway.

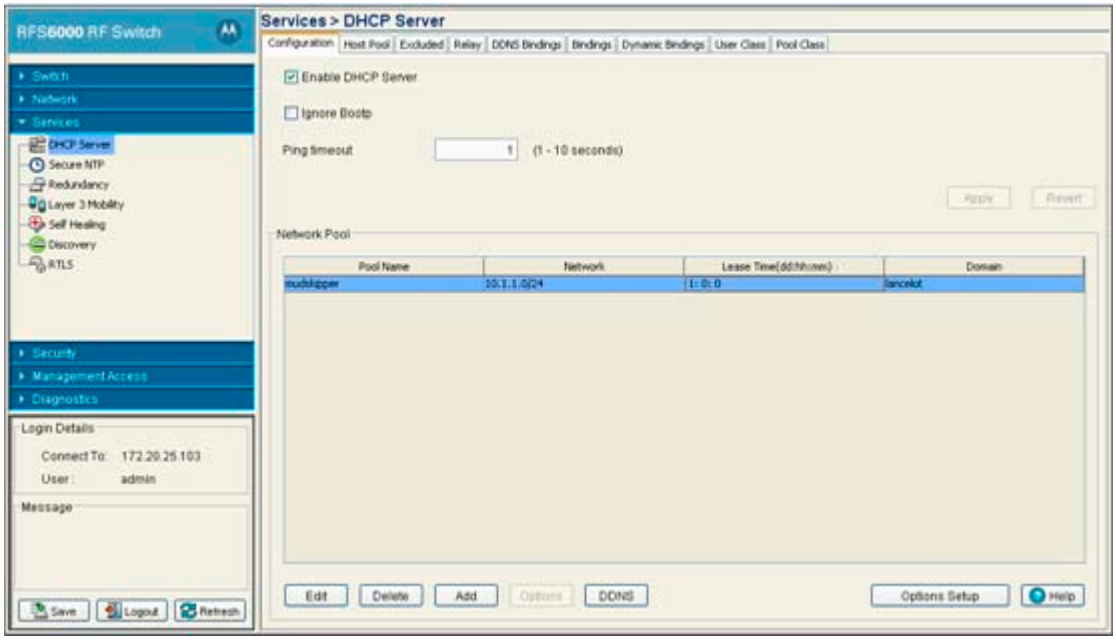
When a DHCP server allocates an address for a client, the client is assigned a lease (which expires after an interval defined by the administrator). Before the lease expires, clients are expected to renew the lease to continue to use the addresses assigned. Once a lease has expired, the client to which that lease was assigned is no longer permitted to use the leased IP address.

NOTE: DHCP Server setting updates are only implemented when the switch is restarted.

NOTE: When using the switch's internal DHCP server ensure that traffic can pass on UDP ports 67 & 68 between the switch and the clients receiving DHCP information.

To configure DHCP:

1. Select **Services** > **DHCP Server** from the main menu tree.



2. Select the **Enable DHCP Server** checkbox to enable the switch's internal DHCP Server for use with global pools.
3. Select the **Ignore BOOTP** checkbox to bypass a BOOTP request.
4. Define an interval (from 1 -10 seconds) for the **Ping timeout** variable. The switch uses the timeout to intermittently ping and discover whether the client requested IP address is already used.

5. Refer to the following as displayed within **Network Pool** field.

Pool Name	Displays the name of the IP pool from which IP addresses can be issued to DHCP client requests on the current interface. The pool is the range of IP addresses available.
Network	Displays the network address for the clients.
Lease Time (dd:hh:mm)	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 MU users change frequently. Use longer leases if there are fewer users.
Domain	Displays the domain name for the current interface.

6. Click the **Edit** button to modify the properties displayed on an existing DHCP pool. For more information, see *Editing the Properties of an Existing DHCP Pool on page 5-5*.
7. To delete an existing DHCP pool from the list of those available, highlight the pool from within the Network Pool field and click the **Delete** button.
8. Click the **Add** button to create a new DHCP pool. For more information, see *Adding a New DHCP Pool on page 5-6*.
9. Click the **Options** button to associate values to options, as defined using the Options Setup functionality. The values associated to options are local to the pool with which they are associated For more information, see *Configuring DHCP Global Options on page 5-8*.
10. Click the **DDNS** button to configure a DDNS domain and server address used with the list of available pools. For more information, see *Configuring DHCP Server DDNS Values on page 5-9*.
11. Click the **Options Setup** button to define the option name, code and type. Associate values to them (by clicking the Options button) only after the options are defined.
12. Click **Apply** to save changes to the screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
13. Click the **Revert** button to display the last saved configuration. Unapplied changes are not saved and must be re-entered.

5.2.1.1 Editing the Properties of an Existing DHCP Pool

The properties of an existing pool can be modified to suit the changing needs of your network.

To modify the properties of an existing pool:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select an existing pool from those displayed (within the Network Pool field) and click the **Edit** button.
3. Modify the name of the IP pool from which IP addresses can be issued to client requests on this interface.
4. Modify the **Domain** name as appropriate for the interface using the pool.
5. Modify the **NetBios Node** used with this particular pool. The NetBios Node could have one of the following types:
   - A **b-broadcast** (broadcast node) broadcasts to query network nodes for the owner of a NetBIOS name.

- A **p-peer** (peer-to-peer node) uses directed calls to communicate with a known NetBIOS name server, such as a *Windows Internet Name Service* (WINS) server, for the IP address of a NetBIOS machine.
- A **m-mixed** is a mixed node that uses broadcasted queries to find a node and queries a known p-node name server for the address.
- A **h-hybrid** is a combination of two or all of the nodes mentioned above.

6. Change the name of the boot file used for this pool within the **Boot File** parameter.
7. From the **Network** field, use the **Associated Interface** drop-down menu to modify (if necessary) the switch interface used for the newly created DHCP configuration. Use VLAN1 as a default interface if no others have been defined.
8. Additionally, define the **IP Address** and **Subnet Mask** used for DHCP discovery and requests between the DHCP Server and DHCP clients.

NOTE: The network IP address and subnet mask of the pool are required to match the addresses of the layer 3 interface for addresses to be supported on that interface.

9. Within the **Lease Time** field, define one of the two kinds of leases the DHCP Server assigns to its clients:
   - *Infinite* - If selected, the client can used the assigned address indefinitely.
   - *Actual Interval* - Select this checkbox to manually define the interval for clients to use the DHCP server assigned addresses. The default lease time is 1 day, with a minimum setting of 1 minute.
10. Within the **Servers** field, change the server type used with the pool and use the **Insert** and **Remove** buttons to add and remove the IP addresses of the routers used.
11. Modify the **Included Ranges** (starting and ending IP addresses) for this particular pool.

    Use the **Insert** and **Remove** buttons as required to define the range of supported IP addresses.

    A network pool without any include range is as good as not having a pool, because it won't be useful in assigning addresses.
12. Click **OK** to save and add the changes to the running configuration and close the dialog.
13. Refer to the **Status** field.

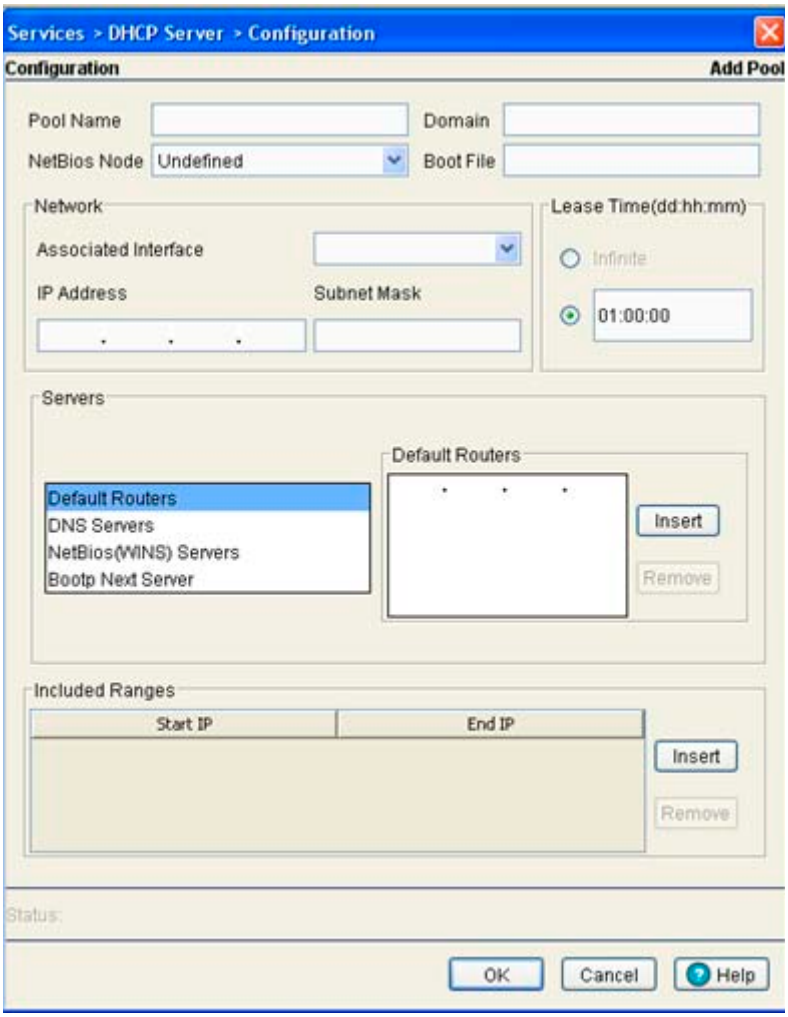
    The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
14. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.2.1.2 Adding a New DHCP Pool

Add a new DHCP pool as needed to suit the address distribution requirements of your network.

To add a DHCP pool:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Click the **Add** button at the bottom of the screen.



3. Enter the name of the IP pool from which IP addresses can be issued to client requests on this interface.
4. Provide the **Domain** name as appropriate for the interface using the pool.
5. Enter the **NetBios Node** used with this particular pool. The NetBios Node could have one of the following types:
   - A **b-broadcast** (broadcast node) uses broadcasting to query nodes on the network for the owner of a NetBIOS name.
   - A **p-peer** (peer-to-peer node) uses directed calls to communicate with a known NetBIOS name server, such as a *Windows Internet Name Service* (WINS) server, for the IP address of a NetBIOS machine.
   - An **m-mixed** is a mixed node that uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address.
   - An **h-hybrid** is a combination of two or all of the nodes mentioned above.
6. Enter the name of the boot file used for this pool within the **Boot File** parameter.

7. From the **Network** field, use the **Associated Interface** drop-down menu to define the switch interface is used for the newly created DHCP configuration. Use VLAN1 as a default interface if no others have been defined.

   Additionally, define the **IP Address** and **Subnet Mask** used for DHCP discovery and requests between the DHCP Server and DHCP clients.

NOTE: The IP address and subnet mask of the pool are required to match the addresses of the layer 3 interface in order for the addresses to be supported through that interface.

8. Within the **Lease Time** field, define one of the two kinds of leases the DHCP Server assigns to its clients:
   - *Infinite* - If selected, the client can use the assigned address indefinitely.
   - *Actual Interval* - Select this checkbox to manually define the interval for clients to use DHCP supplied addresses. The default lease time is 1 day, with a minimum setting of 60 seconds and a maximum value of 946080000 seconds.
9. Within the **Servers** field, change the server type used with the pool and use the **Insert** and **Remove** buttons to add and remove the IP addresses of the routers used.
10. Provide the **Included Ranges** (starting and ending IP addresses) for this particular pool.

    Use the **Insert** and **Remove** buttons as required to define the range of supported IP addresses.

    A network pool without any include range is as good as not having a pool, because it won't be useful in assigning addresses.
11. Click **OK** to save and add the changes to the running configuration and close the dialog.
12. Refer to the **Status** field.

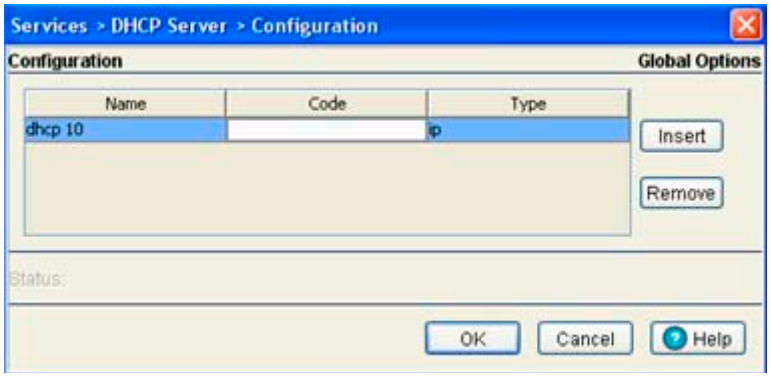
    The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
13. Click **Cancel** to close the dialog without committing updates to the running configuration

5.2.1.3 Configuring DHCP Global Options

The DHCP Server screen’s Configuration and Host Pool tabs can be used to display an additional **Global Options** screen.

To define new global name and value and send it to other peer switches in the mobility domain:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Highlight an existing pool name from within either the Configuration or Host Pool tab and click the **Options Setup** button at the bottom of the screen.



3. Click the **Insert** button to display an editable field wherein the name and value of the DHCP option can be added.
4. **Name** the option as appropriate, assign a **Code** (numerical identifier) and use the **Type** drop-down options to specify a value of ip or ascii to the DHCP global option.
5. Highlight an entry from within the Global Options screen and click the **Remove** button to delete the name and value.
6. Click **OK** to save and add the changes to the running configuration and forward the updates to the other peer switches comprising the mobility domain.
7. Refer to the **Status** field.

   The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **Cancel** to close the dialog without committing updates to the running configuration

5.2.1.4 Configuring DHCP Server DDNS Values

The DHCP Server screen's Configuration tab can be used to display an additional **DDNS** screen. Use this screen to define a DDNS domain name and address for use with the switch.

To configure a global domain name and DDNS server address:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Highlight an existing pool name from within either the Configuration or Host Pool tabs and click the **DDNS** button at the bottom of the screen.

3. Enter a **Domain Name** which represents the forward zone in the DNS server. For example *test.net*.
4. Define the **TTL** (Time to Live) to specify the validity of DDNS records. The maximum value is 864000 seconds.
5. Use the **Automatic Update** drop-down menu to specify whether the automatic update feature is on or off. Select **Server update** to enable a DDNS update from the DHCP server. Select **Client update** to get the DDNS updates from DHCP clients.
6. Select the **Enable Multiple User Class** checkbox if multiple user class support is needed.
7. Use the **DDNS Servers** field to define the IP addresses of the DNS servers.
8. Click **OK** to save and add the changes to the running configuration and close the dialog.
9. Refer to the **Status** field.

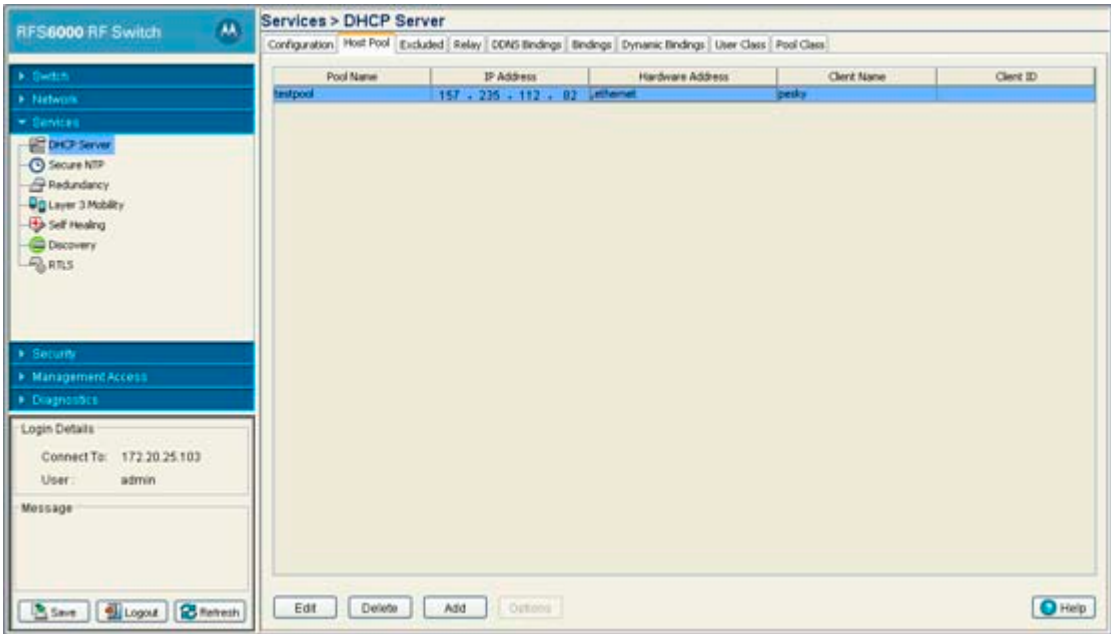
   The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **Cancel** to close the dialog without committing updates to the running configuration

5.2.2 Viewing the Attributes of Existing Host Pools

Refer to the **Host Pool** tab within the DHCP Server screen to view how the host pools reserve IP addresses for specific MAC addresses. This information can be an asset in determining if a new pool needs to be created or an existing pool requires modification.

To view the attributes of existing host pools:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select the **Host Pool** tab.



3. Refer to the following information to assess whether the existing group of DHCP pools is sufficient:

Pool Name	Displays the name of the IP pool from which IP addresses can be issued to DHCP client requests on this interface. The pool is the range of IP addresses for which addresses can be assigned.
IP Address	Displays the IP address for the client on this interface using the pool name listed.
Hardware Address	Displays the type of interface used to pass DHCP discover and request exchanges between the switch DHCP server and DHCP Clients. The Hardware Address field also displays the address of the DHCP client for whom the static IP is reserved.
Client Name	Displays the name of the client requesting DHCP Server support over this interface. This name is ready only cannot be modified using the host pool edit option.
Client ID	Displays the client Identifier, based on this identifier static IP is assigned. Hardware address and Client Identifier should not be configured on the same host pool. A pool name cannot have both a client ID and MAC address.

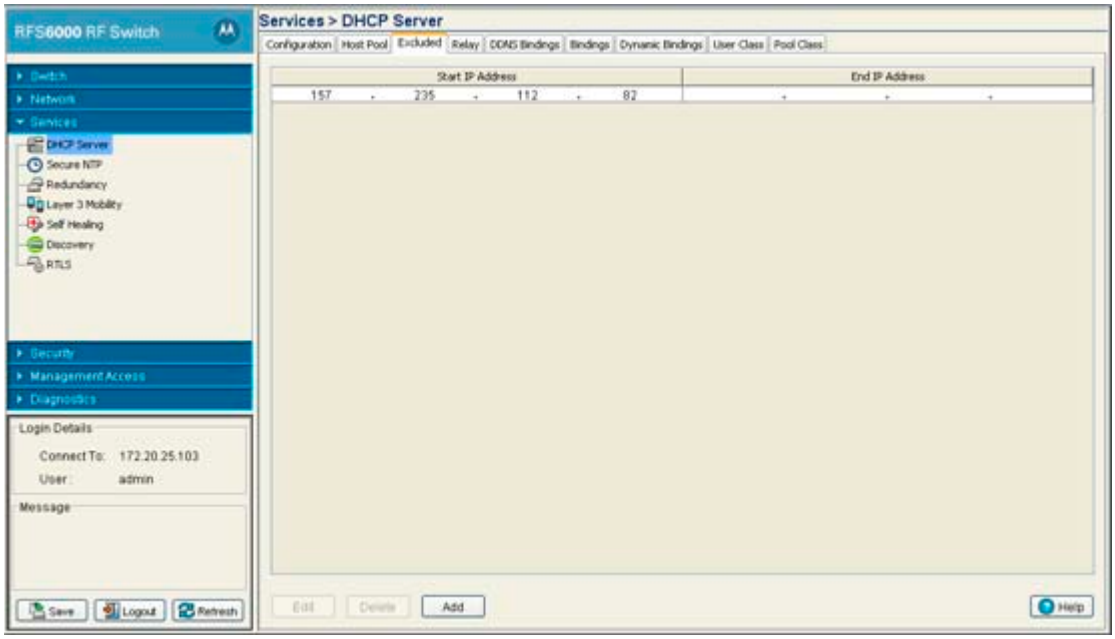
4. Click the **Edit** button to modify the properties displayed on an existing DHCP pool. For more information, see *Editing the Properties of an Existing DHCP Pool on page 5-5*.
5. To delete an existing DHCP pool from the list of those available, highlight the pool from within the Pool Name field and click the **Delete** button.
6. Click the **Add** button to create a new DHCP pool. For more information, see *Adding a New DHCP Pool on page 5-6*.
7. Click the **Options** button to insert a global pool name into the list of available pools. For more information, see *Configuring DHCP Global Options on page 5-8*.
8. Click the **DDNS** button to configure a DDNS domain and server address that can be used with the list of available pools. For more information, see *Configuring DHCP Server DDNS Values on page 5-9*.

5.2.3 Configuring Excluded IP Address Information

The DHCP Server may have some IP addresses unavailable when assigning IP address ranges for a pool. If IP addresses have been manually assigned and fixed, they need to be made available for the administrator to exclude from possible selection.

To view excluded IP address ranges:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Click the **Excluded** tab.



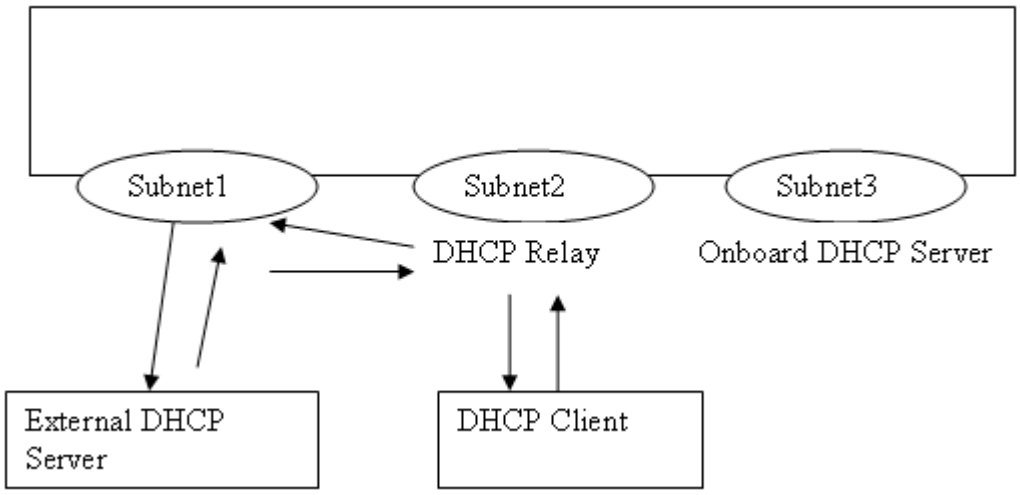
The Excluded tab displays *fixed* IP addresses statically assigned and unavailable for assignment with a pool.

3. Click the **Edit** button to modify the IP address range displayed. For more information, see *Editing the Properties of an Existing DHCP Pool on page 5-5*.
4. To delete an existing DHCP pool from the list of those available to the switch, highlight the pool from within the Network Pool field and click the **Delete** button.
5. Click the **Add** button to create a new IP address range for a target host pool. For more information, see *Adding a New DHCP Pool on page 5-6*.

5.2.4 Configuring the DHCP Server Relay

Refer to the **Relay** tab to view the current DHCP Relay configurations for available switch VLAN interfaces. The Relay tab also displays the VLAN interfaces for which the DHCP Relay is enabled/configured. The Gateway Interface address information is helpful in selecting the interface suiting the data routing requirements between the External DHCP Server and DHCP client (present on one of the switch's available VLANs).

NOTE: DHCP Server and relay can run on different switch VLAN interfaces.

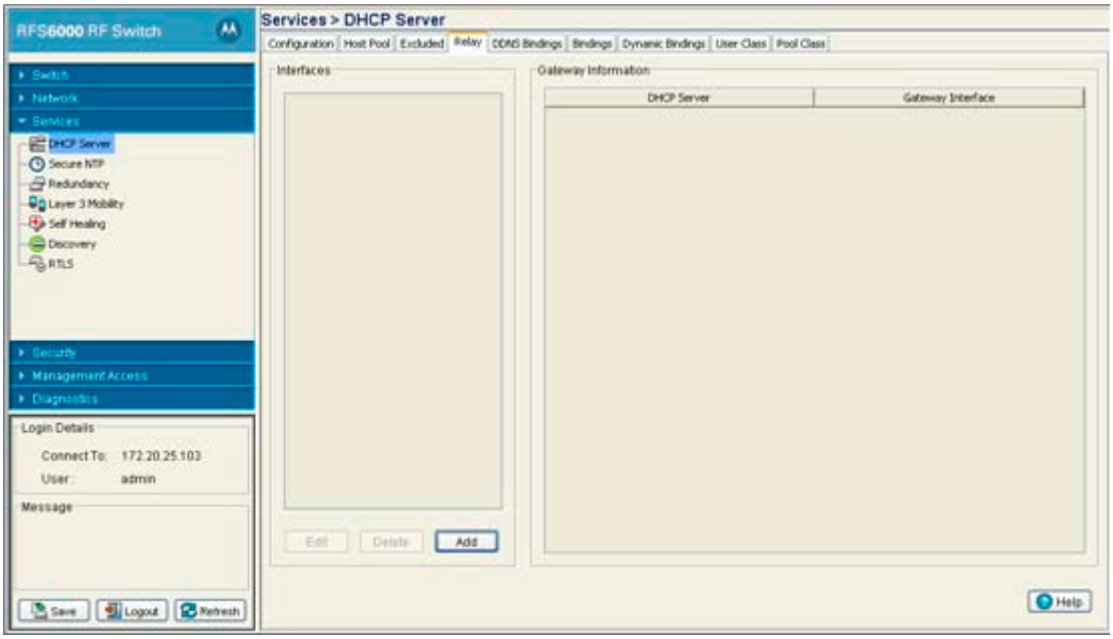


In the illustration above, a DHCP relay address has been configured on subnet 2 (The CLI equivalent is "ip helper-address <subnet1 External DHCP Server IP > <subnet1 Interface Name>"). When configuring a DHCP Relay address, specify the other interface where the external DHCP Server can be reached. In this example, that interface is subnet1. The DHCP relay agent must listen on both subnet1 and subnet2. Consequently, the DHCP Server cannot run on either subnet1 or subnet2 (it must be both).

However, you can run an onboard DHCP server on subnet3 to provide DHCP requests for clients in subnet3. This is independent of the DHCP relay configuration. You cannot run onboard DHCP Server on subnet1 to provide IP addresses to DHCP clients requesting IP addresses using DHCP relay.

To view and configure DHCP relay information:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Click the **Relay** tab.



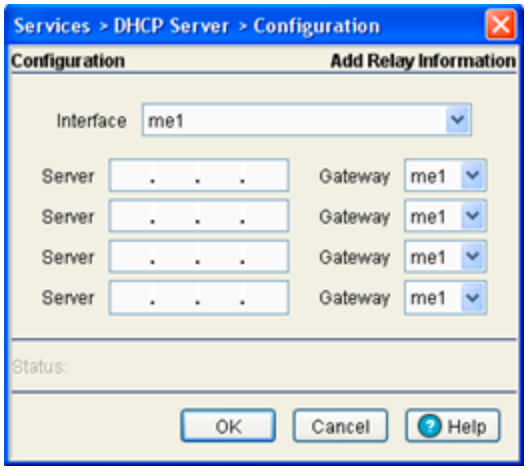
3. Refer to the **Interface**s field for the names of the interfaces available to route information between the DHCP Server and DHCP clients. If this information is insufficient, consider creating a new IP pool or edit an existing pool.
4. Refer to the **Gateway Information** field for DHCP Server and Gateway Interface IP addresses. Ensure these address are not in conflict with the addresses used to route data between the DHCP Server and client.

NOTE: The gateway address should not be set to a VLAN interface used by the switch.

5. Click the **Edit** button to modify the properties displayed on an existing DHCP pool. Refer to step 7 for the information that can be modified for the DHCP relay.
6. To delete an existing DHCP pool from the list of those available to the switch, highlight the pool from within the Network Pool field and click the **Delete** button.

NOTE: The interface VLAN and gateway interface should have their IP addresses set. The interface VLAN and gateway interface should not have DHCP client or DHCP Server enabled. DHCP packets cannot be relayed to an onboard DHCP Server. The interface VLAN and gateway interface cannot be the same.

7. Click the **Add** button to create a new DHCP pool.



a. Use the **Interface** drop-down menu to assign the interface used for the DHCP relay. As VLANs are added to the switch, the number of interfaces available grows.

b. Add **Servers** as needed to supply DHCP relay resources. As Servers are added, use the **Gateway** drop-down menu associated with each Server to supply the interface used to route data. The gateway address should not be set to any VLAN interface used by the switch.

c. Click **OK** to save and add the changes to the running configuration and close the dialog.

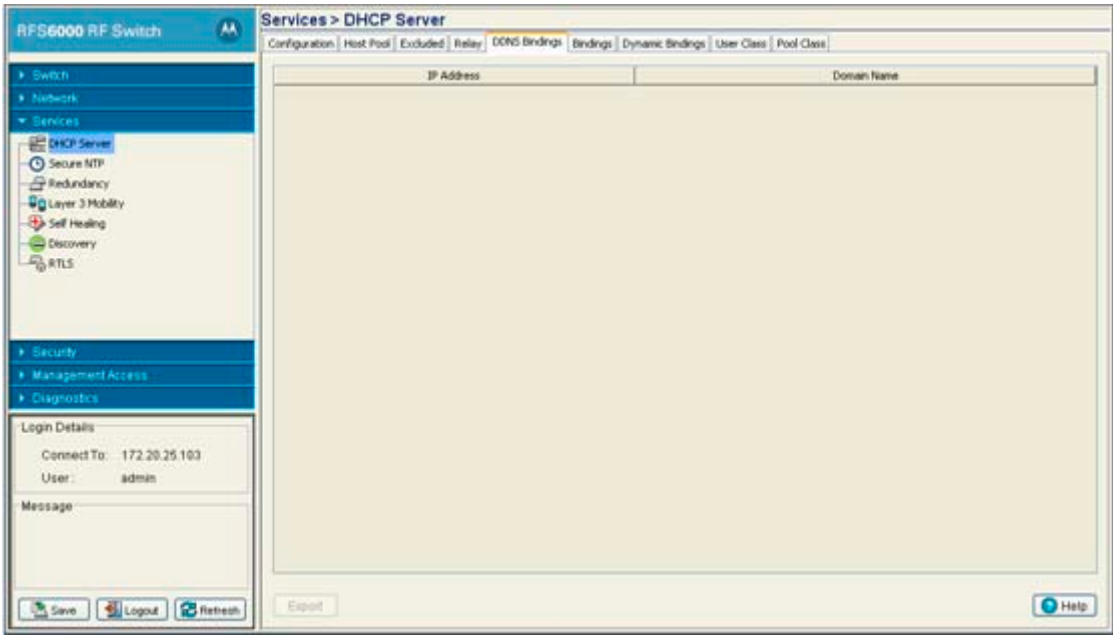
d. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.2.5 Viewing DDNS Bindings

The **DDNS Bindings** tab displays mappings between client IP addresses and domain names. DDNS keeps a domain name linked to a changing IP address. Typically, when a user connects to a network, the user's ISP assigns an unused IP address from a pool of IP addresses (usually done through a DHCP server). This address is only valid for a limited time. The mechanism of dynamically assigning IP addresses increases the pool of assignable IP addresses. DNS is a service, which maintains a database to map a given name to an IP address used for communication on the Internet. The dynamic assignment of IP addresses makes it necessary to update the DNS database to reflect the current IP address for a given name.

To view switch DDNS binding information:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select the **DDNS Bindings** tab.



3. Refer to the contents of the DDNS Bindings tab for the following information:

IP Address	Displays the IP address assigned to the client.
Domain Name	Displays the domain name mapping corresponding to the IP address listed in the left-hand side of the tab.

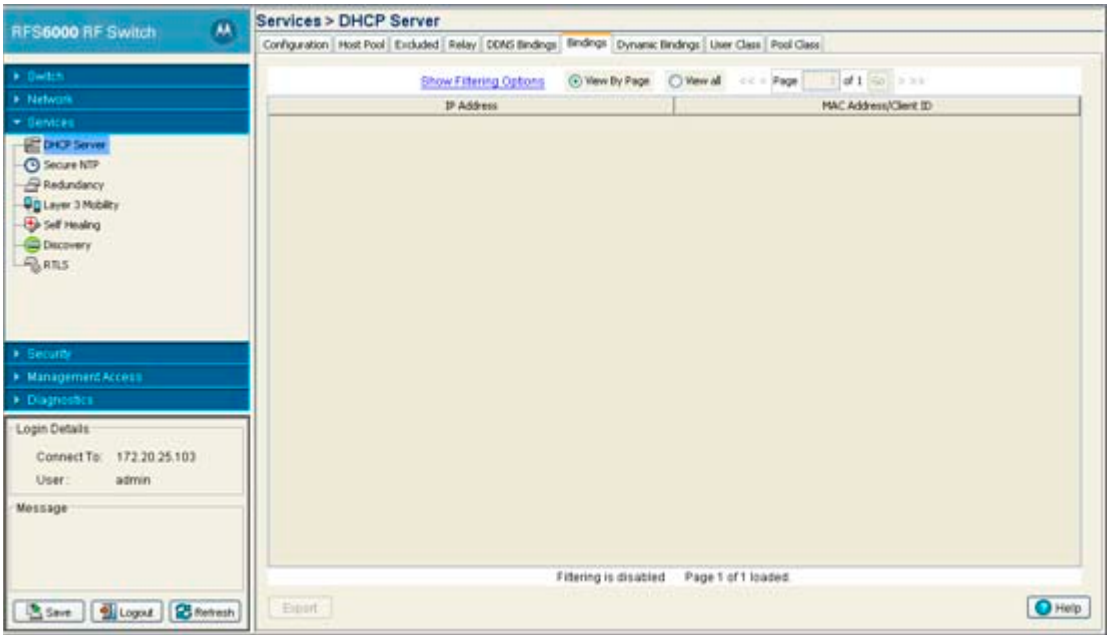
4. Click the **Export** button to display a screen used to export DDNS Binding information to a secure location.

5.2.6 Viewing DHCP Bindings

The Bindings tab displays addresses and expiration times. There are two types of bindings, manual and automatic. Manual bindings map a hardware address to a IP address statically. Automatic bindings dynamically map a hardware address to an IP address from a pool of available addresses.

To view detailed binding information:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select the **Bindings** tab.



3. Refer to the contents of the **Bindings** tab for the following information:

IP Address	Displays a IP address for each client with a listed MAC address. This column is read-only and cannot be modified.
MAC Address / Client ID	Displays the MAC address (client hardware ID) of the client using the switch's DHCP Server to access switch resources. The MAC address is read-only and cannot be modified.

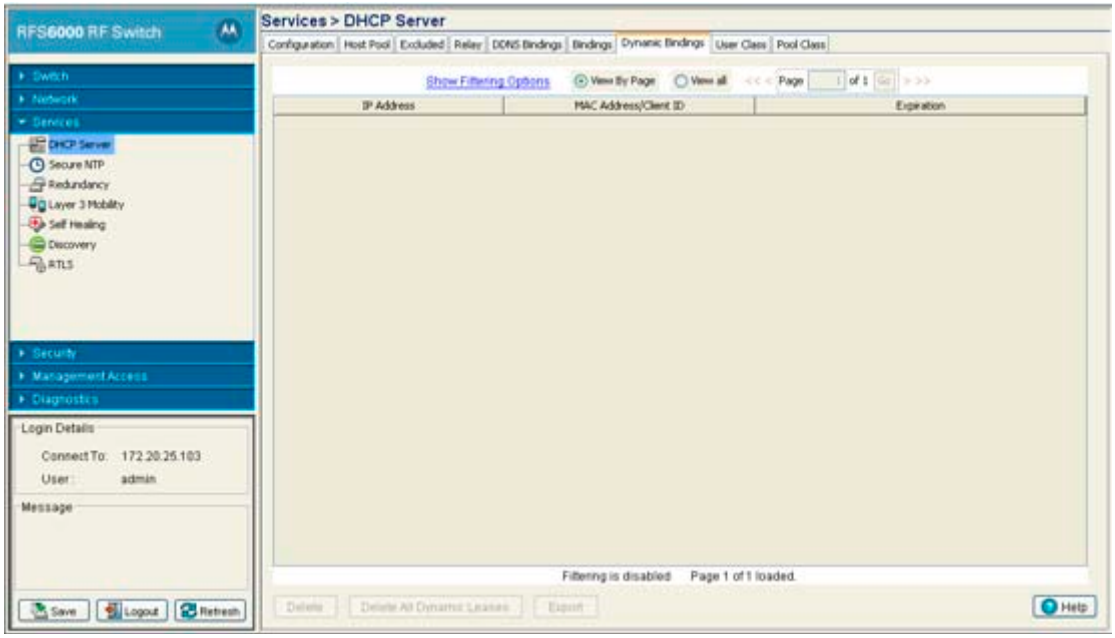
4. Click the **Export** button to display a screen used to export the DHCP Binding information to a secure location.

5.2.7 Reviewing DHCP Dynamic Bindings

Dynamic DHCP bindings automatically map a hardware address to an IP address from a pool of available addresses. The Dynamic Bindings tab displays only automatic bindings.

To view detailed Dynamic DHCP Binding Status information:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select the **Dynamic Bindings** tab.



3. Refer to the contents of the Dynamic Bindings tab for the following:

IP Address	Displays the IP address for each client whose MAC Address is listed in the MAC Address / Client ID column. This column is read-only and cannot be modified.
MAC Address / Client ID	Displays the MAC address (client hardware ID) of the client using the switch's DHCP Server to access switch resources. The MAC address is read-only and cannot be modified.
Expiration	Displays the expiration of the lease used by the client for switch DHCP resources. This column is read-only and cannot be modified.

4. Select an address from those displayed and click the **Delete** button to remove the client from the list displayed. The Delete button is enabled only when one or more rows are selected for deletion.
5. Click on **Delete All Automatic Leases** button to delete all the automatic leased DHCP connections. This button is enabled when one or more rows exist.
6. Click the **Export** button to display a screen used to export the DHCP Binding information to a secure location.

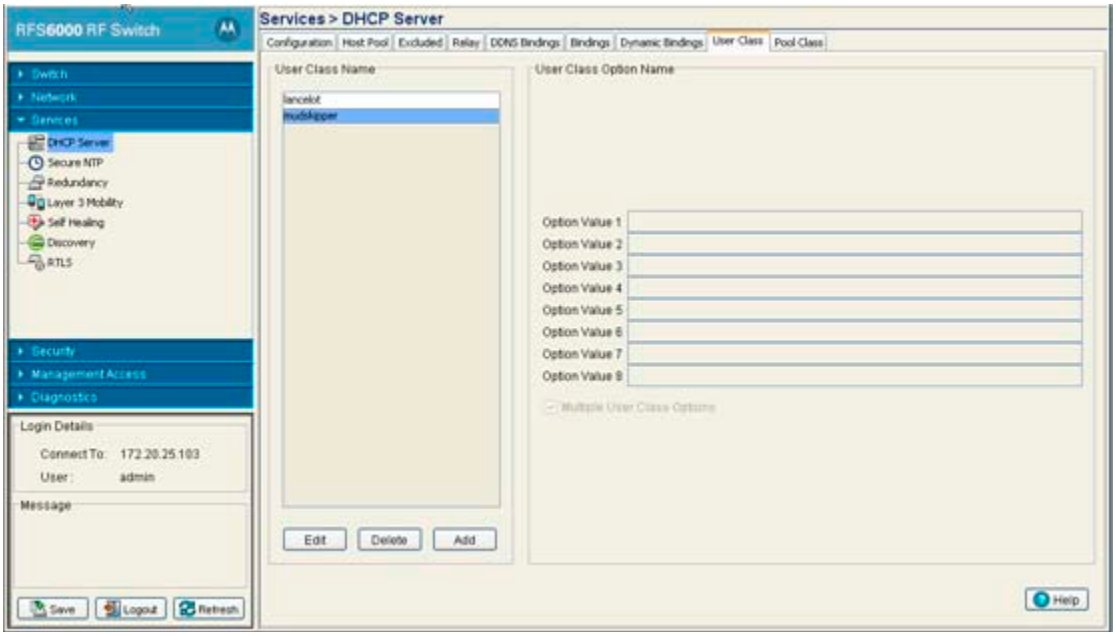
5.2.8 Configuring the DHCP User Class

The DHCP server assigns IP addresses to 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 assigns IP addresses from multiple IP address ranges. 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.

To view the attributes of existing host pools:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select the **User Class** tab to view the DHCP user class and its associated user class option names.



3. The **User Class Name** field displays the client names grouped by the class name.
4. The **User Class Option Name** field displays the names defined for a particular client.

   Select the **Multiple User Class Options** checkbox to associate the user class option names with a multiple user class.
5. Click the **Add** button create a new user class name (client). For more information, see *Adding a New DHCP User Class on page 5-19*.
6. Click the **Edit** button to modify the properties displayed for an existing DHCP User Class Name. For more information, see *Editing the Properties of an Existing DHCP User Class on page 5-20*.
7. To delete an existing DHCP user class and its associated option names from the list available to the DHCP server, select the user class from the **User Class Name** field and click **Delete**.

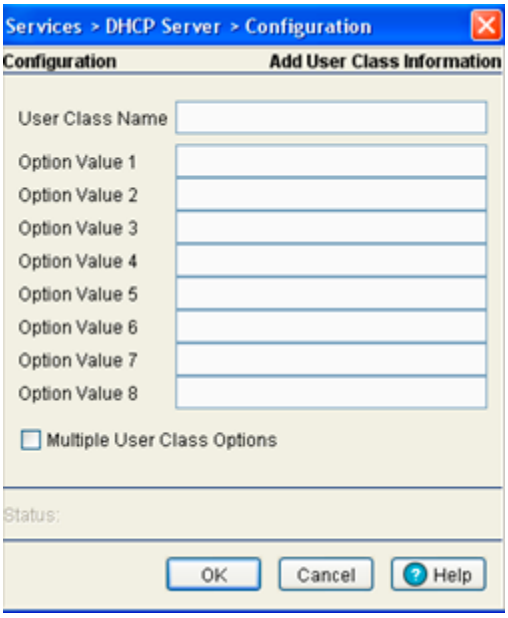
5.2.8.1 Adding a New DHCP User Class

A DHCP user class name can be configured with a maximum of 8 user class option values.

To view and configure the user class options associated with the particular class:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select the **User Class** tab.

3. Click the **Add** button from the **User Class Name** field.



The DHCP server groups clients based on user class option values. DHCP Clients with the defined set of user class option values are identified by class.

a. Enter the **User Class Name** to create a new client. The DHCP user class name should not exceed 32 characters.

b. Enter **Option Values** for the devices associated with the DHCP user class name. The value should not exceed 32 characters.

c. Select the **Multiple User Class Option** checkbox 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.

d. Click **OK** to save and add the new configuration.

e. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.

f. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.2.8.2 Editing the Properties of an Existing DHCP User Class

The properties of an existing DHCP user class can be modified to suit the changing needs of your network. To modify the properties of an existing DHCP user class:

1. Select **Services > DHCP Server** from the main menu tree.
2. Select the **User Class** tab.
3. Select an existing DHCP user class name from the list and click on the **Edit** button from the **User Class Name** field.

   a. The **User Class Name** is a display field and cannot be modified.

   b. Either add or modify the **Option Values** as required to suit the changing needs of your network. The option values should not exceed 50 characters.

c. Select the **Multiple User Class Option** checkbox to enable multiple option values for the user class. This allows the user class to transmit multiple option values to DHCP servers which support multiple user class options.

d. Click **OK** to save and add the new configuration and close the dialog window.

e. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.

f. Click **Cancel** to close the dialog without committing updates to the running configuration.

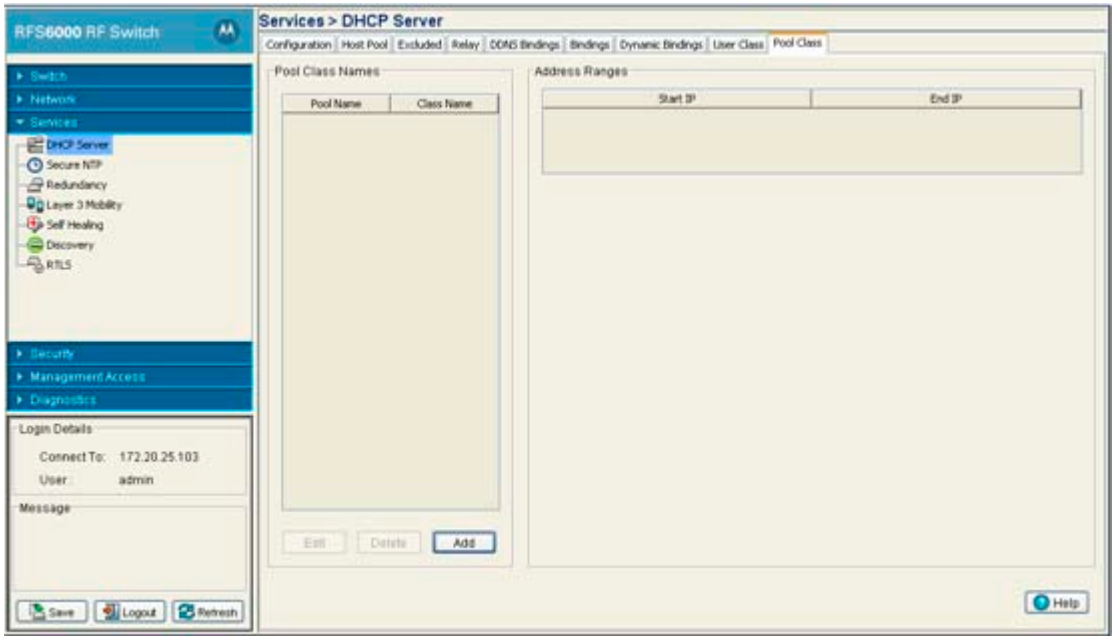
5.2.9 Configuring DHCP Pool Class

The 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 matched against classes. If the client matches one of the classes assigned to the pool, it's assigned the IP address from the range assigned to the class. If the client does not match any of the classes in the pool, it's assigned the IP address from the pool's default range (if configured).

To view the attributes of existing host pools:

1. Select **Services** > **DHCP Server** from the main menu tree.
2. Select the **Pool Class** tab to view the DHCP pool class details.



3. Refer to the **Pool Class Names** field to configure a pool class. A pre configured pool and class must exist to configure a pool class.

   The **Address Ranges** section displays the address ranges associated with the pool class.

4. Click the **Edit** button to modify the properties displayed for an existing DHCP Pool Class Name. For more information, see *Editing an Existing DHCP Pool Class on page 5-22*.
5. To delete an existing DHCP pool class name and its associated address range, select the pool class name from the **Pool Class Names** field and click the **Delete** button.

6. Click the **Add** button create a new pool class name. For more information, see *Adding a New DHCP Pool Class on page 5-22*.

5.2.9.1 Editing an Existing DHCP Pool Class

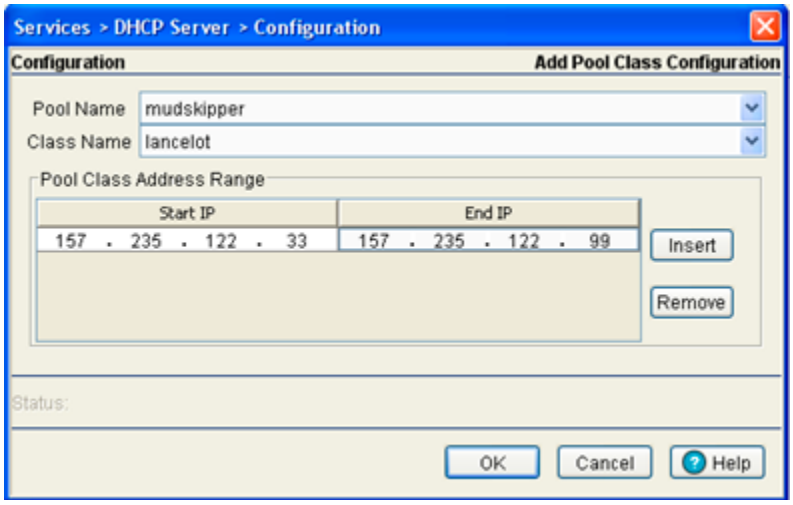
The **Edit DHCP Pool Class Configuration** dialog is used to edit the association of a DHCP pool name to a DHCP class name. It is also used to configure a maximum of 4 pool class address range. To revise an existing DHCP pool class name:

1. Select **Services > DHCP Server** from the main menu tree.
2. Select the **Pool Class** tab.
3. Click on the **Edit** button from the **Pool Class Names** section.
4. Refer to the read-only **Pool Name** to ensure modifications are made to the correct pool name.
5. Use the **Class Name** field to associate an existing class, created using *Adding a New DHCP User Class on page 5-19*.
6. Refer to the **Pool Class Address Range** field to revise an address range. A maximum of 4 address ranges can be assigned to a class.
   a. Use the **Insert** button to revise the Start IP and End IP address range for a class.
   b. Select a address range and click **Remove** to delete that particular address range.
7. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to save the new configuration and close the dialog window.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.2.9.2 Adding a New DHCP Pool Class

The **Add DHCP Pool Class Configuration** dialog is used to associate an existing class, created using *Adding a New DHCP User Class*, to an existing pool, created using *Adding a New DHCP Pool*. It is also used to configure a maximum of 4 pool class address range. To add a new DHCP pool class:

1. Select **Services > DHCP Server** from the main menu tree.
2. Select the **Pool Class** tab.
3. Click on the **Add** button from the **Pool Class Names** section.



4. Use the **Pool Name** field to define a new pool name. Enter the pool name created using *Adding a New DHCP Pool on page 5-6*.
5. Use the **Class Name** field to associate an existing class, created using *Adding a New DHCP User Class on page 5-19*.
6. The **Pool Class Address Range** field is used to assign address range to the class inside the pool. A maximum of 4 address ranges can be assigned to a class.
   a. Use the **Insert** button to enter the Start IP and End IP address range for a class.
   b. Select a address range and click **Remove** to delete that particular address range.
7. Refer to the **Status** field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to save the new configuration and close the dialog window.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.3 Configuring Secure NTP

Secure Network Time Protocol (SNTP) is central for networks that rely on their switch to supply system time. Without an SNTP implementation, switch time is unpredictable, which can result in data loss, failed processes and compromised security. With network speed, memory and capability increasing at an exponential rate, the accuracy, precision and synchronization of network time is essential in a switch managed enterprise network. The switch can either use a dedicated server to supply system time or can use several forms of SNTP messaging to sync system time with network traffic authenticated and secure for switch interoperation.

NOTE: Often, the switch NTP status will not be adequately updated after modifying the NTP configuration. Periodically check the switch NTP status when making changes to ensure the proper time is displayed, as it may take awhile for the switch to update the proper NTP status.

The SNTP configuration activity is divided amongst the following tasks:

- *Defining the SNTP Configuration*
- *Configuring Symmetric Keys*
- *Defining a NTP Neighbor Configuration*
- *Viewing NTP Associations*
- *Viewing NTP Status*

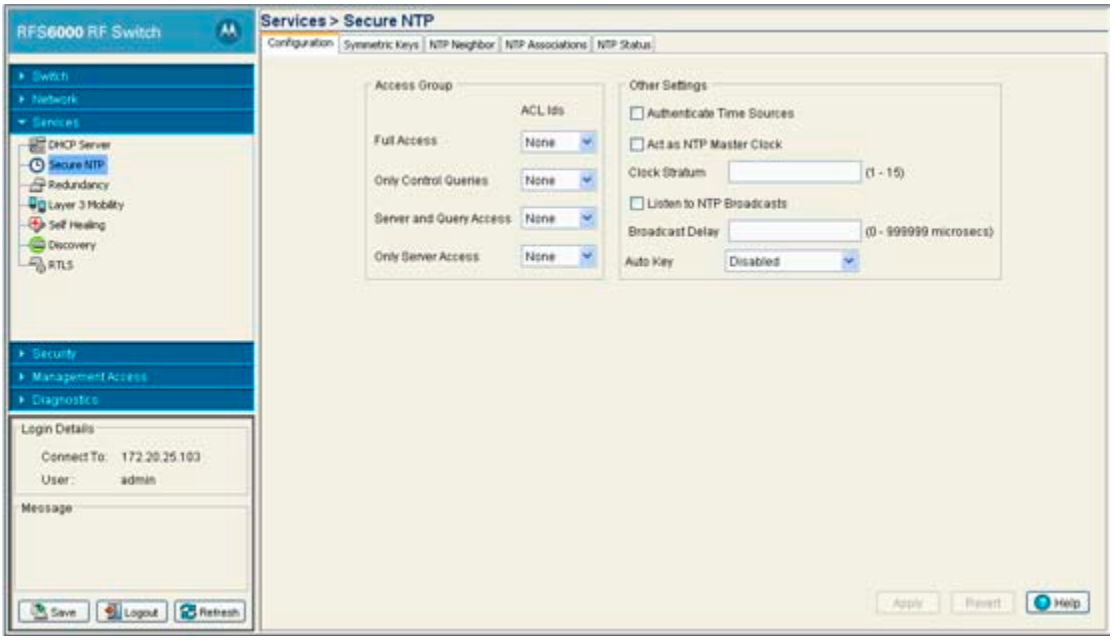
5.3.1 Defining the SNTP Configuration

Symmetric keys are algorithms for cryptography that use trivially related cryptographic keys for both decryption and encryption. The encryption key is related to the decryption key, as they may be identical or there is a simple mechanism to go between keys. The keys represent a shared secret between the switch and its time resource.

NOTE: When using the SNTP service, ensure that traffic can pass on UDP port 123 between the switch and the NTP server.

To define the SNTP configuration:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **Configuration** tab.



3. An ACL Id must be created before it is selectable from any of the drop-down menus. Refer to the **Access Group** field to define the following:

Full Access	Supply a numeric ACL ID from the drop-down menu to provide the ACL full access.
Only Control Queries	Supply a numeric ACL ID from the drop-down menu to provide the ACL only control query access to SNTP resources.
Server and Query Access	Enter a numeric ACL ID from the drop-down menu to provide the ACL Server and Query access to SNTP resources.
Only Server Access	Provide a numeric ACL ID from the drop-down menu to provide the ACL only server access to SNTP resources.

4. Refer to the **Other Settings** field to define the following:

Authenticate Time Sources	Select this checkbox to ensure credential authentication takes place between the SNTP server and the switch. When this checkbox is selected, the Apply and Revert buttons become enabled to save or cancel settings.
Act As NTP Master Clock	When this checkbox is selected, the Apply and Revert buttons become enabled to save or cancel settings within the Other Settings field.
Clock Stratum	Define how many hops (from 1 to 15) the switch is from a SNTP time source. The switch automatically chooses the SNTP resource with the lowest stratum number. The SNTP supported switch is careful to avoid synchronizing to a server that may not be accurate. Thus, the SNTP enabled switch never synchronizes to a machine not synchronized itself. The SNTP enabled switch compares the time reported by several sources, and does not synchronize to a time source whose time is significantly different than others, even if its stratum is lower.
Listen to NTP Broadcasts	Select this checkbox to allow the switch to listed over the network for SNTP broadcast traffic. Once enabled, the switch and the SNTP broadcast server must be on the same network.

Broadcast Delay	Enter the estimated round-trip delay (between 1 and 999999 seconds) for SNTP broadcasts between the SNTP broadcast server and the switch. Define the interval based on the priority of receiving accurate system time frequently. Typically, no more than one packet per minute is necessary to synchronize the switch to within a millisecond of the SNTP broadcast server.
Auto Key	Use use an **Auto Key** drop-down menu to specify whether the a key is disabled, enabled only on the host or enabled only on the client.

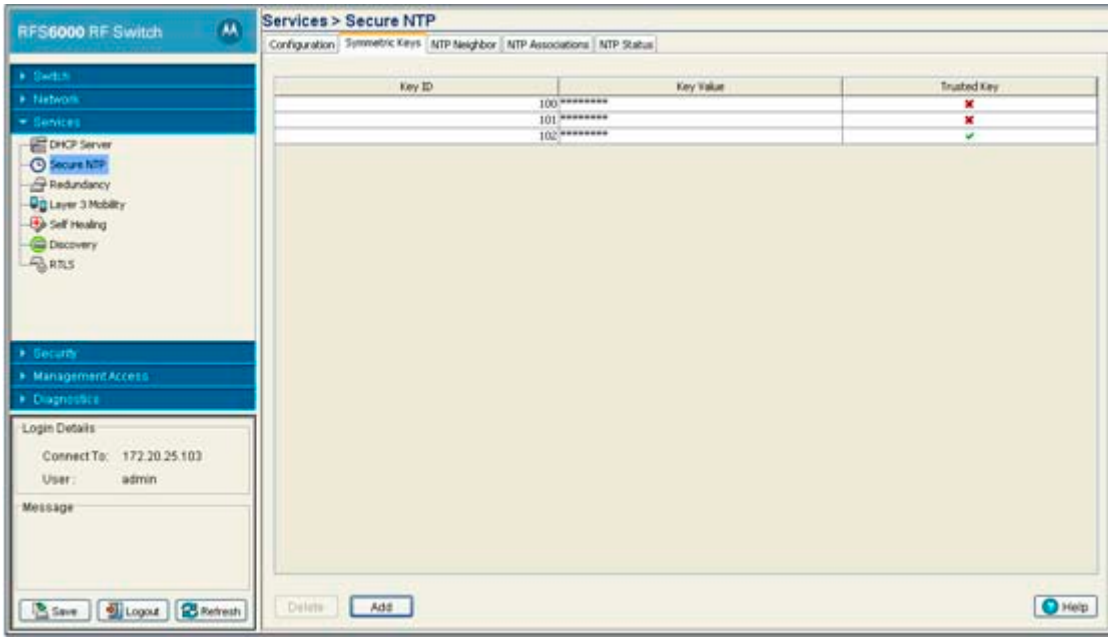
5. Click **Apply** to save changes to the screen. Navigating away from the screen without clicking the Apply button results in all the changes to the screen being discarded.
6. Click the **Revert** button to undo the changes to the screen and revert to the last saved configuration.

5.3.2 Configuring Symmetric Keys

Symmetric keys are algorithms for cryptography that use trivially related cryptographic keys for both decryption and encryption. The encryption key is related to the decryption key, as they may be identical or there is a simple mechanism to go between keys. The keys represent a shared secret between the switch and its time resource.

To review existing Symmetric Key configurations, and (if necessary) add a new one:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **Symmetric Keys** tab.



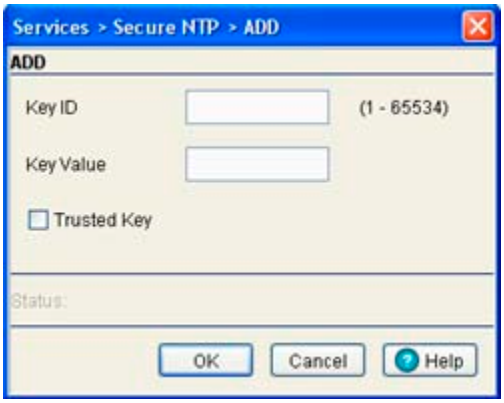
3. Refer to the **Symmetric Key** screen to view the following information.

Key ID	Displays a Key ID between 1-65534. The Key ID is a abbreviation allowing the switch to reference multiple passwords. This makes password migration easier and more secure between the switch and its NTP resource.

Key Value	Displays the authentication value used to secure the credentials of the server providing system time to the switch.
Trusted Key	If a checkmark appears, a trusted key has been associated with a domain name. A trusted key is added when a public key is known, but cannot be securely obtained. Adding the trusted key allows information from the server to be considered secure. The authentication procedures requires both the local and remote servers share the same key and key identifier. Therefore, using key information from a trusted source is important.

4. Select an existing key and click the **Delete** button to permanently remove it from the list of Key IDs.
5. Click the **Add** button to create a new Symmetric Key that can be used by the switch.

CAUTION: After an NTP synchronization using a Symmetric Key, the NTP status will not automatically be updated.



6. Enter a Key ID between 1-65534. The **Key ID** is a Key abbreviation allowing the switch to reference multiple passwords.

   This makes password migration easier and more secure between the switch and its NTP resource.
7. Enter an authentication **Key Value** used to secure the credentials of the NTP server providing system time to the switch.
8. Select the **Trusted Key** checkbox to use a trusted key.

   A trusted key should be used when a public key is known, but cannot be securely obtained. Adding a trusted key allows data to be considered secure between the switch and its SNTP resource.
9. Refer to the **Status** field.

   The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to save and add the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

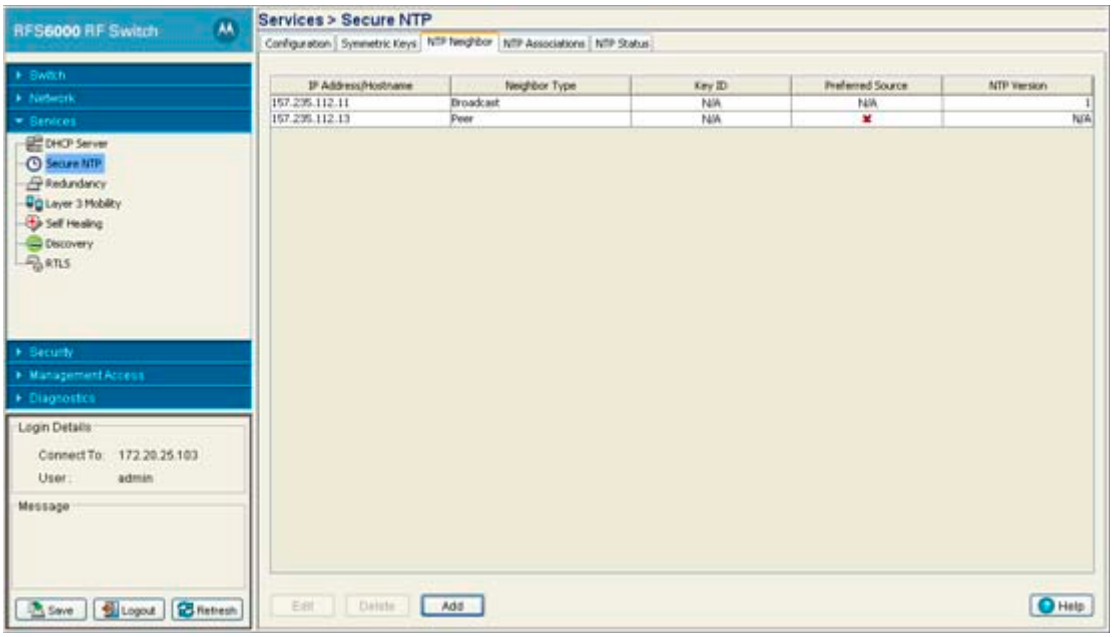
5.3.3 Defining a NTP Neighbor Configuration

The switch's NTP association can be either a neighboring peer (the switch synchronizes to another associated device) or a neighboring server (the switch synchronizes to a dedicated SNTP server resource).

Refer to the **NTP Neighbor** tab to assess the switch's existing configurations (both peer and server) and, if necessary, modify the attributes of an existing peer or server configuration or create a new neighbor peer or server SNTP configuration.

To review the switch's existing NTP neighbor configurations:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **NTP Neighbor** tab.



3. Refer to the following information (as displayed within the NTP Neighbor tab) to assess whether an existing neighbor configuration can be used as is, if an existing configuration requires modification or a new configuration is required.

IP Address/ Hostname	Displays the numeric IP address of the resource (peer or server) providing switch SNTP resources. Ensure the server is on the same subnet as the switch to provide SNTP support.
Neighbor Type	Displays whether the NTP resource is a Peer (another associated peer device capable of SNTP support) or a Server (a dedicated NTP server resource). This designation is made when adding or editing an NTP neighbor.
Key ID	Displays whether AutoKey Authentication or Symmetric Key Authentication is used to secure the interaction between the switch and its NTP resource. This designation is made when adding or editing an NTP neighbor.
Preferred Source	Displays whether this NTP resource is a preferred NTP resource. Preferred sources (those with a checkmark) are contacted before non-preferred resources. There can be more than one preferred source.
NTP Version	Displays a NTP version between 1 and 4. Currently version three and four implementations of NTP are available. The latest version is NTPv4, but the official Internet standard is NTPv3.

4. Select an existing neighbor and click the **Edit** button to modify the existing peer or server designation, IP address, version, authentication key ID and preferred source designation.

5. Select an existing entry and click the **Delete** button to remove it from the table.
6. Click the **Add** button to define a new peer or server configuration that can be added to the existing configurations displayed within the NTP Neighbor tab.For more information, see *Adding an NTP Neighbor on page 5-29*.

5.3.4 Adding an NTP Neighbor

To add a new NTP peer or server neighbor configuration to those available for synchronization:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **NTP Neighbor** tab.
3. Click the **Add** button.

4. Select the **Peer** checkbox if the SNTP neighbor is a peer to the switch (non FTP server) within the switch's current subnet.
5. Select the **Server** checkbox if the neighbor is a server within the switch's current subnet.
6. Select the **Broadcast Server** checkbox to allow the switch to listen over the network for NTP broadcast traffic.

   The switch's NTP configuration can be defined to use broadcast messages instead of messaging between fixed NTP synchronization resource addresses. Use a NTP broadcast to listen for NTP synchronization packets within a network. To listen to NTP broadcast traffic, the broadcast server (and switch) must be

on the same subnet. NTP broadcasts reduce configuration complexity since both the switch and its NTP resources can be configured to send and receive broadcast messages.

NOTE: If this checkbox is selected, the AutoKey Authentication checkbox is disabled, and the switch is required to use Symmetric Key Authentication for credential verification with its NTP resource. Additionally, if this option is selected, the broadcast server cannot be selected as a preferred source.

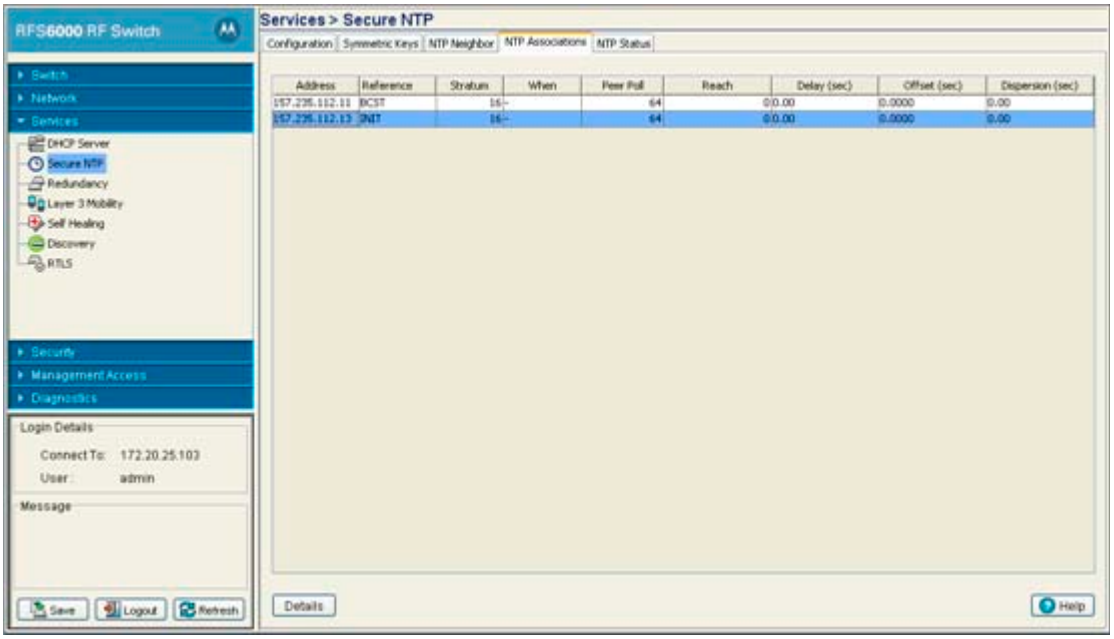
7. Enter the **IP Address** of the peer or server providing SNTP synchronization.
8. Select the **Hostname** checkbox to assign a hostname to the server or peer for further differentiation of other devices with a similar configuration.
9. Use the **NTP Version** drop-down menu to select the version of SNTP to use with this configuration Currently version three and version four implementations of NTP are available. The latest version is NTPv4, but the official Internet standard is NTPv3.
10. If necessary, select the **No Authentication** checkbox to allow communications with the NTP resource without any form of security. This option should only be used with known NTP resources.
11. Select the **AutoKey Authentication** checkbox to use an Auto key protocol based on the public key infrastructure (PKI) algorithm. The SNTP server uses a fast algorithm and a private value to regenerate key information on the arrival of a message. The switch sends its designated public key to the server for credential verification and the two exchange messages. This option is disabled when the Broadcast Server checkbox is selected.
12. Select the **Symmetric Key Authentication** checkbox to use a single (symmetric) key for encryption and decryption. Since both the sender and the receiver must know the same key, it is also referred to as shared key cryptography. The key can only be known by the sender and receiver to maintain secure transmissions.
13. Enter an **Key ID** between 1-65534. The Key ID is a Key abbreviation allowing the switch to reference multiple passwords.
14. Select the **Preferred Source** checkbox if this NTP resource is a preferred NTP resource. Preferred sources are contacted before non-preferred resources. There can be more than one preferred source.
15. Refer to the **Status** field. The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
16. Click **OK** to save and add the changes to the running configuration and close the dialog.
17. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.3.5 Viewing NTP Associations

The interaction between the switch and a SNTP server constitutes an association. SNTP associations can be either a peer association (the switch synchronizes to the another system or allows another system to synchronize to it), or a server association (only the switch synchronizes to the SNTP resource, not the other way around).

To review the switch's current SNTP associations:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **NTP Associations** tab.

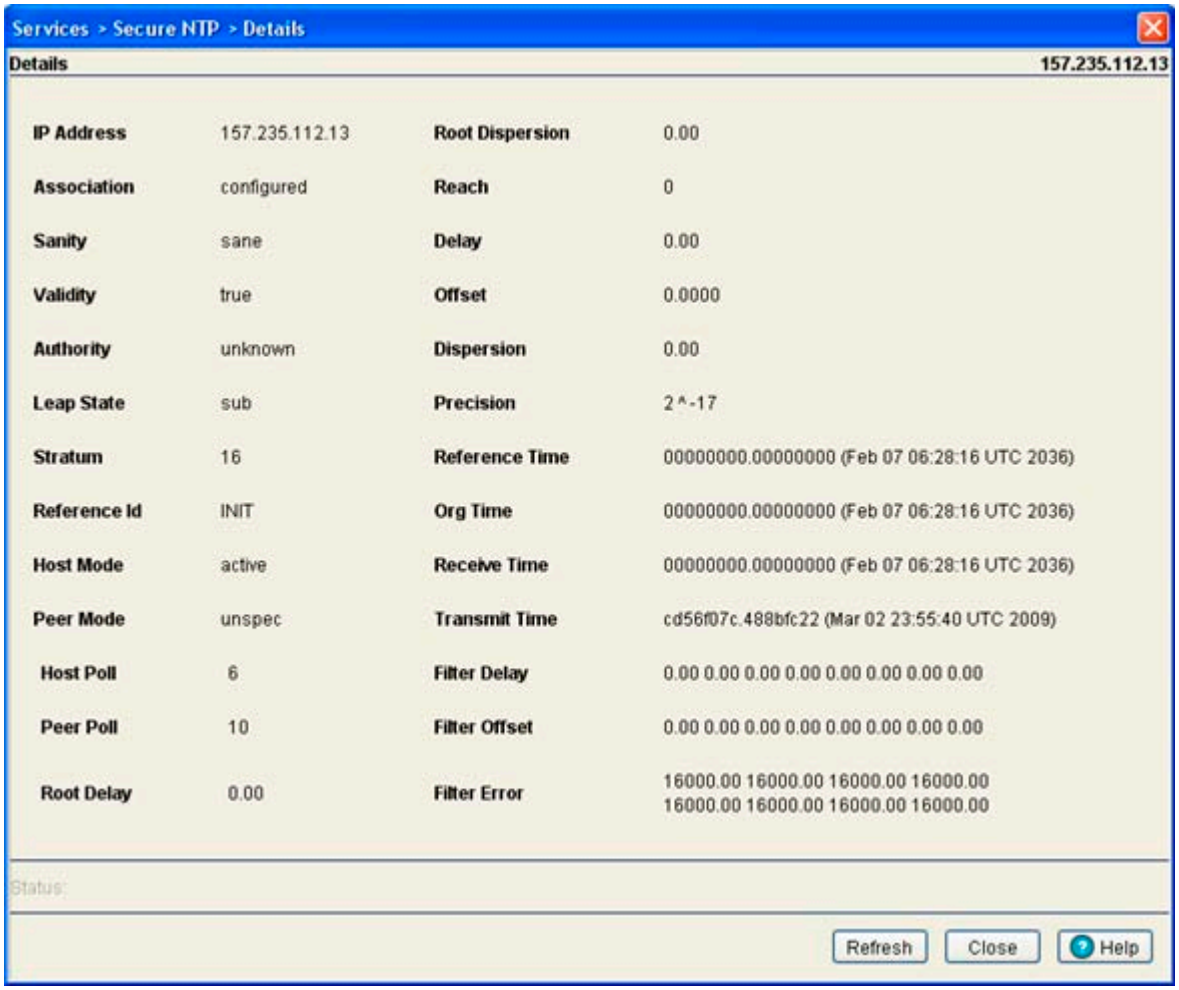


3. Refer to the following SNTP Association data for each SNTP association displayed:

Address	Displays the numeric IP address of the SNTP resource (Server) providing SNTP updates to the switch.
Reference Clock	Displays the address of the time source the switch is synchronized to.
Stratum	Displays how many hops the switch is from a SNTP time source. The switch automatically chooses the SNTP resource with the lowest stratum. The SNTP supported switch is careful to avoid synchronizing to a server that may not be accurate. Thus, the NTP enabled switch never synchronizes to a machine not synchronized itself. The SNTP enabled switch compares the time reported by several sources, and does not synchronize to a time source whose time is significantly different than others, even if its stratum is lower.
When	Displays the date and time when the SNTP association was initiated. Has the association been trouble free over that time?
Peer Poll	Displays the maximum interval between successive messages, in seconds to the nearest power of two.
Reach	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.

Delay (sec)	Displays the round-trip delay (in seconds) for SNTP broadcasts between the SNTP server and the switch.
Offset (sec)	Displays the calculated offset between the switch and SNTP server. The switch adjusts its clock to match the server's time value. The offset gravitates toward zero over time, but never completely reduces its offset to zero.
Dispersion (sec)	Displays how scattered the time offsets are (in seconds) from a SNTP time server

NOTE: Select an existing NTP association and click the **Details** button to display additional information useful in discerning whether the association should be maintained



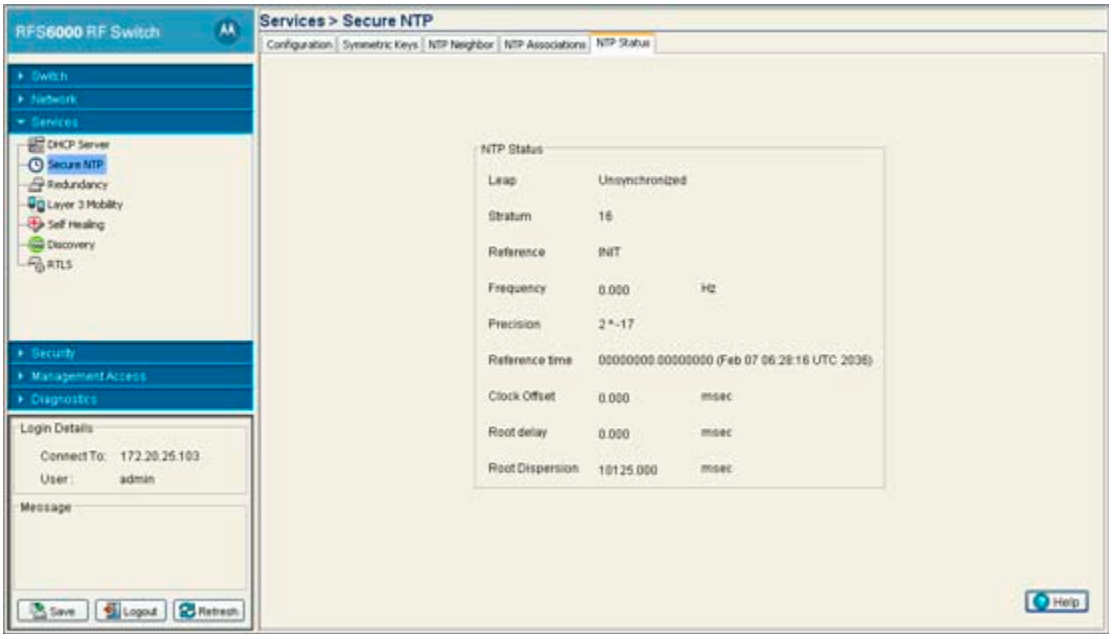
5.3.6 Viewing NTP Status

Refer to the **NTP Status** tab to display performance (status) information relative to the switch's current NTP association. Verifying the switch's SNTP status is important to assess which resource the switch is currently getting its system time from, as well as the time server's current differences in time attributes as compared to the current switch time.

CAUTION: After an NTP synchronization using a Symmetric Key, the NTP status will not automatically update.

To review the switch's current NTP associations:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **NTP Status** tab.



3. Refer to the **SNTP Status** field to review the accuracy and performance of the switch's ability to synchronize with a NTP server:

Leap	Indicates if a second will be added or subtracted to SNTP packet transmissions, or if the transmissions are synchronized.
Stratum	Displays how many hops the switch is from its current NTP time source.
Reference	Displays the address of the time source the switch is synchronized to.
Frequency	A SNTP server clock's skew (difference) for the switch
Precision	Displays the precision (accuracy) of the switch's time clock (in Hz). The values that normally appear in this field range from -6 for mains-frequency clocks to -20 for microsecond clocks found in some workstations.
Reference time	Displays the time stamp at which the local clock was last set or corrected.
Clock Offset	Displays the time differential between switch time and the NTP resource.

Root delay	The total round-trip delay in seconds. This variable can take on both positive and negative values, depending on the relative time and frequency offsets. The values that normally appear in this field range from negative values of a few milliseconds to positive values of several hundred milliseconds.
Root Dispersion	Displays the nominal error relative to the primary time source in seconds. The values that normally appear in this field range from 0 to several hundred milliseconds.

5.4 Configuring Switch Redundancy and Clustering

Configuration and network monitoring are two tasks a network administrator faces as a network grows in terms of the number of managed nodes (switches, routers, wireless devices etc.). Such scalability requirements lead network administrators to look for managing and monitoring each node from a single centralized management entity. The switch not only provides a centralized management solution, it provides centralized management from any single switch in the network without restricting or dedicating one switch as a centralized management node. This eliminates dedicating a management entity to manage all redundancy members and eliminates the possibility of a single point of failure.

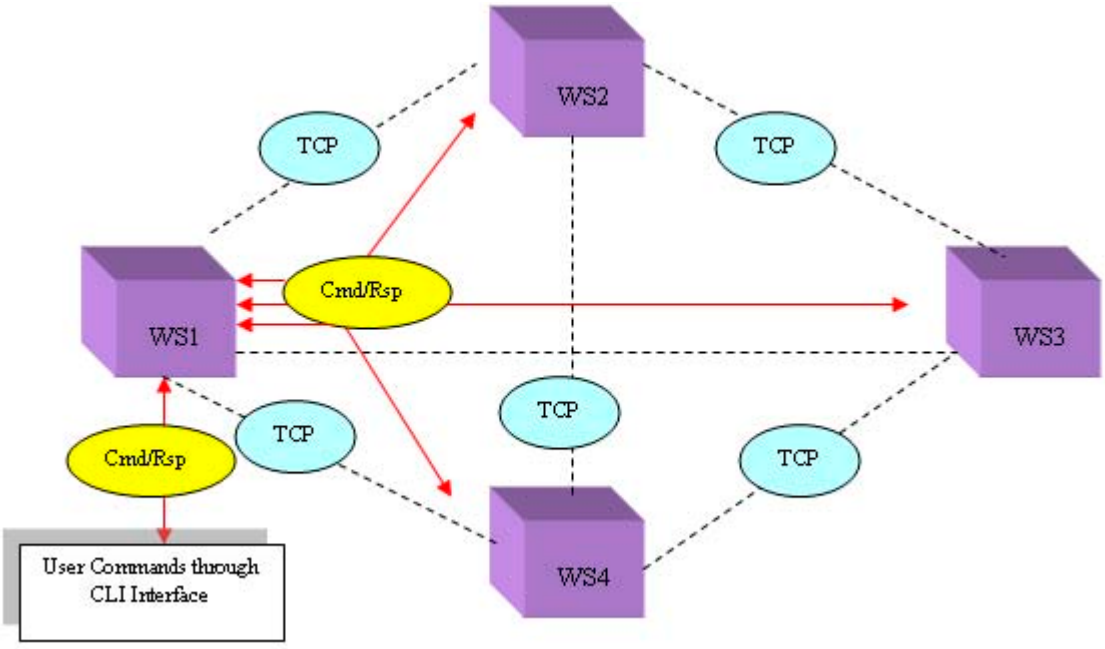
A redundancy group (cluster) is a set of switches (nodes) uniquely identified by group/cluster ID. Within the redundancy group, members discover and establish connections to other group members. The redundancy group has full mesh connectivity using TCP as the transport layer connection.

Up to 12 switches can be configured as members of a redundancy group to significantly reduce the chance of a disruption in service to WLANs and associated MUs in the event of failure of a switch or intermediate network failure. All members can be configured using a common file (cluster-config) using DHCP options. This functionality provides an alternative method for configuring members collectively from a centralized location, instead of configuring specific redundancy parameters on individual switches.

Configure each switch in the cluster by logging in to one participating switch. The administrator does not need to login to each redundancy group member, as one predicating switch can configure each member in real-time without “pushing” configurations between switches. A new CLI context called *cluster-cli* is available to set the configuration for all members of the cluster. All switch CLI commands are considered cluster configurable.

In the following example, there are four switches (WS1, WS2, WS3 and WS4) forming a redundancy group. Each switch has established a TCP connection with the others in the group. There is an additional CLI context called cluster-context. A user/administrator can get into this context by executing a *cluster-cli enable* under the CLI interface (future releases will have this support in the Web UI and SNMP interfaces). When the user executes this command on WS1, WS1 creates a virtual session with the other switches in the redundancy group (WS2, WS3 and WS4). Once the virtual session is created, any command executed on WS1 is executed

on the other switches at the same time. This is done by the cluster-protocol running on WS1, by duplicating the commands and sending them to the group over the virtual connection:



After sending the command to other members, the cluster-management protocol (at WS1) waits for a response from the members of the redundancy group. Upon receiving a response from each member, WS1 updates the user's screen and allows the user to enter/execute the next command.

The wait time required to collect responses from other switches is predefined, so if any one or more members does not respond to a given command within the defined interval, the command originating switch displays whatever responses have been collected and ignores the delayed responses. This time-based response mechanism eliminates the possibility of indefinite response hangs and allows for quicker redundancy group configuration.

There is no fixed master-slave relationship between members. Typically, a switch can be considered a master for the command it originates. Responding members can be considered slaves with respect to that command.

This virtual master-slave relationship makes this design unique when compared to existing centralized management systems. Having a virtual master-slave relationship eliminates a single point of failure, since a user can make use of any switch as the group centralized management entity (using the cluster-management context).

NOTE: When using the redundancy feature make sure that UDP traffic on port 51515 is open between the redundant switches.

To view status and membership data and define a redundancy group configuration, refer to the following:

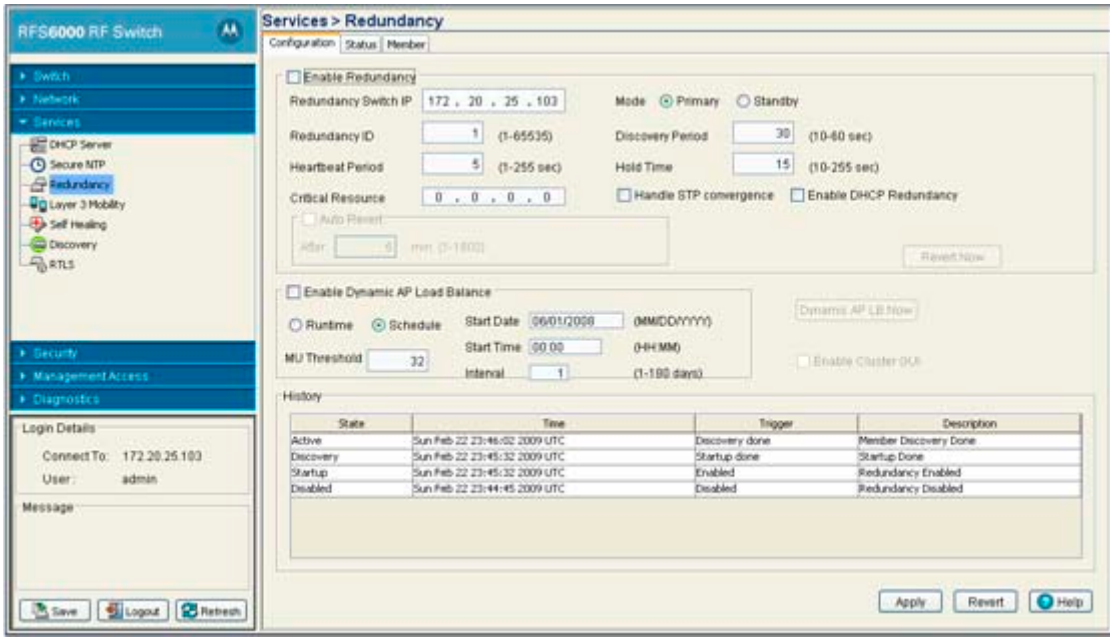
- *Configuring Redundancy Settings*
- *Reviewing Redundancy Status*
- *Configuring Redundancy Group Membership*
- *Redundancy Group License Aggregation Rules*
- *Managing Clustering Using the Web UI*

5.4.1 Configuring Redundancy Settings

To configure switch redundancy:

1. Select **Services** > **Redundancy** from the main menu tree.

   The Redundancy screen displays with the Configuration tab selected.



NOTE: MUs on an independent WLAN will not see any disruptions on a switch fail-over.

2. Refer to the **Configuration** field to define the following:

Enable Redundancy	Select this checkbox to enable/disable clustering. Clustering must be disabled to set a redundancy related parameter. All the modifiable values are grayed out if enabled
Redundancy Switch IP	Define the destination IP address used to send heartbeats and update messages.
Mode	A member can be in either in **Primary** or **Standby** mode. In the redundancy group, all 'Active' members adopt Access Ports except the 'Standby' members who adopt Access Ports only when an 'Active' member has failed or sees an access-port not adopted by a switch.
Redundancy ID	Define an ID for the cluster group. All the switches configured in the cluster should have the same Cluster ID. The valid range is 1-65535.
Discovery Period	Use the **Discovery Period** to configure a cluster member discovery interval. During the discovery time, a switch discovers the existence of other switches within the redundancy group. Configure an interval between 10 and 60 seconds. The default value is 30 seconds.

Heartbeat Period	The **Heartbeat Period** is the interval heartbeat messages are sent. Heartbeat messages discover the existence and status of other members within the group. Configure an interval between 1 and 255 seconds. The default value is 5seconds.
Hold Time	Define the **Hold Time** for a redundancy group. If there are no heartbeats received from a peer during the hold time, the peer is considered down. In general, the hold period is configured for three times the heartbeat period. Meaning, if three consecutive heartbeats are not received from the peer, the peer is assumed down and unreachable. The hold time is required to be longer than the heartbeat interval. Configure a hold time between 10 and 255 seconds. The default is 15 seconds.
Critical Resource	Enter the IP address of the critical resource. When the heartbeat is lost, this resource will be checked for reachability. The critical resource can be any gateway, server or host. If the critical resource is not reachable and the heartbeat is still lost, the switch will deadopt APs and continue to deadopt APs until instructed otherwise.
Handle STP convergence	Select the **Handle STP convergence** checkbox to enable *Spanning Tree Protocol* (STP) convergence for the switch. In general, this protocol is enabled in layer 2 networks to prevent network looping. If the network is enabled for STP to prevent looping, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance Access Ports at startup.
Enable DHCP Redundancy	Enables DHCP Redundancy for member switches. DHCP Redundancy allows an administrator to have only one DHCP server running at any time in a cluster. The clustering protocol enables all peers participating in DHCP redundancy to determine the active DHCP server among them. The switch with lowest Redundancy IP is selected as the active DHCP server for the cluster. This selected active DHCP server can be either a primary or standby switch. The other switches do not provide DHCP service as long as the selected DHCP server switch is active.
Auto Revert	Check this box to enable the **Auto Revert** feature and specify the time (in minutes) for the switch to revert. Configure the interval between 1 and 1800 minutes. The default revert time is 5 minutes. When a primary switch fails, the standby switch takes over APs adopted by the primary. If the auto revert feature is enabled, when the failed primary switch comes back up, the standby starts a timer based on the auto-revert interval. At the expiry of auto-revert interval (if the primary switch is still up), the standby switch releases all adopted APs and goes back to a monitoring mode. The expiry timer either will be stopped or restarted if the primary switch goes down and comes up during the auto-revert interval.
Revert Now	Reverts an active fail-over standby switch to a passive standby switch. When a user presses this button, the standby switch will un-adopt all its adopted APs and move into a standby (passive) mode only if all configured members are up again. The revert function does not push APs to the primary switch unless the primary switch has failed over.

NOTE: If the critical resource IP is defined, the resource needs to be checked for reach-ability whenever their is heartbeat lost or APs may lose adoption.

NOTE: Redundancy uses UDP port 51515 for both source and destination port. The TCP connection uses 51515 as the destination port, the source port is selected from the range of 32768 to 61000.

3. To enable **Dynamic AP Load Balancing,** check the **Enable Dynamic AP Load Balancing** option and define the parameters below:

Runtime/Schedule	Select Runtime or Schedule to determine when load balancing will run. If Runtime is selected, load balancing will initiate anytime a new active switch is added to the redundancy group. If Schedule is selected you can configure a start date and time to execute load balancing. This feature is not available when Dynamic Load Balancing is enabled.
Start Date	If Schedule is selected as the load balancing mode, enter a start date for load balancing to take place.
Start Time	If Schedule is selected as the load balancing mode, enter a start time for load balancing to take place.
MU Threshold	The MU threshold specifies the number of minimum number of active MUs on an AP to stop the AP from resetting for load balancing.
Interval	If Schedule is selected as the load balancing mode, enter an interval (in days) for how often load balancing should take place. The valid range is between 1 and 180 days.

4. Once Dynamic Load Balancing parameters are set, click the **Dynamic AP LB Now** button to run Dynamic AP Load Balancing.
5. Managing clustering in the Web UI is done through the **Cluster GUI** feature. Check the **Enable Cluster GUI** checkbox to enable this feature. The **Cluster GUI** feature updates many key screens in the Web UI allowing you to see APs and MUs managed by all active members of a cluster.
6. Refer to the **History** field to view the current state of the redundancy group.

State	Displays the new state (status) of the redundancy group after a Trigger event has occurred.
Time	Displays the Timestamp (time zone specific) when the state change occurred.
Trigger	Displays the event causing the redundancy group state change on the switch.
Description	Displays a redundancy event description defining the redundancy group state change on the switch. Typical states include Redundancy Disabled or Redundancy Enabled.

7. Click **Apply** to save any changes to the screen. Navigating away from the screen without clicking the Apply button results in all the changes on the screen being discarded.
8. Click the **Revert** button to undo the changes to the screen and revert to the last saved configuration.

5.4.2 Reviewing Redundancy Status

The switch is capable of displaying the status of the collective membership of the cluster. Use this information to assess the overall health and performance of the group.

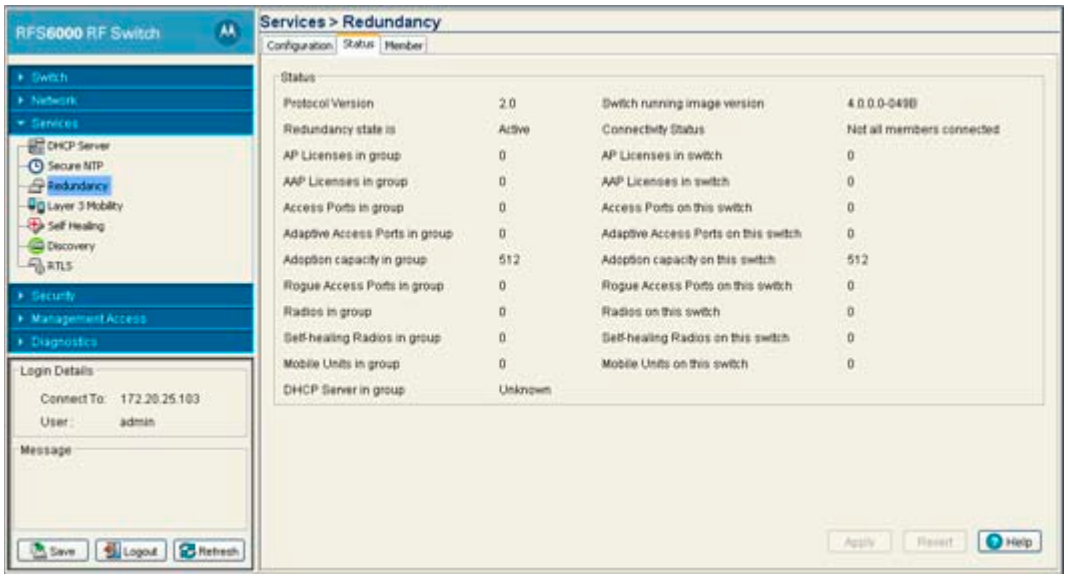
NOTE: When ETH2 of one of the group members is unplugged, the other members report that this member as gone, but an AP will continue to be adopted by the switch with no ETH2 connectivity.

To configure switch redundancy memberships:

1. Select **Services** > **Redundancy** from the main menu tree.

   The Redundancy screen displays with the Configuration tab selected.

2. Select the **Status** tab.



3. Refer to the **Status** field to assess the current state of the redundancy group.

Protocol Version — The Cluster Protocol should be set to an identical value for each switch in the redundancy group. The protocol version is one of the parameters used to determine whether two peers can form a group.

Redundancy state is — Displays the state of the redundancy group. When the redundancy feature is disabled, the state is "Disabled." When enabled, it goes to a "Startup" state. From "Startup" it goes to a "Discovery" state immediately if the STP convergence is not enabled. Otherwise, it remains in "Startup" for a period of 50 seconds (the standard STP convergence time). During the discover state, the switch exchanges heartbeats and update messages to discover other members and define the redundancy group license. After discerning memberships, it moves to an Active state. There is no difference in state execution for Primary and Standby modes.

AP Licenses in Group — Displays the number of Access Ports that can be adopted in the redundancy group. This value is calculated when a member starts-up, is added, is deleted or a license changes (downgrade and upgrade.) This value is equal to the highest license level of its members. It is NOT the sum of the license level of its members. For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-46*.

AAP Licenses	Displays the number of Adaptive APs that can be adopted in the redundancy group. This value is calculated when a member starts-up, is added, is deleted or a license changes (downgrade and upgrade.) This value is equal to the highest license level of its members. It is NOT the sum of the license level of its members. For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-46*
Access Ports in group	Displays the total of the number of Access Ports adopted by the entire membership of the redundancy group.
Adaptive Access Ports in Group	Displays the total of the number of Adaptive APs adopted by the entire membership of the redundancy group.
Adoption capacity in group	Displays the combined AP adoption capability for each switch radio comprising the cluster. Compare this value with the adoption capacity on this switch to determine if the cluster members have adequate adoption capabilities.
Rogue Access Ports in group	Displays the cumulative number of rogue APs detected by the members of the group. Compare this value with the number of rogues detected by this AP to discern whether an abundance of rogues has been located by a particular switch and thus escalates a security issue with a particular switch.
Radios in group	Displays the combined number (sum) of radios a amongst all the members of the redundancy group.
Self-healing radios in group	Displays the number of radios within the cluster that have self-healing capabilities enabled. Compare this value with the total number of radios within the group to determine how effectively the radios within the cluster can self-heal if problems exist.
Mobile Units in group	Displays the combined number of MU associations for the members of the redundancy group. Compare this number with the number of MUs on this switch to determine how effectively MU associations are distributed within the cluster.
DHCP Server in Group	Displays the total number of DHCP Servers available for DHCP resources for the combined cluster membership.
Switch running image version	Displays the switch firmware image version currently running on the switch. Compare this version with the latest version available from Motorola to ensure the switch supports the latest feature set available.
Connectivity Status	Displays the current connectivity status of the cluster membership.
AP Licenses in switch	Displays the total number of Access Port device adoption licenses available to this switch.
AAP Licenses in switch	Displays the total number of Adaptive Access Port device adoption licenses available to this switch.
Access Ports on this switch	Displays the total of the number of Access Ports adopted by this switch.
Adaptive Access Ports on this switch	Displays the total of the number of Adaptive Access Ports adopted by this switch.

Adoption capacity on this switch	Displays the AP adoption capability for this switch. Compare this value with the adoption capacity for the entire cluster to determine if the cluster members (or this switch) have adequate adoption capabilities. For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-46*.
Rogue Access Ports on this switch	Displays the number of rogue APs detected by this switch. Compare this value with the cumulative number of rogues detected by the group to discern whether an abundance of rogues has been located by a particular switch and thus escalates a security issue.
Radios on this switch	Displays the number of radios used with this switch.
Self-healing radios on this switch	Displays the number of radios on this switch with self-healing enabled. Compare this value with the total number of radios within the group to determine how effectively radios can self-heal if problems exist.
Mobile Units on this switch	Displays the number of MUs currently associated with the radio(s) used with this switch. Compare this number with the number of MUs within the group to determine how effectively MUs are distributed within the cluster.

4. The **Apply** and **Revert** buttons are unavailable for use with the Status screen, as there are no editable parameters to save or revert.

5.4.3 Configuring Redundancy Group Membership

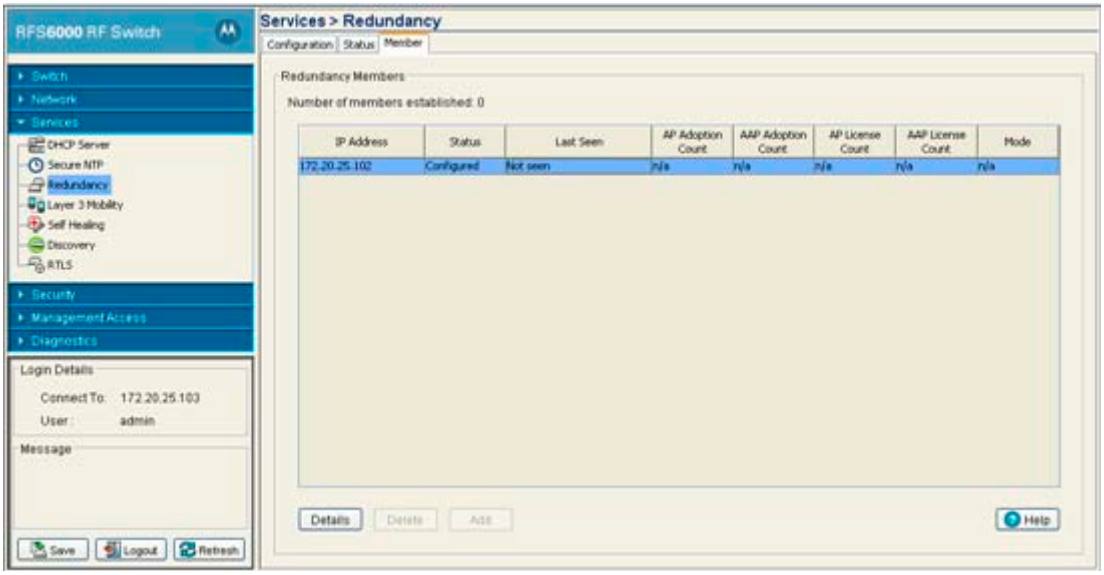
The redundancy group should be disabled to conduct an Add/Delete operation. There are a minimum of 2 members needed to comprise a Redundancy Group, including the initiating switch

To configure switch redundancy memberships:

1. Select **Services** > **Redundancy** from the main menu tree.

   The Redundancy screen displays with the Configuration tab selected.

2. Select the **Member** tab.



3. Refer to the following information within the Member tab:

IP Address	Displays the IP addresses of the redundancy group member.
Status	Displays the current status of this group member. This status could have the following values: • *Configured* - The member is configured on the current wireless service module. • *Seen* - Heartbeats can be exchanged between the current switch and this member. • *Invalid* - Critical redundancy configuration parameter(s) of the peer (heartbeat time, discovery time, hold time, Redundancy ID, Redundancy Protocol version of this member) do not match this switch's parameters. • *Not Seen* - The member is no more seen by this switch. • *Established* - The member is fully established with this current module and licensing information already been exchanged between this switch and the member. • *Unknown* - No status information could be obtained.
Last Seen	Displays the time when this member was last seen by the switch.
AP Adoption Count	Displays the number of Access Ports adopted by this member.
AAP Adoption Count	Displays the number of Adaptive APs adopted by this member.

AP License Count	Displays the number of Access Port licenses installed on this member.
AAP License Count	Displays the number of Adaptive AP licenses installed on this member.
Mode	The Redundancy Mode could be Active or Standby depending on the mode configuration on the member. Refer to the Configuration screen to change the mode.

4. Select a row, and click the **Details** button to display additional details for this member. For more information, see *Displaying Redundancy Member Details on page 5-43*.
5. Select a row and click the **Delete** button to remove a member from the redundancy group. The redundancy group should be disabled to conduct an Add or Delete operation.
6. Click the **Add** button to add a member to the redundancy group. The redundancy group should be disabled to conduct an Add or Delete operation. For more information, see *Adding a Redundancy Group Member on page 5-45*.

5.4.3.1 Displaying Redundancy Member Details

Use the **Details** screen (in conjunction with its parent Member screen) to display additional (more detailed) information on the group member selected within the Member screen.

To review the details

1. Select **Services** > **Redundancy** from the main menu tree.

   The Redundancy screen displays with the Configuration tab selected.
2. Select the **Member** tab.
3. Highlight a member of the group and select the **Details** button.

4. Refer to the following redundancy member information:

IP Address	Displays the IP addresses of the members of the redundancy group. There are a minimum of 2 members needed to define a redundancy group, including this current module.
Status	Displays the current status of this group member. This status could have the following values: • *Configured* - The member is configured on the current wireless service module. • *Seen* - Heartbeats can be exchanged between the current switch and this member. • *Invalid* - Critical redundancy configuration parameter(s) of the peer (heartbeat time, discovery time, hold time, Redundancy ID, Redundancy Protocol version of this member) do not match this switch's parameters. • *Not Seen* - The member is no more seen by this switch. • *Established* - The member is fully established with this current module and licensing information already been exchanged between this switch and the member.
AP Adoption Count	Displays the number of Access Ports adopted by this member.
AAP Adoption Count	Displays the number of Adaptive Access Ports adopted by this member.
Adoption Capacity	Displays the maximum number of Access Ports this member is licensed to adopt. For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-46*.
AP License Count	Displays the number of Access Port licenses available for this switch. For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-46*.
AAP License Count	Displays the number of Adaptive Access Port licenses available for this switch. For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-46*.
Image Version	Displays the image version currently running on this member. Is the selected version complimentary with this switch's version?
First Seen	Displays the time this member was first seen by the switch.
Last Seen	Displays the time this member was last seen by the switch.
Mode	The Redundancy Mode could be Active or Standby depending on the mode configuration on the member. Refer to the Configuration screen to change the mode
HB Sent	Displays the number of heartbeats sent from the switch to this member since the last reboot of the switch.
HB Received	Displays the number of heartbeats received by the switch since the last reboot.
Updates Sent	Displays the number of updates sent from the switch since the last reboot. Updates include, authorization level, group authorization level and number of Access Ports adopted.

Updates Received	Displays the number of updates received by the current switch from this member since the last reboot.
Radio Portals	Displays the number of radio portals detected on each redundancy member listed.
Associated MUs	Display the number of MUs associated with each member listed.
Rogue APs	Displays the number of Rogue APs detected by each member. Use this information to discern whether these radios represent legitimate threats to other members of the redundancy group.
Self Healing Radios	Displays the number of self healing radios on each detected member. These radios can be invaluable if other radios within the redundancy group were to experience problems requiring healing by another radio.

5. Refer to the **Status** field.

   The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.

6. Click **Close** to close the dialog without committing updates to the running configuration.

5.4.3.2 Adding a Redundancy Group Member

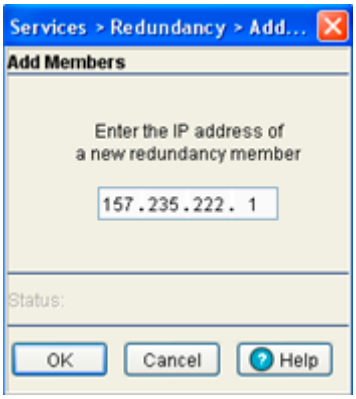
Use the **Add** screen as the means to add a new member (by adding their IP address) to an existing redundancy group (cluster).

To add a new member to a redundancy group:

1. Select **Services** > **Redundancy** from the main menu tree.

   The **Redundancy** screen displays with the **Configuration** tab selected.

2. Select the **Member** tab.
3. Select the **Add** button.



4. Enter the IP Address of a new member.
5. Click **OK** to save and add the changes to the running configuration and close the dialog.
6. Refer to the **Status** field.

   The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.

7. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.4.4 Redundancy Group License Aggregation Rules

The following are rules governing license usage amongst members of a redundancy group:

- A redundancy group license is determined by adding individual switch licenses.
- Do not allow different port speed/duplex settings on members. Each members should have the settings.
- In a redundancy group of three switches (S1, S2 and S3), if S1 has X licenses, S2 has Y licenses and S3 has Z licenses, the license count is X+Y+Z (the aggregation of each switch).
- A cluster license is re-calculated whenever a new switch brings existing licenses to a group or an existing switch's license value changes (increases or decreases).
- A simple switch reboot will not initiate a new cluster license calculation, provided the re-booted switch does not come up with different installed license.
- A change to an installed license during runtime initiates a cluster license calculation.
- If an existing redundancy group member goes down, it will not initiate a cluster license calculation.
- Whenever the cluster protocol is disabled, a member switch forgets the learned cluster license as well as peer information needed to compute license totals.
- If the switch start-up configuration is removed, a member switch forgets the learned cluster license as well as peer information needed to compute license totals.
- If adding a new switch (with zero or non-zero installed license) to a group with at least one license contributing switch down, the new group member will receive a different cluster license value.

  For example, for a cluster of three switches (S1 = 6, S2 = 6 and S3 = 6 licenses), the group license count is 18. If S1 goes down, the license count is still 18, since the license calculation is not initiated if a member switch goes down. If S4 (with zero licenses) is introduced, S4 becomes part of the group (can exchange updates and other packets), but has license count of 12 (NOT 18), even though S2 and S3 still show a license count of 18. This should be an indicator a new member has been introduced during a period when the redundancy group is not operating with all its license contributing members.

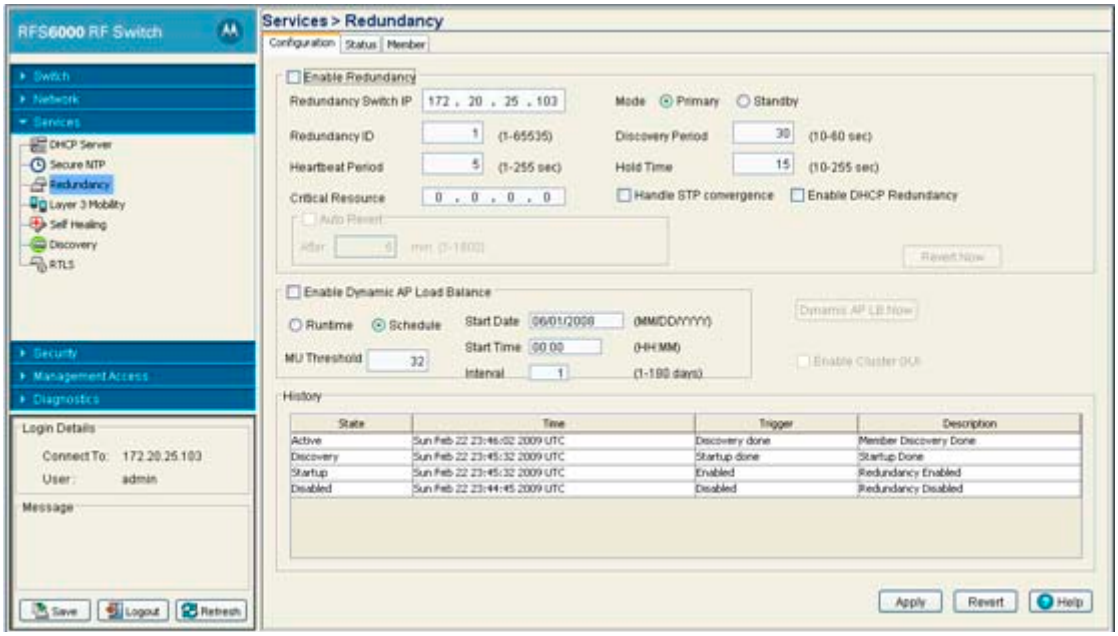
5.4.5 Managing Clustering Using the Web UI

Managing clustering in the Web UI is done through the **Cluster GUI** feature. The Cluster GUI feature updates many key screens in the Web UI allowing you to see APs and MUs managed by all active members of a cluster.

To enable the Cluster GUI feature:

1. Select **Services** > **Redundancy** from the main menu tree

   The **Redundancy** screen displays with the **Configuration** tab selected.



2. Configure redundancy settings using the Command Line Interface or the using the Web UI as described in *Configuring Redundancy Settings on page 5-36*.
3. Add any redundancy group members using the Command Line Interface or using the Web UI as described in *Configuring Redundancy Group Membership on page 5-42*.
4. On the **Configuration** tab, check the Enable Redundancy checkbox and then check the **Enable Cluster GUI** box.
5. Click the **Apply** button to enable the **Cluster GUI** feature.
6. Once **Cluster GUI** is enabled a **Switch** field will be available in many of the Access Port and mobile unit related screens. The **Switch** field is displays which cluster members the APs and MUs are associated with identified by their IP address.

NOTE: When accessing the switch Web UI through a NATed interface the **Cluster GUI** features will only be accessible if TCP ports 80 and 161 are opened on the router or gateway.

5.5 Layer 3 Mobility

Refer to the following sections to configure Layer 3 Mobility:

- *Configuring Layer 3 Mobility*
- *Defining the Layer 3 Peer List*
- *Reviewing Layer 3 Peer List Statistics*
- *Reviewing Layer 3 MU Status*

5.5.1 Configuring Layer 3 Mobility

Layer 3 mobility is a mechanism enabling a MU to maintain the same Layer 3 address while roaming throughout a multi-VLAN network. This enables transparent routing of IP datagrams to MUs during their movement, so data sessions can be maintained while they roam (in for voice applications in particular). Layer 3 mobility maintains TCP/UDP sessions in spite of roaming among different IP subnets.

A mobility domain comprises of a network of switches among which an MU can roam seamlessly without changing its IP address. Each switch in the mobility domain needs a mobility domain string identifier so MUs roaming between switches can retain their Layer 3 address and maintain application-layer connectivity.

When a MU enters a mobility domain (by associating with a switch), it is first assigned a home switch. The home switch is responsible for assigning a VLAN for the MU and communicating the MU's mobility-related parameters to the other switches in the mobility domain. The home switch does not change for the remainder of the MU's presence in the mobility domain. All data packets transmitted/received by the MU including DHCP and ARP are tunneled through the home switch. The IP address for the MU is assigned from the VLAN to which the MU belongs (as determined by the home switch).

The current switch is the switch in the mobility domain an MU is currently associated to. The current switch changes as the MU roams and establishes different associations. The current switch is responsible for delivering data packets from the MU to its home switch and vice-versa.

CAUTION: An Access Port is required to have a DHCP provided IP address before attempting layer 3 adoption, otherwise it will not work. Additionally, the Access Port must be able to find the IP addresses of the switches on the network.

To locate switch IP addresses on the network:

- Configure DHCP option 189 to specify each switch IP address.
- Configure a DNS Server to resolve an existing name into the IP of the switch. The Access Port has to get DNS server information as part of its DHCP information. The default DNS name requested by an AP300 is “Symbol-CAPWAP-Address”. However, since the default name is configurable, it can be set as a factory default to whatever value is needed.

Key aspects of Layer 3 Mobility include:

- Seamless MU roaming between switches on different Layer 3 subnets, while retaining the same IP address.
- Static configuration of mobility peer switches.
- Layer 3 support does not require any changes to the MU. In comparison, other solutions require special functionality and software on the MU. This creates numerous inter-working problems with working with MUs from different legacy devices which do not support Layer 2 switching.
- Support for a maximum of 20 peers, each handling up to a maximum of 500 MUs.

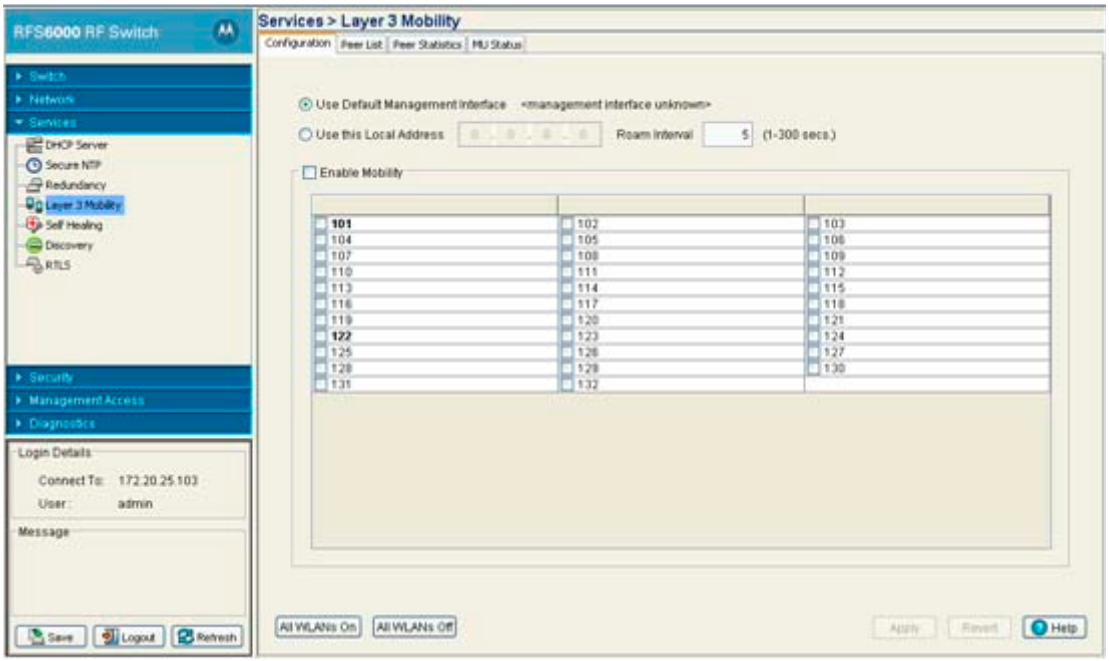
- A full mesh of GRE tunnels can be established between mobility peers. Each tunnel is between a pair of switches and can handle data traffic for all MUs (for all VLANs) associated directly or indirectly with the MU.
- Data traffic for roamed MUs is tunneled between switches by encapsulating the entire Layer 2 packet inside GRE with a proprietary code-point.
- When MUs roam within the same VLAN (Layer 2 Roaming), the behavior is retained by re-homing the MU to the new switch so extra hops are avoided while forwarding data traffic.
- MUs can be assigned IP addresses statically or dynamically.
- Forward and reverse data paths for traffic originating from and destined to MUs that have roamed from one Layer 3 subnet to another are symmetric.

NOTE: When using Layer 3 Mobility ensure that TCP traffic on port 58788 is allowed on the network(s) where mobile units will be roaming from and to.

To configure Layer 3 Mobility for the switch:

1. Select **Services** > **Layer 3 Mobility** from the main menu tree.

   The **Layer 3 Mobility** screen appears with the **Configuration** tab displayed.



2. Select the **Use Default Management Interface** checkbox to use the switch's default management interface IP address for MUs roaming amongst different Layer 3 subnets. The IP address displayed to the right of the checkbox is used by Layer 3 MU traffic.
3. If wanting to use a local IP addresses (non switch management interface) for MUs roaming amongst different Layer 3 subnets, select the **Use this Local Address** checkbox and enter an IP address.
4. Use the **Roam Interval** to define maximum length of time MUs within selected WLAN are allowed to roam amongst different subnets.

5. Refer to the table of WLANs and select the checkboxes of those WLANs you wish to enable Layer 3 mobility for.

   Once the settings are applied, MUs within these WLANs can roam amongst different subnets.

6. Select the **Enable Mobility** checkbox to enable a MU to maintain the same Layer 3 address while roaming throughout a multi-VLAN network.
7. Select the **All WLANs On** button to enable mobility for each WLAN listed.

   If unsure if you want to enable mobility for each WLAN, manually select just those you want to enable.

8. Select the **All WLANs Off** button to disable mobility for each WLAN listed.
9. Click the **Apply** button to save the changes made within this screen. Clicking Apply overwrites the previous configuration.
10. Click the **Revert** button to disregard any changes made within this screen and revert back to the last saved configuration.

5.5.2 Defining the Layer 3 Peer List

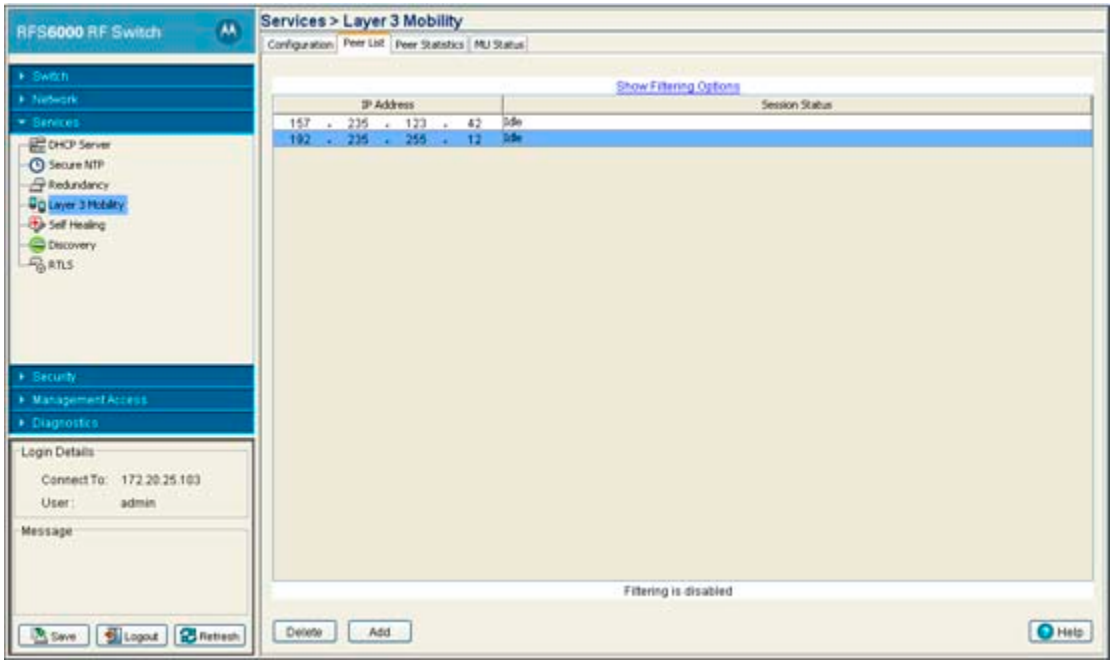
The Layer 3 Peer List contains the IP addresses MUs are using to roam amongst various subnets. This screen is helpful in displaying the IP addresses available to those MUs requiring access to different subnet resources.

To define the Layer 3 Peer List:

1. Select **Services** > **Layer 3 Mobility** from the main menu tree.

   The **Layer 3 Mobility** screen appears with the Configuration tab displayed.

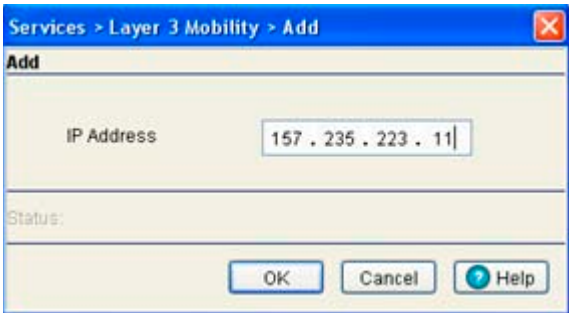
2. Select the **Peer List** tab.



3. Refer to the contents of the Peer List for existing IP addresses and Layer 3 MU session status.

   Use this information to determine whether a new IP address needs to be added to the list or an existing address needs to be removed.

4. Select an IP address from those displayed and click the **Delete** button to remove the address from the list available for MU Layer 3 roaming amongst subnets.
5. Click the **Add** button to display a screen used for adding the IP address to the list of addresses available for MU Layer 3 roaming.



Enter the IP addresses in the area provided and click the **OK** button to add the addresses to the list displayed within the **Peer List** screen.

5.5.3 Reviewing Layer 3 Peer List Statistics

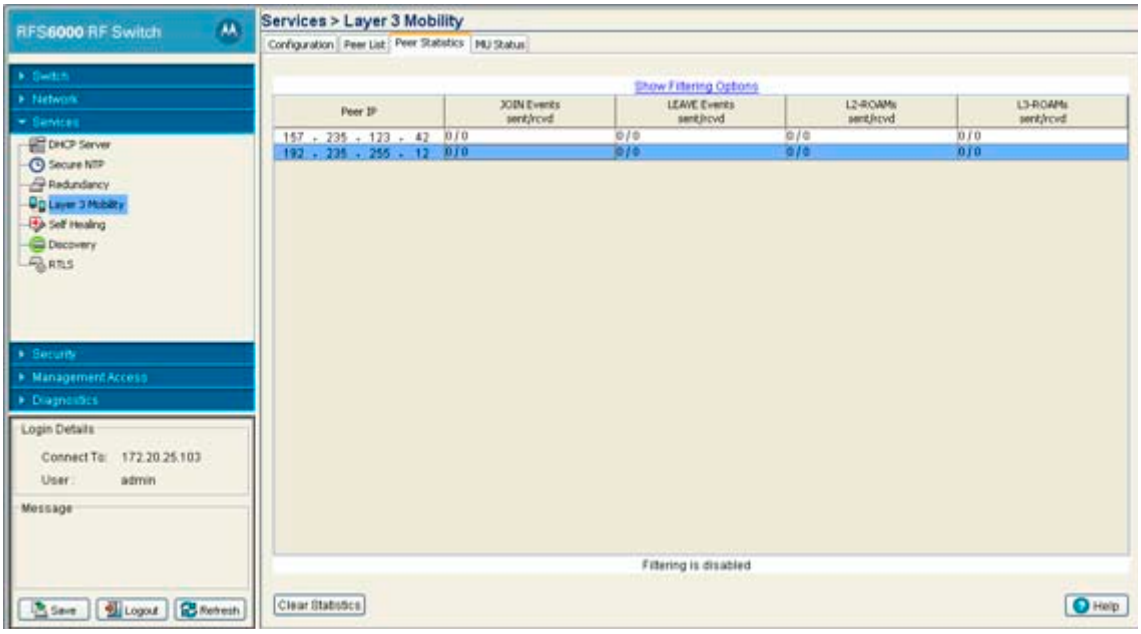
When a MU roams to a current switch on the same layer 3 network, it sends a L2-ROAM message to the home switch to indicate the MU has roamed within the same VLAN. The old home switch forwards the information to all its peers. The MU is basically re-synchronized to the new current switch, but keeps its old IP address. The same procedure is followed, even if the new current switch is on a different layer 3 subnet, but uses the same VLAN ID (overlapping VLAN scenario).

Tracking these message counts is important to gauge the behavior within the mobility domain.The Layer 3 Mobility screen contains a tab dedicated to tracking the message sent between the current switch, home switch and MU.

To view layer 3 peer statistics

1. Select **Services** > **Layer 3 Mobility** from the main menu tree.

   The **Layer 3 Mobility** screen appears with the Configuration tab displayed.
2. Select the **Peer Statistics** tab.



3. Refer to the following information within the Peer Statistics tab:

Peer IP	Displays the IP addresses of the peer switches within the mobility domain. Each peer can support up to 500 MUs.
JOIN Events sent/rcvd	Displays the number of JOIN messages sent and received. JOIN messages advertise the presence of MUs entering the mobility domain for the first time. When a MU (currently not present in the MU database) associates with a switch, it immediately sends a JOIN message to the host switch with MAC, VLAN and IP information (both current and home switch IP info). The home switch forwards the JOIN to all its peers (except the one from which it received the original message). JOIN messages are always originated by the current switch. JOIN messages are also used during the home switch selection phase to inform a candidate home switch about a MU. The current switch selects the home switch (based on its local selection mechanism) and sends a JOIN message to the home switch that is forwarded it to all its peers.
LEAVE Events sent/rcvd	Displays the number of LEAVE messages sent and received. LEAVE messages are sent when the switch decides a MU originally present in the MU database is no longer present in the mobility domain. The criterion to determine the MU has actually left the network is implementation specific. The current switch sends the LEAVE message with the MU's MAC address information to the home switch, which eventually forwards the message to each mobility peer.

L2-ROAMs sent/rcvd	Displays the number of Layer 2 ROAM messages sent and received. When a MU roams to a new switch on a different layer 3 network (MU is mapped to a different VLAN ID), it sends a L3-ROAM message to the home switch with the new IP information for the current switch it is associated with. The L3-ROAM message is then forwarded by the home switch to each peer.
L3-ROAMs sent/rcvd	Displays the number of Layer 3 ROAM messages sent and received. When a MU roams to a new current switch (on the same layer 3 subnet as the old current switch), it sends a L2-ROAM message to the old home switch with the new home switch-IP and current switch-IP information. This L2-ROAM message is then forwarded by the old home switch to each peer.

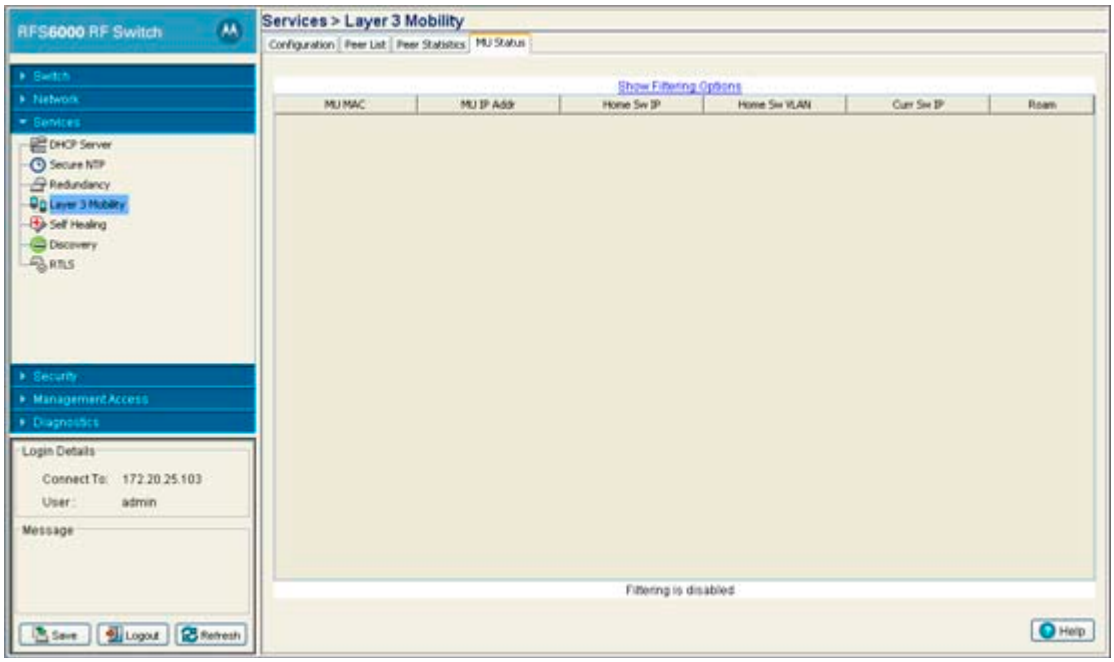
4. Click the **Clear Statistics** button to remove the data displayed for the selected peer IP address.

5.5.4 Reviewing Layer 3 MU Status

The Layer 3 Mobility **MU Status** tab displays a set of MU stats for associated MUs within the mobility domain. Use the MU status information to familiarize yourself with these MUs and their mobility-related parameters to distinguish new MUs entering the network from existing MUs roaming within the mobility domain.

To view Layer 3 mobility MU statistics

1. Select **Services** > **Layer 3 Mobility** from the main menu tree.
2. Select the **MU Status** tab.



5.6 Configuring Self Healing

The switch supports a feature called *Self Healing* that enables radios to take corrective action when one or more radios fail. To enable the feature the user must specify radio neighbors that would self heal if either

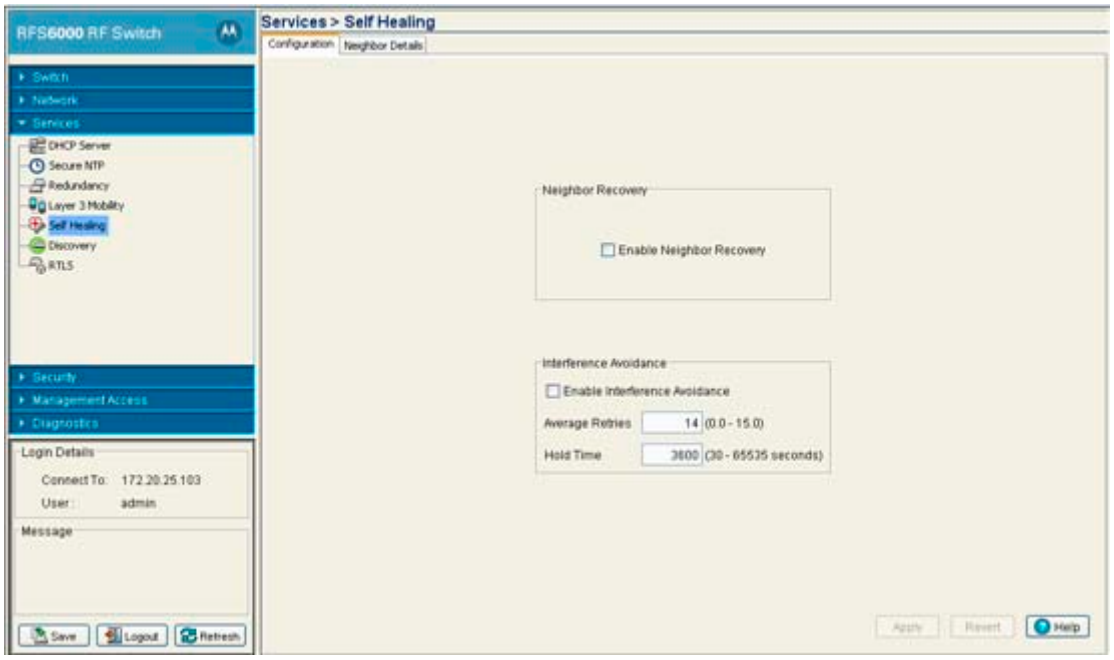
one goes down. The neighbor radios do not have to be of the same type. Therefore, an 11bg radio can be the neighbor of a 11a radio and either of them can self heal when one of them fails.

The switch initiates self healing when it looses communication with the Access Port or when another radio (configured in detector mode) informs the switch a particular radio is not transmitting beacons.

To configure self-healing on the switch:

1. Select **Services** > **Self Healing** from the main menu tree.

   The Self Healing page launches with the **Configuration** tab displayed.



2. Select the **Enable Neighbor Recovery** checkbox.

   Enabling Neighbor Recovery is required to conduct manual neighbor detection.

3. Refer to the **Interference Avoidance** field to define the following settings:

Enable Interference Avoidance	When enabled, the switch is capable of switching channels on an Access Port (*Automatic Channel Selection*) if interference is observed on the current operating channel.
Average Retries	Displays the average number of retries for a MU to communicate with a neighbor radio. Define a retry value between 0.0 and 15.0 retry attempts. Average Retries is a threshold value, when exceeded ACS is initiated. The default is 14.
Hold Time	Set the interval (in seconds) that disables interference avoidance after detection. The hold time prevents the radio from re-running ACS continuously. The default is 3600.

4. Click the **Apply** button to save the changes made within this screen. Clicking Apply overwrites the previous configuration.
5. Click the **Revert** button to disregard any changes made within this screen and revert back to the last saved configuration.

5.6.1 Configuring Self Healing Neighbor Details

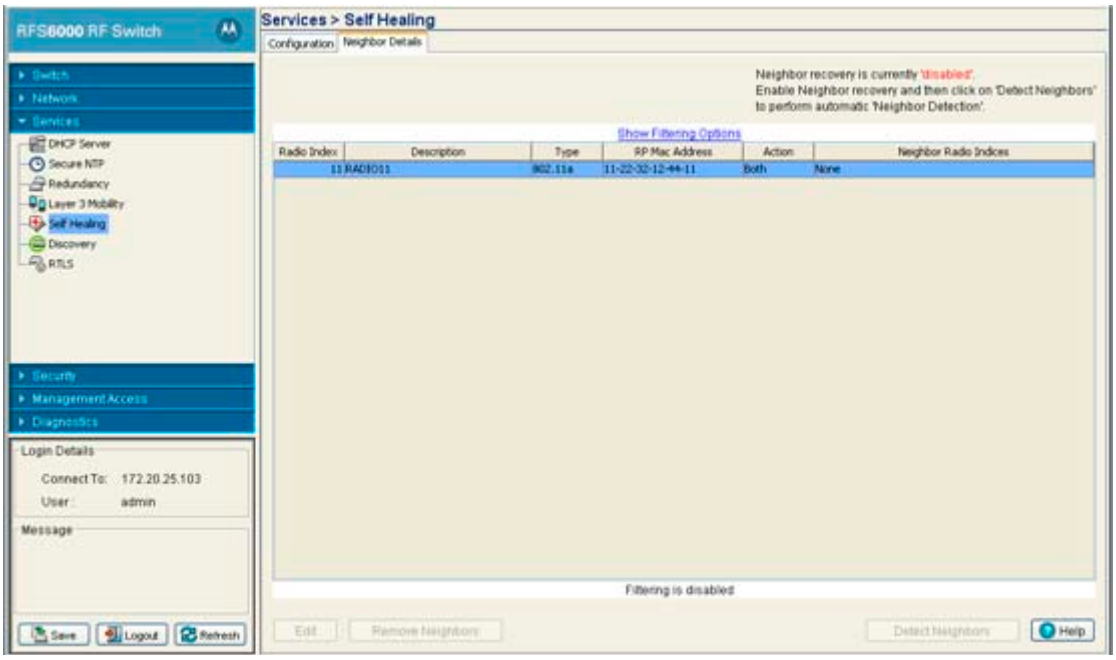
The Neighbor Details page displays all the radios configured on the switch and their neighbor designations.

To configure self-healing on the switch:

1. Select **Services** > **Self Healing** from the main menu tree.

   The Self Healing page launches with the **Configuration** tab displayed.

2. Select the **Neighbor Details** tab.



   The top right-hand corner displays whether neighbor recovery is currently enabled or disabled. To change the state, click the **Enable Neighbor Recovery** checkbox within the Configuration tab.

3. Refer to the following information as displayed within the Neighbor Recovery screen.

Radio Index	Displays a numerical identifier used (in conjunction with the radio's name) to differentiate the radio from its peers.
Description	Displays a text description used (in conjunction with the radio's index) to differentiate the radio from its peers.
Type	Displays the radio as either a 802.11a or 802.11bg radio.
RP Mac Address	Displays the Ethernet MAC address of the Access Port. Use the Access Port MAC Address for the addition or deletion of the radio.

Action	Displays the self healing action configured for the radio. Options include: • *Raise Power* - The transmit power of the radio is increased when a neighbor radio is not functioning as expected. • *Open Rates* - Radio rates are decreased to support all rates when a neighbor radio is not functioning as expected. • *Both* - Increases power and increases rates when a neighbor radio is not functioning as expected. • *None* - No action is taken when a neighbor radio is not functioning as expected.
Neighbor Radio Index	Displays the indexes of the radio's neighbors.

4. Highlight an existing neighbor and click the **Edit** button to launch a screen designed to modify the self healing action and/or neighbors for the radio. For more information, see *Editing the Properties of a Neighbor on page 5-56*.
5. Select the **Remove Neighbors** button to remove all neighbors from the selected radio's neighbor list.
6. Click the **Detect Neighbors** button to auto-determine neighbors for the radios.

NOTE: The **Detect Neighbors** button is enabled only when the **Enable Neighbor Recovery** checkbox is selected from within the Configuration tab. Ensure this option has been enabled before trying to detect neighbors.

Enabling this feature automatically makes each radio disassociate with their attached MUs, clear the current neighbor list and move into detection mode to detect neighboring radios.

Neighbor detection works best if all radios are configured and adopted. Starting the automatic neighbor detection feature disassociates MUs and clears the current neighbor configuration.

5.6.1.1 Editing the Properties of a Neighbor

Use the **Edit** screen to specify the neighbor of a selected radio and the action the radio performs in the event its neighbor radio fails.

To edit the properties of a neighbor:

1. Select **Services** > **Self Healing** from the main menu tree.
2. Select the **Neighbor Details** tab.
3. Select an existing neighbor and click the **Edit** button.

   The radio index and description display in the upper right corner of the screen. The **Available Radios** value represents the radios that can be added as a neighbor for the target radio. **Neighbor Radios** are existing radios (neighbors).
4. Select one of the following four actions from the Self Healing Action drop-down menu:
   - *None* - The radio takes no action at all when its neighbor radio fails.
   - *Open Rates* - The radio will default to factory-default rates when its neighbor radio fails.
   - *Raise Power* - The radio raises its transmit power to the maximum provided its power is lower than the maximum permissible value.
   - *Both* - The radio will open its rates as well as raise its power.
5. Click the **Add ->** button to move a radio from the Available Radios list to the Neighbor Radios list. This dedicates neighbors for this radio.

6. Select a radio and click **<- Remove** to move the radio from the Neighbor Radios list to the Available Radios list.
7. Refer to the **Status** field for an update of the edit process.

   The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to save the changes to the running configuration and close the dialog.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.7 Configuring Switch Discovery

Switch discovery enables the SNMP discovery (location) of devices. To discover devices in the specified range of IP addresses, the switch Web UI sends SNMP GET requests (using the user specified SNMP v2 or v 3 version) to all IP addresses on the specified network. The results of the discovery are helpful for isolating devices compatible for operation with the locating switch, thus extending the potential coverage area and MU support base within the switch managed network.

Use the **Discovery Profiles** tab to view existing SNMP search profiles using a user defined range of IP addresses. Existing profiles can be modified or deleted and new profiles can be added as needed. Refer to the **Recently Found Devices** tab to view a table of devices discovered by the current discovery process. Each discovered device compatible with the locating switch is displayed in a shaded color to distinguish it from non-compatible devices.

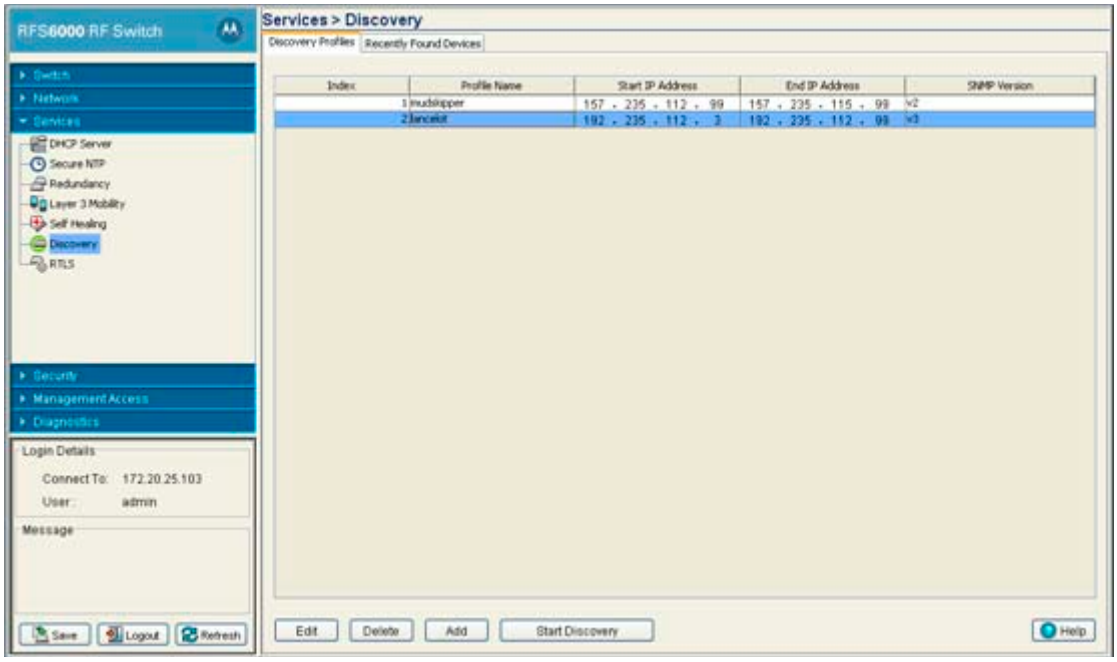
CAUTION: Switch discovery can be a time consuming operation. However, the switch discovery operation is a standalone process. This allows users to perform other configuration operations when discovery is running in the background.

5.7.1 Configuring Discovery Profiles

To configure switch discovery:

1. Select **Services** > **Discovery** from the main menu tree.

   The **Discovery** page launches with the **Discovery Profiles** tab displayed



2. Refer to the following information within the Discovery Profiles tab to discern whether an existing profile can be used as is, requires modification (or deletion) or if a new discovery profile is required.

Index	Displays the numerical identifier used to differentiate this profile from others with similar configurations. The index is supplied to new profiles sequentially.
Profile Name	Displays the user-assigned name for the profile. The profile name should associate the profile with the group of devices or area where the discovered devices are anticipated to be located.
Start IP Address	Displays the starting numeric (non DNS) IP address from where the search for available network devices is conducted.
End IP Address	Displays the ending numeric (non DNS) IP address from where the search for available network devices is conducted.
SNMP Version	Displays the version of the SNMP (either SNMP v2 or v3) used for discovering available network devices.

3. Select an existing profile and click the **Edit** button to modify the profile name starting and ending IP address and SNMP version. Motorola recommends editing a profile only if some of its attributes are still valid, if the profile is obsolete, delete it and create a new one.
4. Select an existing profile and click the **Delete** button to remove this profile from the list of available profiles.
5. Click the **Add** button to display a screen used to define a new switch discovery profile. For more information, see *Adding a New Discovery Profile on page 5-59*.
6. Click the **Start Discovery** button to display a **Read Community String** (SNMP v2) or V3 **Authentication** (SNMP v3) screen.

   compromise switch security. Therefore, when Start Discovery is selected, the switch prompts the user to verify their SNMP credentials against the SNMP credentials of discovered devices. SNMP v2 and v3

credentials must be verified before the switch displays discovered devices within the Recently Found Devices table.

If SNMP v2 is used with a discovering profile, a **Read Community String** screen displays.The Community String entered is required to match the name used by the remote network management software of the discovered switch

If SNMP v3 is used with a discovering profile, a **V3 Authentication** screen displays. The User Name and Password are required to match the name used by the remote network management software of the discovered switch

When the credentials of the V2 Read Community or V3 Authentication screens are satisfied, the switch discovery process begins.

7. If necessary, click the **Stop Discovery** button (enabled only during the discovery operation) to stop the discovery operation.

5.7.1.1 Adding a New Discovery Profile

If the contents of an existing profile are no longer relevant to warrant modification using the Edit function, then a new switch discovery profile should be created

To create a new switch discovery profile:

1. Select **Services** > **Discovery** from the main menu tree.
2. Click the **Add** button at the bottom of the screen.

3. Define the following parameters for the new switch discovery profile:

Profile Name	Define a user-assigned name used to title the profile. The profile name should associate the profile with the group of devices or area where the discovered devices should be located.
Start IP Address	Enter the starting numeric (non DNS) IP address from where the search for available network devices is conducted.
End IP Address	Enter the ending numeric (non DNS) IP address from where the search for available network devices is conducted
SNMP Version	Use the drop-down menu to define the SNMP version (either v2 or v3) used for discovering available network devices.

4. Refer to the **Status** field for an update of the edit process.

   The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.

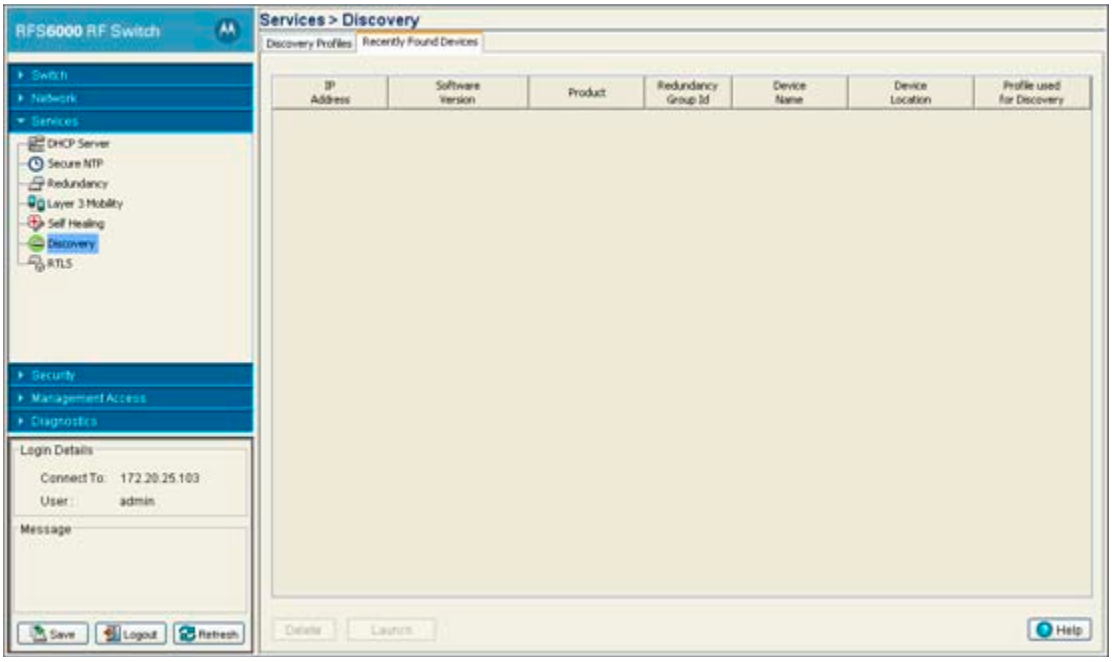
5. Click **OK** to save the changes to the running configuration and close the dialog.
6. Click **Cancel** to close the dialog without committing updates to the running configuration.

5.7.2 Viewing Discovered Switches

Refer to the **Recently Found Devices** tab to view a table of devices found by the discovery process. Each discovered device compatible with the locating switch (running switch software version 1.1 or higher) is displayed in a shaded color to distinguish it from non-compatible devices. The switch Web UI enables users display the Web UI of the discovered device in a separate browser window.

To view the devices located by the switch:

1. Select **Services** > **Discovery** from the main menu tree.
2. Select the **Recently Found Devices** tab.



3. Refer to the following within the Recently Found Devices screen to discern whether a located device should be deleted from the list or selected to have its Web UI launched and its current configuration modified.

IP Address	Displays the IP address of the discovered switch. This IP address obviously falls within the range of IP addresses specified for the discovery profile used for the device search. If the IP addresses displayed do not meet your search expectations, consider creating a new discovery profile and launching a new search.
Software Version	Displays the software version running on the discovered device.
Product	Displays the name of the device discovered by the device search. If the list of devices discovered is unsatisfactory, consider configuring a new discovery policy and launching a new search.
Redundancy Group ID	If the discovered device is part of a redundancy group, its cluster ID displays within this column. The Redundancy ID would have been assigned using the Switch > Redundancy screen.
Device Name	Displays the device name assigned to the discovered device. This name would have been assigned using the Switch > Configuration screen.
Device Location	Displays the device location defined to the discovered device. The location would have been assigned using the Switch > Configuration screen.
Profile used for Discovery	Displays the profile selected from within the Discovery Profiles tab and used with the Start Discovery function to discover devices within the switch managed network. If the group of devices discovered and displayed within the Recently Found Devices tab does not represent the device demographic needed, consider going back to the Discovery Profiles tab and selected a different profile for the switch discovery process.

4. If a discovered switch is of no interest, select it from amongst the discovered devices displayed and click the **Delete** button.

   Once removed, the located device cannot be selected and its Web UI displayed.

5. Select a discovered device from amongst those located and displayed within the Recently Found Devices screen and click the **Launch** button to display the Web UI for that switch.

CAUTION: When launching the Web UI of a discovered device, take care not to make configuration changes rendering the device ineffective in respect to its current configuration.

5.8 Locationing

5.8.1 RTLS Overview

The Motorola *Real Time Locationing System* (RTLS) is a wireless radio frequency solution that continually monitors and reports the real-time location of tracked resources. Unlike competing solutions, which are based solely on WI-Fi, the Motorola solution is RF agnostic and supports passive RFID, active RFID and other emerging RF and non-RF technologies. Motorola's location solution leverages standards based Wi-Fi access points and RFID readers, so no proprietary infrastructure is needed. By using standard 802.11 access points and Wi-Fi tags, a Wi-Fi network can now work as the backbone for data, voice, video and also serve sensor networks for a real-time location system. This quickly translates into faster deployment and improved cost-effectiveness.RTLS delivers end-user applications based on:

- The location of mobile devices (devices with location enabling technology, such as a WiFi supported handheld, Wi-Fi laptop or cell phone)
- The location of an attached tag (a location enabled mobile device in miniaturized form, for example a WiFi tag, UWB tag or RFID tag that is attached to a person, vehicles or a package)

A Motorola WLAN switch can facilitate true RF technology-agnostic mobility, allowing customers to view, manage and troubleshoot their RF network (Wi-Fi, RFID, UWB, mesh etc.) and provide accurate asset locationing information across multiple networks in real-time. This solution can also be packaged as a locationing appliance.

5.8.2 SOLE - Smart Opportunistic Location Engine

SOLE is an on-board location engine using a combination of innovative algorithms to determine location based on asset type. SOLE fuses the location information reported by several technologies into one seamless environment to get more meaningful results.

SOLE helps locate assets (including rogues) including passive tags, semi-passive tags, active tags (UWB,802.11, RFID etc) and MUs. SOLE returns the location of passive tags as seen by mobile RFID readers (like a MC9090) by combining the 802.11 reader's location with RFID antenna direction/location data.

Applications (users) inform SOLE (RF switch) about a facility map, location of infrastructure and zones. A zone is an area of specific interest with respect to whenever an asset becomes visible or invisible in that area.

SOLE uses the following input variables as needed for the specific tag type calculating location:

- User configurations
- RSSI propagation based on facility layout and RF barriers as specified by the user
- Smart surroundings (fixed wireless devices such as printers, price verifiers, near me tags as installed in the facility)
- Runtime RF environment

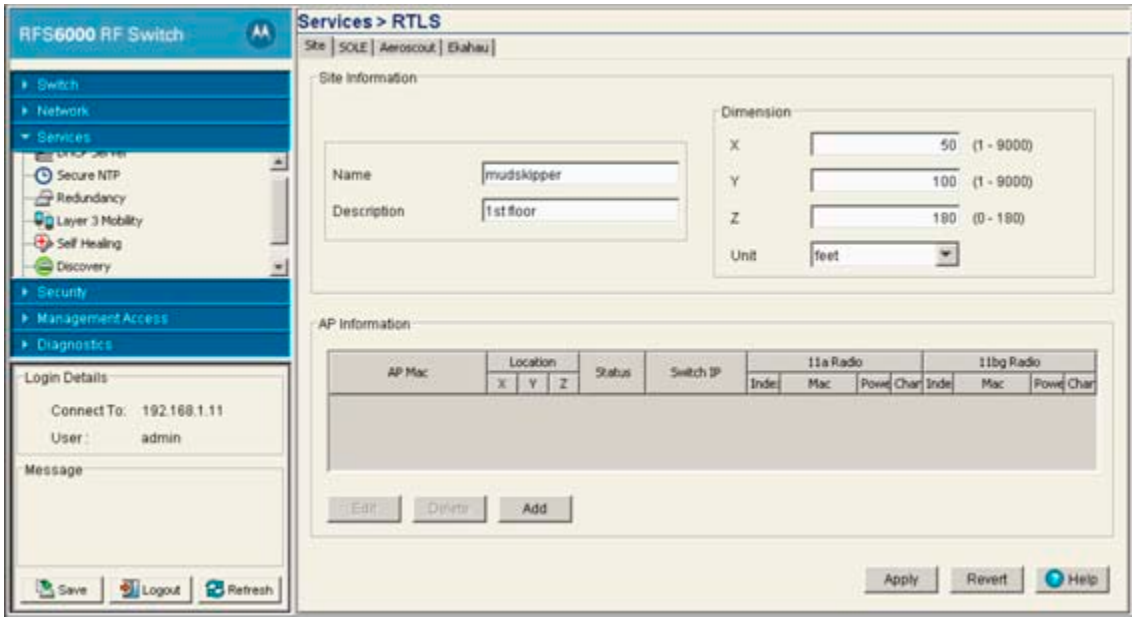
SOLE is capable of receiving input of location from external 3rd party location engines such as Aeroscout, and Ekahau. SOLE also has a self learning process that adapts with a changing environment. SOLE also provides an open platform for supporting new architectures, future algorithms or newer asset types.

5.8.3 Defining Site Parameters

In order for the locationing engine to function properly the site parameters must first be defined. Sites are defined on an X,Y axis with the upper left corner of the site being assigned a value of 0,0. When the locations of tags are displayed, they are displayed in the same X,Y format relative to the origin value of 0,0.

To configure your site parameters:

1. Select **Services** > **RTLS** from the main menu tree.



2. Select the **Site** tab.
3. Enter a **Name** and optionally a **Description** for the site:.

Name	Enter a name for the site where locationing is deployed. This is for identification purposes only.
Description	Provide a description of the site where locationing is deployed. This is an optional field.

4. When mapping a site for locationing, an origin point must be selected in one of the corners of the site. That origin will become the upper left corner of the site map with coordinates of 0,0. The length and width of the site is then mapped out on the X and Y axis (with length being X and width being Y). Those length and width along with the height are entered into the field below.

5. Define the **Dimensions** used to define the site size:

Length	Enter the length of the site. This is the X axis of your site map based on the origin point of 0,0. The size is either in feet or meters depending on which unit of measure is selected below. The valid range for length is 1-3000m or 1-9000ft.
Width	Enter the width of the site. This is the Y axis of your site map based on the origin point of 0,0. The size is either in feet or meters depending on which unit of measure is selected below. The valid range for width is 1-3000m or 1-9000ft.
Height	Enter the height of the site. The size is either in feet or meters depending on which unit of measure is selected below. The acceptable range for height is 0-60m or 0-180ft. Height is an optional parameter and is not taken into account by the locationing algorithm.
Unit	Use the drop-down menu to select the unit of measure used for dimensions. The options are feet or meters.

6. The **AP Information** section displays the following information about APs:

AP MAC	Lists the MAC Addresses of all APs which have been configured for RTLS.
Location: X Coordinate	Displays the value of the X Coordinate for each AP. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map. This value is user configured and not detected by the switch. For information on how to configure AP location information, see *Adding AP Location Information on page 5-65*.
Location: Y Coordinate	Displays the value of the Y Coordinate for each AP. The Y coordinate is relative to the origin point of 0,0 in the upper left corner of the site map. This value is user configured and not detected by the switch. For information on how to configure AP location information, see *Adding AP Location Information on page 5-65*.
Location: Z Coordinate	Displays the value of the Z Coordinate for each AP. The Z coordinate is the height of the AP relative to the lowest point of the site. This value is user configured and not detected by the switch. For information on how to configure AP location information, see *Adding AP Location Information on page 5-65*.
Status	Displays the status value for each AP.
Switch IP	Displays the IP address of switch associated with each AP configured for RTLS.
11a Radio	Displays the Index, MAC Address, Power and Channel information for the 802.11a radio on each AP.
11b Radio	Displays the Index, MAC Address, Power and Channel information for the 802.11b radio on each AP.

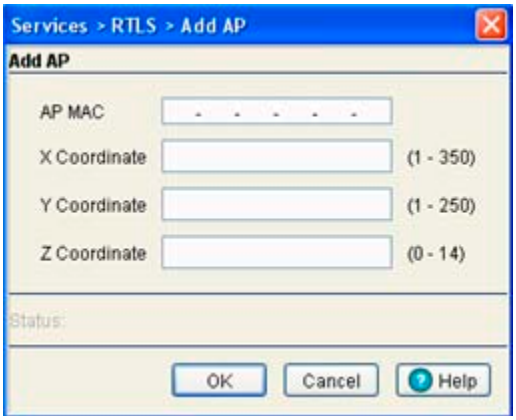
7. Click the **Apply** button to save the changes made within this screen. Clicking Apply overwrites the previous configuration.
8. Click the **Revert** button to disregard any changes made within this screen and revert back to the last saved configuration.

5.8.3.1 Adding AP Location Information

To add AP Location information for your site

1. Select **Services** > **RTLS** from the main menu tree.

2. Select the **Site** tab.
3. Click the **Add** button

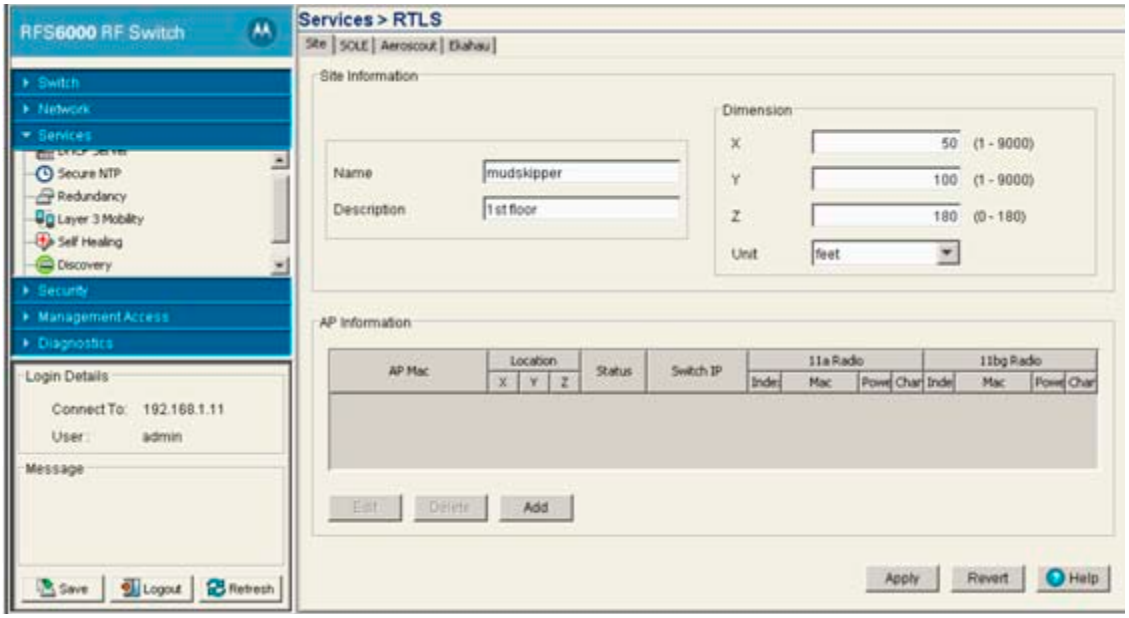


4. Provide the AP's MAC address and X, Y, and Z coordinates.
5. Select **OK** when completed to save your AP configuration.

5.8.4 Configuring SOLE Parameters

To configure the switch's internal SOLE locationing engine:

1. **Services** > **RTLS** from the main menu tree.



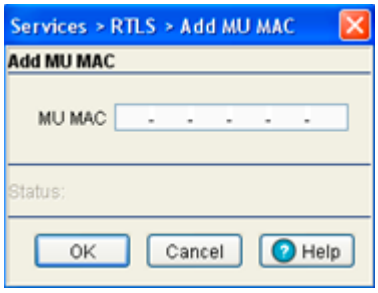
2. Select the **SOLE** tab.
3. Check the **Locate All Mobile-Units** checkbox to locate all MUs known to the switch across all WLANs. This will also disable manual entry of MU MAC addresses in the field below.
   This takes effect immediately when the box is checked.
4. Enter a value for the **MU Locate Interval** in seconds.

   The **MU Locate Interval** determines how often the locationing of MUs is updated. The valid range for this is between 5 to 3600 seconds.

5. Click the **Apply** button to save the MU Locate Interval value.
6. Click the **Revert** button to cancel any changes made within MU Locate Interval value and revert back to the last saved configuration.

NOTE: AP coordinates can only be configured in the Command Line Interface. For more information on configuring AP coordinates please consult the Motorola RF Switch CLI Reference.

7. The **MU MAC** table allows you to manually add or remove MAC Addresses which can be located by the SOLE engine. This supports a maximum of 512 MUs. This table is disabled when the **Locate All MUs** checkbox is selected.
   a. To add MUs to the **MU MAC** table click the **Add** button to open a dialogue box allowing you to add a MAC Address to the **MU MAC** table allowing it to be located by the switch's SOLE engine.



   b. To remove a MAC Address from the **MU MAC** table select a MAC Address from the table and click the **Delete** button to remove that MU. This table is disabled when the Locate All MUs checkbox is selected.

Once SOLE has been enabled MUs found by the locationing engine will be displayed in the **Located MUs** table at the bottom of the page. For each located MU the following information is displayed:

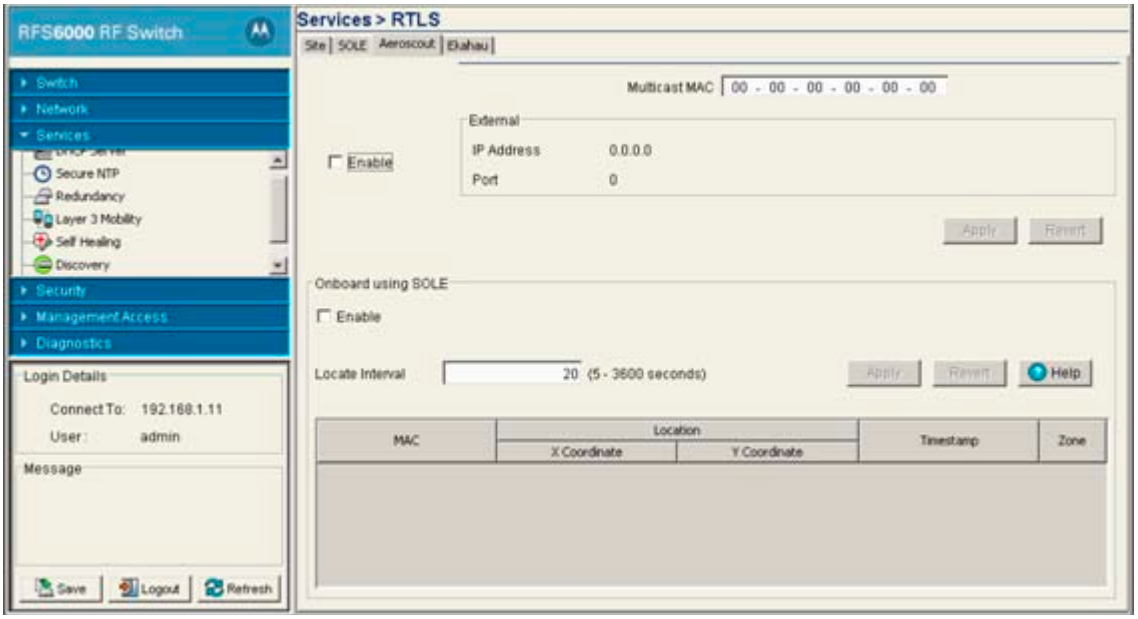
MAC	Lists the MAC Addresses of all MUs which have been located by the switch.
Location: X Coordinate	Displays the value of the X Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Location: Y Coordinate	Displays the value of the Y Coordinate for each located MU. The Y coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Timestamp	Displays the last time for each MU that its location was computed by the switch.
Zone	Lists the last known zone for each located MU. Zone configuration can be defined using the CLI interface only. When no zones are configured, the switch defaults the entire site to Zone 0.

NOTE: Zone configuration can be defined using the CLI interface only. For information on Zone Configuration please see the *Motorola RF Switch CLI Reference*.

5.8.5 Configuring Aeroscout Parameters

To configure the switch to work with an external Aeroscout RTLS engine:

1. **Services** > **RTLS** from the main menu tree.



2. Select the **Aeroscout** tab.
3. Check the **Enable** checkbox to globally enable Aeroscout RTLS support on the switch. This takes effect immediately when the box is checked.
4. Enter the **Multicast MAC Address** used for all Aeroscout tags to send updates via multicast to the MAC address specified. Typically the MAC address will start with 01-0C-CC-XX-XX-XX.

NOTE: To use the onboard SOLE engine to locate Aeroscout tags, site parameters, AP location (Command Line Interface only) and Zone configuration (optional, Command Line Interface only) must be configured.

5. Click the **Apply** button to save the **Multicast MAC Address** value.
6. Click the **Revert** button to cancel any changes made within **Multicast MAC Address** value and revert back to the last saved configuration.
7. If the **Multicast MAC Address** is configured and Aeroscout support is enabled the following information will be displayed:

IP Address	Displays the IP address of the external Aeroscout RTLS engine.
Port	Displays the port number which the switch uses to connect to the external Aeroscout RTLS engine.

8. To use the onboard SOLE engine to locate Aeroscout tags check the **Enable** checkbox. This is enabled immediately after checking the box.
9. If the onboard SOLE engine is enabled to locate Aeroscout tags, enter a **Locate Interval** in seconds to specify how often the known tags are located by the SOLE engine.
10. Click the **Apply** button to save the **Locate Interval** value.
11. Click the **Revert** button to cancel any changes made within **Locate Interval** value and revert back to the last saved configuration.

If the onboard SOLE engine is enabled to locate Aeroscout tags the following information will be displayed for each located MU:

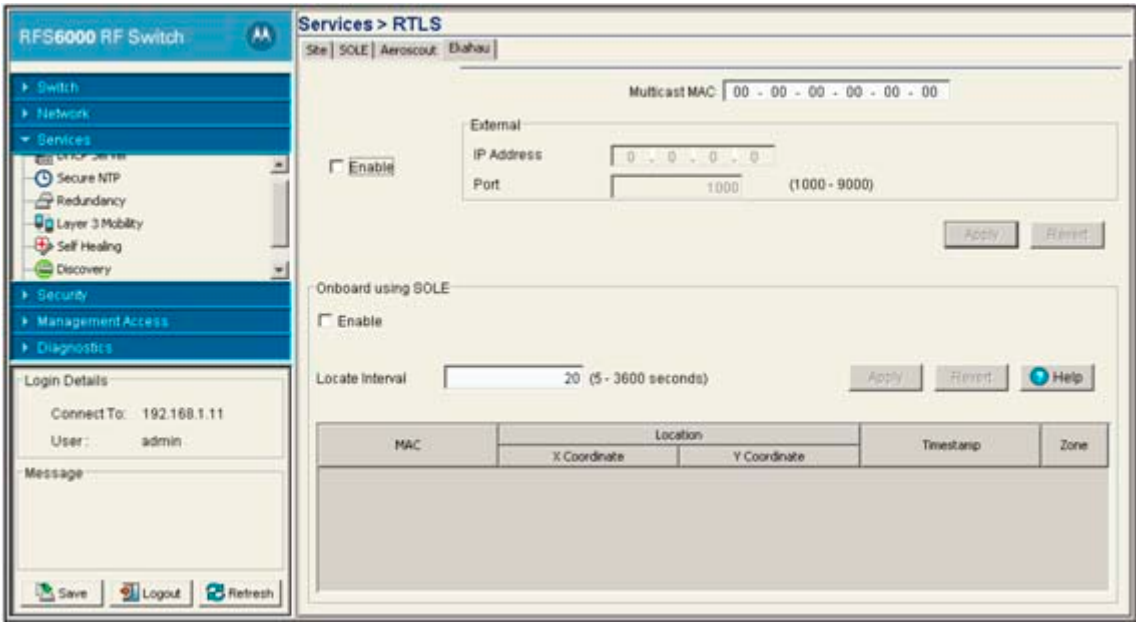
MAC	Lists the MAC Addresses of all MUs which have been located by the switch.
Location: X Coordinate	Displays the value of the X Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Location: Y Coordinate	Displays the value of the Y Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Timestamp	Displays the last time for each MU that its location was computed by the switch.
Zone	Lists the last known zone for each located MU. Zone configuration can be defined using the CLI interface only. When no zones are configured, the switch defaults the entire site to Zone 0.

NOTE: Zone configuration can be defined using the CLI interface only. For information on Zone Configuration please see the *Motorola RF Switch CLI Reference*.

5.8.6 Configuring Ekahau Parameters

To configure the switch to work with an external Ekahau RTLS engine:

1. **Services** > **RTLS** from the main menu tree.



2. Select the **Ekahau** tab.
3. Check the **Enable** checkbox to globally enable Ekahau support on the switch.

   This takes effect immediately when the box is checked.

4. Enter the **Multicast MAC Address** used for all Ekahau tags to send updates via multicast to the MAC address specified. Typically the MAC address will start with 01-0C-CC-XX-XX-XX.

NOTE: To use the onboard SOLE engine to locate Ekahau tags, site parameters, AP location (Command Line Interface only) and Zone configuration (optional, Command Line Interface only) must be configured.

5. Specify the **IP Address** of the Ekahau RTLS engine server.
6. Enter the **Port** number used to communicate with the Ekahau RTLS engine. The port range must be between 1000 and 9000.
7. Click the **Apply** button to save the **Multicast MAC Address, IP Address** and **Port** information
8. Click the **Revert** button to cancel any changes made within **Multicast MAC Address, IP Address** and **Port** settings and revert back to the last saved configuration.
9. If the **Multicast MAC Address, IP Address** and **Port** values are configured and Ekahau RTLS support is enabled the following information will be displayed:

IP Address	Displays the IP address of the external Ekahau RTLS engine.
Port	Displays the port number which the switch uses to connect to the external Ekahau RTLS engine.

10. To use the onboard SOLE engine to locate Ekahau tags check the **Enable** checkbox. This is enabled immediately after checking the box.
11. If the onboard SOLE engine is enabled to locate Ekahau tags, enter a **Locate Interval** in seconds to specify how often the known tags are located by the SOLE engine.
12. Click the **Apply** button to save the **Locate Interval** value.
13. Click the **Revert** button to cancel any changes made within **Locate Interval** value and revert back to the last saved configuration.

If the onboard SOLE engine is enabled to locate Ekahau tags the following information will be displayed for each located MU:

MAC	Lists the MAC Addresses of all MUs which have been located by the switch.
Location: X Coordinate	Displays the value of the X Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Location: Y Coordinate	Displays the value of the Y Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Timestamp	Displays the last time for each MU that its location was computed by the switch.
Zone	Lists the last known zone for each located MU. Zone configuration can be defined using the CLI interface only. When no zones are configured, the switch defaults the entire site to Zone 0.

NOTE: Zone configuration can be defined using the CLI interface only. For information on Zone Configuration please see the *Motorola RF Switch CLI Reference*.

6

Switch Security

This chapter describes the security mechanisms available to the switch. This chapter describes the following security configuration activities:

- *Displaying the Main Security Interface*
- *AP Intrusion Detection*
- *MU Intrusion Detection*
- *Configuring Firewalls and Access Control Lists*
- *Configuring NAT Information*
- *Configuring IKE Settings*
- *Configuring IPSec VPN*
- *Configuring the Radius Server*
- *Creating Server Certificates*
- *Configuring Enhanced Beacons and Probes*

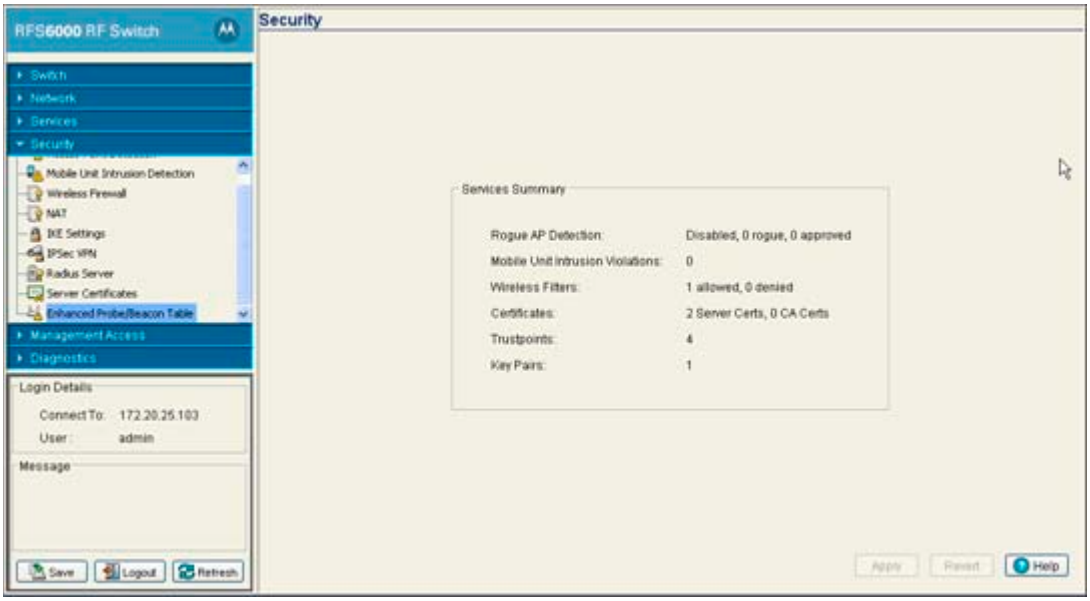
6.1 Displaying the Main Security Interface

Refer to main **Security** interface for a high level overview of device intrusion and switch access permission options.

NOTE: When the switch's configuration is successfully updated (using the Web UI), the effected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the effected screen's Status field remains displayed. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To view main menu security information:

1. Select **Security** from the main menu tree.



2. Refer to the following information to discern if configuration changes are warranted:

Rogue AP Intrusion Detection	Displays the enabled or disabled switch state to detect potentially hostile Access Ports (the definition of which is defined by you). Once detected, rogue devices can be added to a list of devices either approved or denied from interoperating within the switch managed network. For more information, see *AP Intrusion Detection on page 6-2*.
Mobile Unit Intrusion Detection	Displays the state of the switch protecting against threats from MUs trying to find network vulnerabilities. For more information, see *MU Intrusion Detection on page 6-10*.
Wireless Filters	Displays the state of the filters used to either allow or deny a MAC address (or groups of MAC addresses) from associating with the switch. For more information, see *Configuring Firewalls and Access Control Lists on page 6-13*.
Certificates	Displays the number of Server and CA certificates currently used by the switch. For more information, see *Creating Server Certificates on page 6-97*.
Trustpoints	Displays the number of trustpoints currently in use by this switch. The trustpoint signing the certificate can be a certificate authority, corporation or an individual. A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. For more information, see *Using Trustpoints to Configure Certificates on page 6-98*.
Key Pairs	Displays the number of Key Pairs currently used by the switch. For more information, see *Configuring Trustpoint Associated Keys on page 6-106*.

The **Apply** and **Revert** buttons are greyed out within this screen, as there is no data to be configured or saved.

6.2 AP Intrusion Detection

Use the **Access Point Detection** menu options to view and configure the detection of other Access Points. The Access Point Detection screen consists of the following tabs:

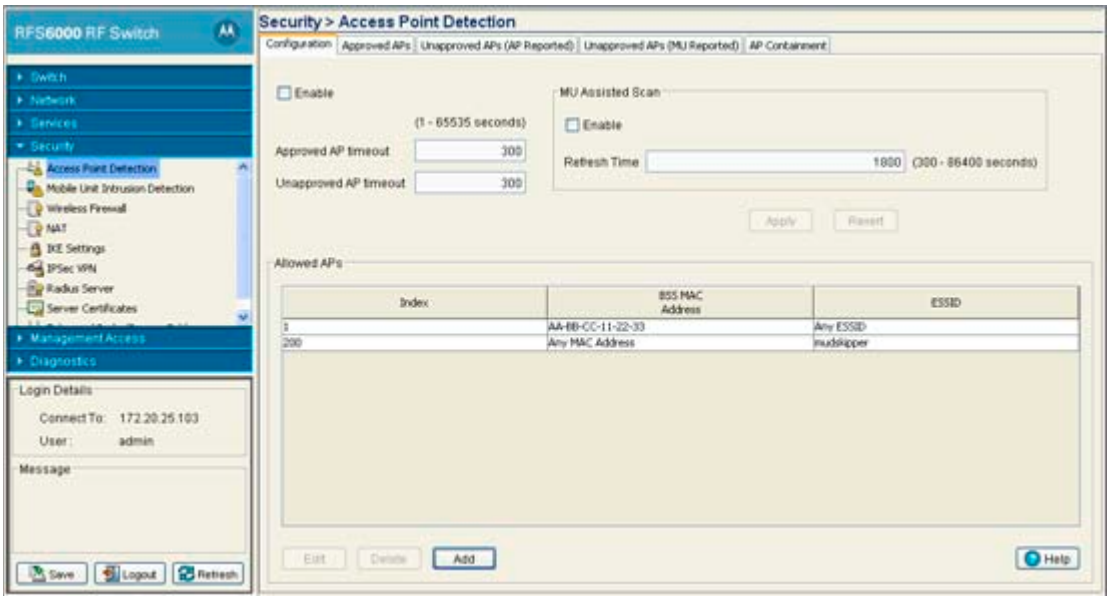
- *Enabling and Configuring AP Detection*
- *Approved APs*
- *Unapproved APs (AP Reported)*
- *Unapproved APs (MU Reported)*
- *AP Containment*

6.2.1 Enabling and Configuring AP Detection

Use the **Configuration** screen to allow the switch to detect potentially hostile Access Points, set the number of detected APs allowed and define the timeout and threshold values used for detection. The switch can enable both Access Ports and MUs to scan and detect Access Points within the switch managed network. Continually re-validating the credentials of associated devices reduces the possibility of an Access Point hacking into the switch managed network.

To configure AP Detection:

1. Select **Security** > **Access Port Intrusion Detection** from the main menu.
2. Select the **Configuration** tab.



3. Enable AP assisted scanning and timeout intervals as required.

Enable — Select the **Enable** checkbox to enable associated Access Ports to detect potentially hostile Access Points (the definition of which defined by you). Once detected, the Access Points can be added to a list of APs either approved or denied from interoperating within the switch managed network.

Approved AP timeout	Define a value (in seconds) the switch uses to timeout (previously approved) Access Points that have not communicated with the switch. The range is from 1-65535 seconds, with a default of 300 seconds. This value is helpful for continually re-validating Access Points that interoperate within the switch managed network.
Unapproved AP timeout	Define a value (in seconds) the switch uses to remove Access Points that have not communicated with the switch. The range is from 1-65535 seconds, with a default of 300 seconds.

4. Refer to the **MU Assisted Scan** field to enable associated MUs to assist in the detection of Access Points.

Enable	Select the **Enable** checkbox to enable associated MUs to detect potentially hostile Access Points (the definition of which defined by you). Once detected, these devices can be added to a list of Access Points either approved or denied from interoperating within the switch managed network.
Refresh Time	Define a value (in seconds) associated MUs use to scan for Access Points. The range is from 300 - 86400 seconds, with a default of 1800 seconds.

NOTE: When using MU Assisted Scans with an AP300 Access Port the MU Assisted scan will begin as soon as the **Enable** checkbox is selected. Subsequent scans will take place based on the time defined in the **Refresh Time** field.

NOTE: When using MU Assisted Scans with an AP-5131 the MU Assisted scan will not begin immediately. The first scan will begin after the current **Refresh Time** cycle has expired.

5. Click the **Apply** button to save the changes made.
6. Click the **Revert** button to cancel any changes and revert back to the last saved configuration.
7. Refer to the **Allowed APs** field to view the policies used for interpreting Access Points as allowed.

Index	Displays the numerical identifier (index value) assigned to this particular set of Allowed APs. Assign this value by clicking **Add** for a new set of Access Point address information or click the **Edit** button to revise the index. The Index can be used as reference to group specific devices numerically to a specific range of MAC or ESSID addresses. This user cannot modify the index from this screen.
BSS MAC Address	Displays the MAC address of the Allowed AP(s). The MAC addresses displayed are defined by clicking the **Add** button and entering a specific MAC address or by allowing all MAC addresses to be allowed. The list of MAC addresses allowed can be modified by highlighting an existing entry, clicking the **Edit** button and revising the properties of the MAC address.
ESSID	Displays the ESSIDs of the Allowed AP(s). The addresses displayed are defined by clicking the **Add** button and entering a specific MAC address or by allowing all MAC addresses to be allowed. The list of MAC addresses allowed can be modified by highlighting an existing entry, clicking the **Edit** button and revising the properties of the MAC address.

8. Select an Allowed AP and click the **Edit** button to launch a screen used to modify the index and SSID of the AP. For more information, see *Adding or Editing an Allowed AP on page 6-5*.
9. Select an Allowed AP and click the **Delete** button to remove the AP from list of Allowed APs.

10. Click the **Add** button to display a screen used to enter device information for a new AP added to the Allowed AP list. For more information, see *Adding or Editing an Allowed AP on page 6-5*.

6.2.1.1 Adding or Editing an Allowed AP

To add a new address range or modify the address range used to designate devices as allowed:

1. Select **Security** > **Access Point Intrusion Detection** from the main tree menu.
2. Click the **Configuration** tab.
3. Select an existing Allowed AP and click the **Edit** button to modify the properties of an existing Allowed AP or click the **Add** button to define the attributes of a new Allowed AP.

4. If adding a new Allowed AP, use the **Index** parameter to assign a numerical index value to this particular Access Point. The index range is from 1-200. If editing an existing Allowed AP, this is a read only field and cannot be modified.
5. Refer to the **BSS MAC Address** field to define the following:

Any MAC Address/ Specific MAC Address	Click the **Any MAC Address** radio button to allow any MAC address detected on the network as an Allowed AP. This is not necessary if a specific MAC address is used with this index. Click the second radio button to enter a specific MAC address as an Allowed AP. Use this option if (for network security) you want to restrict the number of MAC Addresses to a single MAC address.

6. Refer to the **ESSID** field to configure Access Point ESSID permissions.

Any ESSID/Specific ESSID	Click the **Any ESSID** radio button to allow any ESSID located on the network as an Allowed AP. This may not be necessary if a specific ESSID was used with this particular index. Click the second radio button to enter a specific ESSID as an Allowed AP. Use this option if (for network security) you want to restrict the number of device ESSIDs saved for this index to a single Access Point ESSID.

7. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to use the changes to the running configuration and close the dialog.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.2.2 Approved APs

Those Access Points detected and approved for operation within the switch managed network can be separately displayed to assess the reporting (detecting) AP, the channel of operation, the last time the AP was observed on the network and the ESSID. Use this information to assess if an approved Access Point was incorrectly defined as approved and requires categorization as an unapproved and disallowed AP.

To review the attributes of allowed APs:

1. Select **Security** > **Access Port Intrusion Detection** from the main menu.
2. Select the **Approved APs** tab.

3. The **Approved APs** table displays the following information:

BSS MAC Address	Displays the MAC Address of approved APs. These MAC addresses are APs observed on the network meeting the criteria (MAC and ESSIDs) of allowed APs.
Reporting Radio	Displays the numerical value assigned to the radio used with the specific device MAC Address and SSID listed for this approved AP.
Channel	Displays the channel the approved AP is currently transmitting on. If this device is operating on a channel not frequently used within your network segment, perhaps the device is correctly defined as an approved AP.
Last Seen (Seconds)	Displays the time (in seconds) the approved AP was last seen on the network.
ESSID	Displays the SSID of each approved AP.

4. The **Number of Approved APs** is simply the sum of all of approved Access Point MAC Addresses detected.

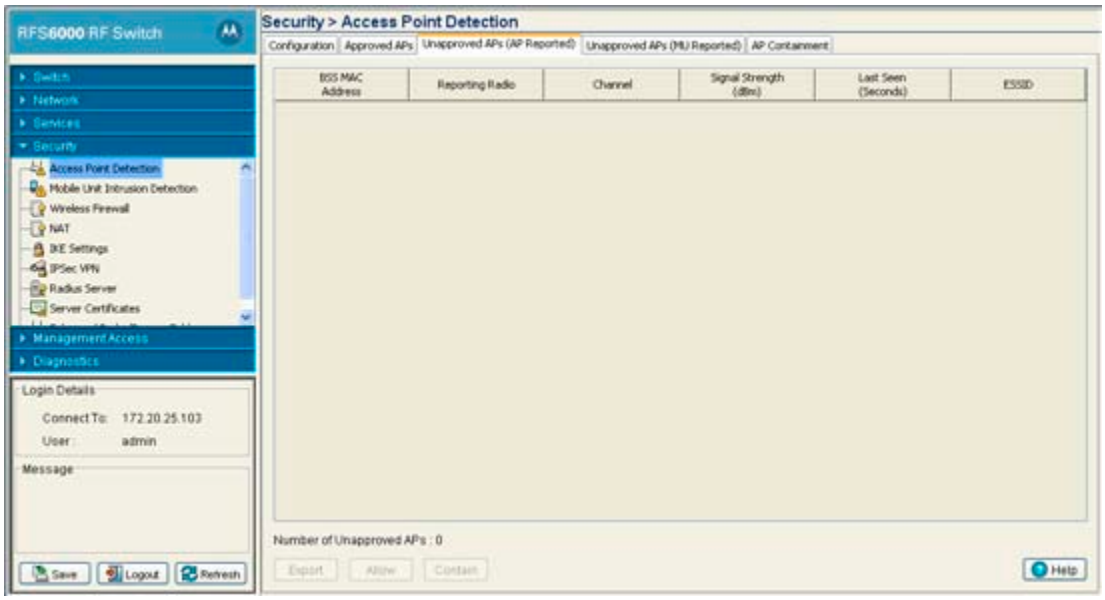
5. Click on the **Export** button to export the contents of the table to a Comma Separated Values file (CSV).

6.2.3 Unapproved APs (AP Reported)

Use the **Unapproved APs (AP Reported)** tab to review Access Points detected by associated switch Access Port radios and are restricted from operation within the switch managed network. The criteria for restriction was defined using the **Security > Access Port Intrusion Detection > Configuration** screen.

To view Access Port detected unapproved Access Points:

1. Select **Security** > **Access Port Intrusion Detection** from the main menu tree.
2. Click on the **Unapproved APs (AP Reported)** tab.



3. The **Unapproved APs (AP Reported)** table displays the following information:

BSS MAC Address	Displays the MAC Address of each Unapproved AP. These MAC addresses are Access Points observed on the network, but have yet to be added to the list of Approved APs, and are therefore interpreted as a threat on the network. If a MAC Address displays on the list incorrectly, click the **Allow** button and add the MAC Address of a newly Allowed AP index.
Reporting Radio	Displays the numerical value for the radio used with the detecting AP.
Channel	Displays the channel the Unapproved AP is currently transmitting on.
Signal Strength (dbm)	Displays the *Relative Signal Strength Indicator* (RSSI) for the detected (and unapproved) AP. AP's with a strong signal may pose a more significant risk within the switch managed network.
Last Seen (Seconds)	Displays the time (in seconds) the Unapproved AP was last seen on the network by the detecting AP.
ESSID	Displays the ESSID of each Unapproved AP. These ESSIDs are device ESSIDs observed on the network, but have yet to be added to the list of Approved APs and are therefore interpreted as a threat. If an ESSID displays on the list incorrectly, click the **Allow** button and add the ESSID to a new Allowed AP index.

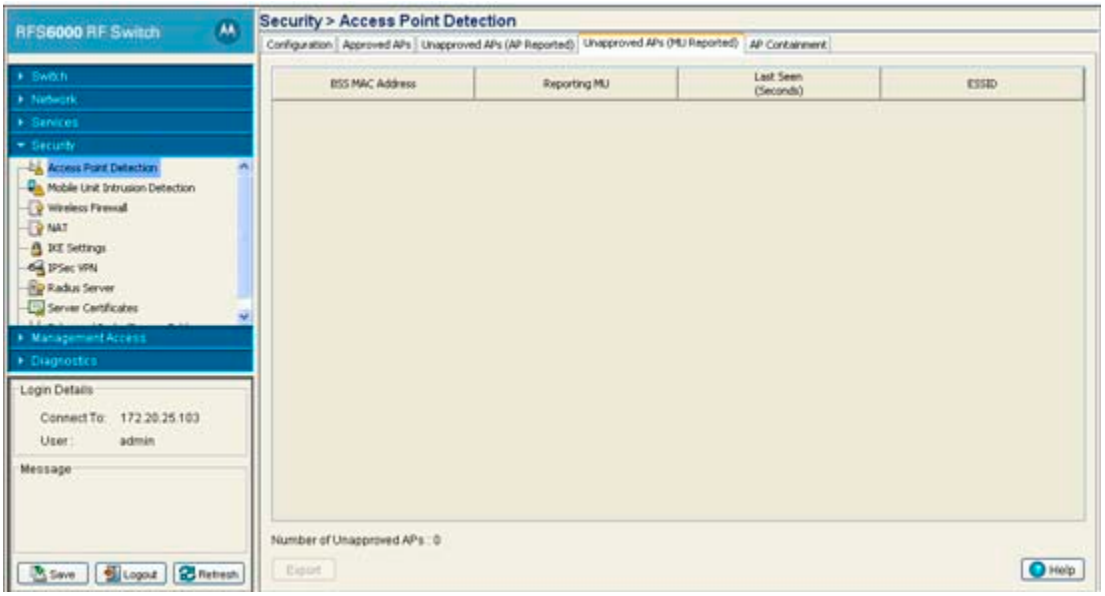
4. The **Number of Unapproved APs** is simply the sum of all of Unapproved Radio MAC Addresses detected.
5. If a radio's MAC address is listed incorrectly, highlight the MAC Address and click the **Allow** button.

   Assign an Index and define the required device address information to move the device into the list of approved Access Point MAC addresses. The number of Unapproved APs updates accordingly as devices are added and removed.
6. Click the **Export** button to export the contents of the table to a *Comma Separated Values* file (CSV).

6.2.4 Unapproved APs (MU Reported)

Use the **Unapproved APs (MU Reported)** tab to review unapproved Access Points detected by associated MUs. The criteria for Access Point approval was defined using the **Security > Access Port Intrusion Detection > Configuration** screen, using the values defined within the **MU Assisted Scan** field.To view unapproved Access Points detected by switch radio associated MUs:

1. Select **Security** > **Access Port Intrusion Detection** from the main menu tree.
2. Click on the **Unapproved APs (MU Reported)** tab.



3. The **Unapproved APs (MU Reported)** table displays the following information:

BSS MAC Address	Displays the MAC Address of each Unapproved AP. These MAC addresses are Access Points observed on the network (by associated MUs), but have yet to be added to the list of approved APs, and are therefore interpreted as a threat on the network.
Reporting MU	Displays the numerical value for the detecting MU.
Last Seen (Seconds)	Displays the time (in seconds) the Unapproved AP was last seen on the network by the detecting MU. Use this interval to determine whether the detected MU is still a viable threat.
ESSID	Displays the ESSID of each Unapproved AP. These ESSIDs are device ESSIDs observed on the network, but have yet to be added to the list of Approved APs and are therefore interpreted as a threat.

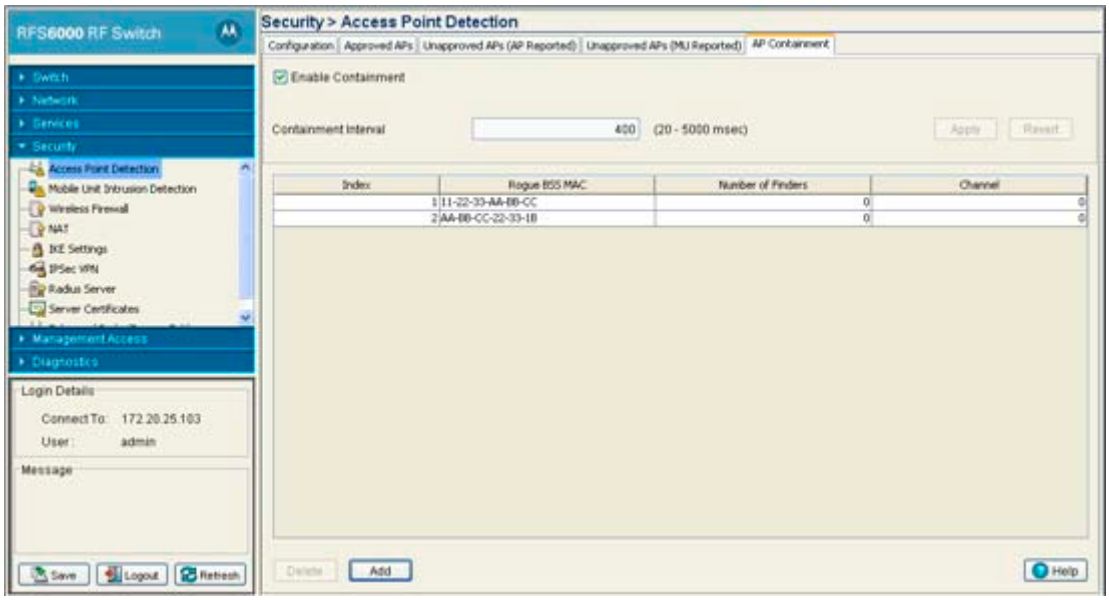
4. The **Number of Unapproved APs** is simply the sum of all of Unapproved Radio MAC Addresses detected.
5. Click the **Export** button to export the contents of the table to a Comma Separated Values file (CSV).

6.2.5 AP Containment

Use the rogue **AP Containment** feature to provide protection from rogue Access Points by disrupting traffic to mobile units associated with the Rogue AP and prevents new mobile units from getting associated to the Rogue AP.

To configure Access Point Containment and view rogue APs:

1. Select **Security** > **Access Port Intrusion Detection** from the main menu tree.
2. Click on the **AP Containment** tab.



The **AP Containment screen** is divided into two sections, configuration and rogue AP information.

3. To enable the AP containment feature, check the **Enable Containment** checkbox and specify a **Containment Interval** between 20 and 5000 miliseconds.
   The Containment Interval field determines the interval after which broadcast 802.11 de-authentication messages will be sent.
4. When the containment feature has been enabled and a **Containment Interval** has been set, click the **Apply** button to enable the feature and save the interval value.
5. The rogue AP table displays the following information about known rogue APs:

Index	A unique numerical ID assigned by the switch for each of the known rogue APs.
Rogue BSS Mac	Display a list of all know Rogue BSS MAC Addresses known to the switch.
Number of Finders	Displays the number of detector APs that have found each specified Rogue AP.
Channel	Displays the channels that each of the known Rogue APs are broadcasting on.

6. To manually add a rogue AP to the table, click the **Add** button and enter the MAC address of the known rogue AP.

7. To remove an AP from the rogue AP table, select that AP and click the **Delete** button.

6.3 MU Intrusion Detection

Unauthorized attempts to access the switch managed LAN by MUs is a significant threat to the network, and one that is very pervasive currently. The switch has several means to protect against threats from MUs trying to find network vulnerabilities.

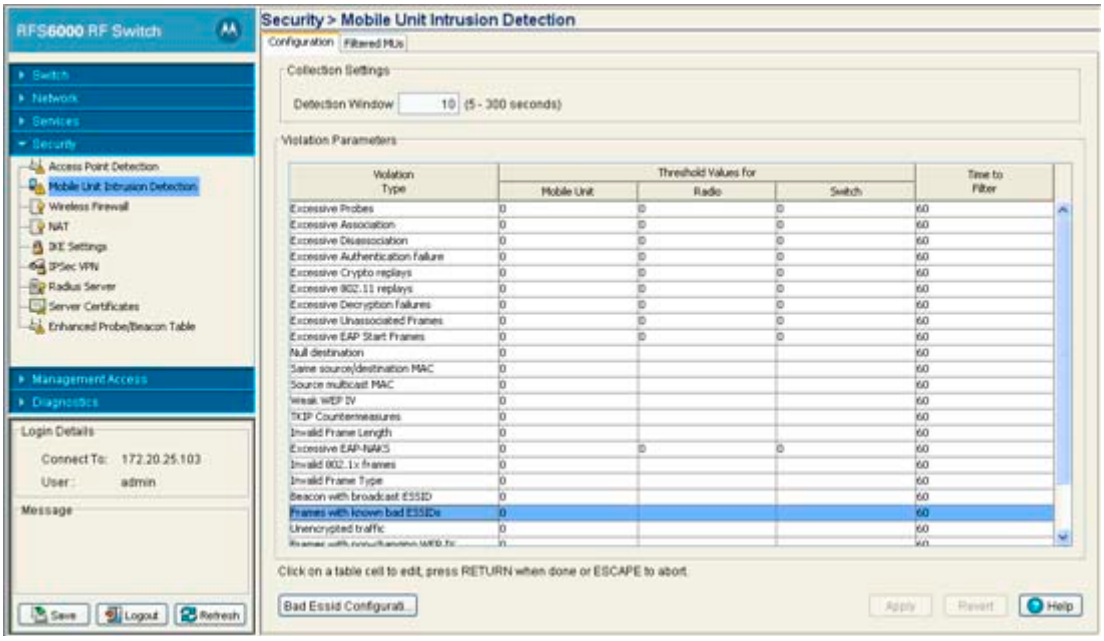
Use the switch's **Mobile Unit Intrusion Detection** facility to view and configure MU intrusion related information. The Mobile Unit Intrusion Detection screen provides the following functionalities:

- *Configuring MU Intrusion Detection*
- *Viewing Filtered MUs*

6.3.1 Configuring MU Intrusion Detection

To configure MU intrusion detection:

1. Select **Security** > **Mobile Unit Intrusion Detection** from the main tree menu.
2. Click the **Configuration** tab.



The MU Intrusion Detection tab consists of the following two fields:

- *Collection Settings*
- *Violation Parameters*

3. Within the **Collection Settings** field, set the **Detection Window** interval (in seconds) the switch uses to scan for MU violations. The available range is from 5 - 300 seconds.

4. Refer to the **Violation Parameters** field to define threshold values that trigger an alarm:

Violation Type	Displays the name of the violation for which threshold values are set in the MU, radio and switch columns.
Mobile Unit	Set the MU threshold value for each violation type. If exceeded, the MU will be filtered and displayed within the Filtered MUs screen. For non-threshold violations, setting the value to 1 enables detection.
Radio	Set the radio threshold value for each violation type. If exceeded, the MU is filtered and displayed within the Filtered MUs screen.
Switch	Set the switch's threshold value for each violation type. If exceeded, the offending MU is filtered (from the switch) and displayed within the Filtered MUs screen.
Time to Filter	Set the interval (in seconds) the switch uses to filter out MUs defined as committing a violation. Refer to *Viewing Filtered MUs on page 6-12* to review the contents of MUs filtered thus far.

CAUTION: Setting MU threshold values too low can jeopardize MU performance or break the MU's connection.

5. When using the **Frames with known bad ESSID**s violation parameter it is necessary to enter a list of known bad ESSIDs for the violation parameter. To enter this information, select **Frames with known bad ESSIDs** and then click the **Bad Essid Config** button to launch a dialogue box where bad ESSIDs can be added and removed.

NOTE: If using the **Frames with known bad ESSIDs** violation parameter if no ESSIDs are entered in the **Bad Essid Config** dialogue, this parameter will not function.

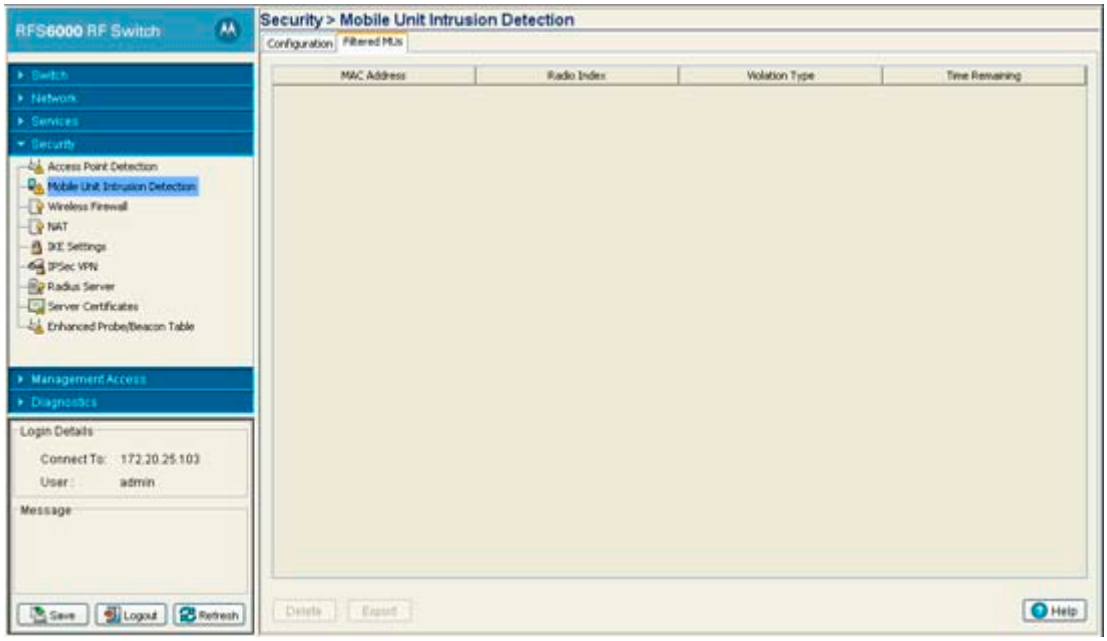
6. Click on **Apply** button to save the configuration.
7. Click on **Revert** to rollback to the previous configuration.

6.3.2 Viewing Filtered MUs

Periodically check the **Filtered MUs** tab to review MUs filtered by the switch for incurring a violation based on the settings defined within the **Configuration** tab. Each MU listed can be deleted from the list or its attributes exported to a user defined location.

To view status of those MUs filtered using the settings defined within the **Configuration** tab:

1. Select **Security** > **Mobile Unit Intrusion Detection** from the main tree menu.
2. Click on the **Filtered MUs** tab.



The Filtered MUs tab displays the following read-only information for detected MUs:

MAC Address	Displays the MU's MAC address. Defer to this address as the potentially hostile MU's identifier.
Radio Index	The radio index displays the index of the detected MU. Use this information to discern whether the detected MU is known and whether is truly constitutes a threat.

Violation Type — Displays the reason the violation occurred for each detected MU. Use the Violation Type to discern whether the detected MU is truly a threat on the switch managed network (and must be removed) or can be interpreted as a non threat. The following violation types are possible:

- *Excessive Probes*
- *Excessive Association*
- *Excessive Disassociation*
- *Excessive Authentication failure*
- *Excessive Crypto replays*
- *Excessive 802.11 replays*
- *Excessive Decryption failures*
- *Excessive Unassociated Frames*
- *Excessive EAP Start Frames*
- *Null destination*
- *Same source/destination MAC*
- *Source multicast MAC*
- *Weak WEP IV*
- *TKIP Countermeasures*
- *Invalid Frame Length*
- *Excessive EAP-NAKS*
- *Invalid 802.1x frames*
- *Invalid Frame Type*
- *Beacon with broadcast ESSID*
- *Frames with known bad ESSIDs*
- *Unencrypted traffic*
- *Frames with non-changing WEP IV*
- *Detect Adhoc Networks*
- *De-auth from broadcast smac*
- *Invalid Sequence Number*

NOTE: The following violation types require the Access Port be in scan mode:

- *Beacon with broadcast ESSID*
- *Frames with known bad ESSIDs*

Time Remaining — Displays the time remaining before the next filter activity. Detected MUs are removed from the filtered list when they no longer violate the thresholds defined within the Configuration tab.

3. Select a detected MU and click the **Delete** button to remove it from the list of MUs you are tracking as potential threats within the switch managed network.
4. Click on the Export button to export the contents of the table to a Comma Separated Values file (CSV).

6.4 Configuring Firewalls and Access Control Lists

An *Access Control List* (ACL) is a a sequential collection of permit and deny conditions that apply to switch packets. When a packet is received on an interface, the switch compares the fields in the packet against any

applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists.

NOTE: If a packet does not meet any of the criteria specified in the ACL, the packet is dropped.

Use the **Wireless Firewall** screen to view, add and configure access control configurations. Typically, an ACL consists of series of entries called an Access Control Entry (ACE). Each ACE defines the rule which defines whether the packets needs to be switched/routed or needs to be dropped. The ACL screen displays three tabs:

- *Security Policy*
- *Configuration*
- *Statistics*

Each of these tabs has sub tabs which provide configuration options for creating and attaching the ACLs.

NOTE: For an overview of how the switch uses an ACL to filter permissions to the switch managed network, go to *ACL Overview on page 6-14*.

6.4.1 ACL Overview

An ACL contains an ordered list of *Access Control Entries* (ACEs). Each ACE specifies an action and a set of conditions that a packet must satisfy in order to match the ACE. The order of conditions in the list is critical because the switch stops testing conditions after the first match.

The switch supports the following ACLs to filter traffic:

- *Router ACLs* — Applied to VLAN (Layer 3) interfaces. These ACLs filter traffic based on Layer 3 parameters like *source IP, destination IP, protocol types* and *port numbers*. They are applied on packets routed through the switch. Router ACLs can be applied to inbound traffic only, not both directions.
- *Port ACLs*— Applied to traffic entering a Layer 2 interface. Only switched packets are subjected to these kind of ACLs. Traffic filtering is based on Layer 2 parameters like–*source MAC, destination MAC, Ethertype, VLAN-ID, 802.1p bits* (OR) Layer 3 parameters like– source IP, destination IP, protocol, port number.

NOTE: Port and router ACLs can be applied only in an inbound direction. WLAN ACLs support applying ACLs in the inbound and outbound direction.

- *Wireless LAN ACLs* - A Wireless LAN ACL is designed to filter/mark packets based on the wireless LAN from which they arrived rather than filtering the packets arrived on Layer 2 ports.

For more information, see

- *Router ACLs*
- *Port ACLs*
- *Wireless LAN ACLs*
- *ACL Actions*
- *Precedence Order*

6.4.1.1 Router ACLs

Router ACLs are applied to Layer 3 or VLAN interfaces. If an ACL is already applied in a particular direction on an interface, applying a new one will replace the existing ACL. Router ACLs are applicable only if the switch acts as a gateway, and traffic is inbound only.

The switch supports two types of Router ACLs:

- *Standard IP ACL*—Uses the source IP address as matching criteria.
- *Extended IP ACL*—Uses the source IP address, destination IP address and IP protocol type as basic matching criteria. It can also include other parameters specific to a protocol type (like source and destination port for TCP/UDP protocols).

Router ACLs are stateful and are not applied on every packet routed through the switch. Whenever a packet is received from a Layer 3 interface, it is examined against existing sessions to determine if it belongs to an established session. ACLs are applied on the packet in the following manner.

1. If the packet matches an existing session, it is not matched against ACL rules and the session decides where to send the packet.
2. If no existing sessions match the packet, it is matched against ACL rules to determine whether to accept or reject it. If ACL rules accept the packet, a new session is created and all further packets belonging to that session are allowed. If ACL rules reject the packet, no session is established.

A session is computed based on:

- *Source IP address*
- *Destination IP address*
- *Source Port*
- *Destination Port*
- *ICMP identifier*
- *Incoming interface index*
- *IP Protocol*

NOTE: Port and router ACLs can be applied only in an inbound direction. WLAN ACLs support applying ACLs in the inbound and outbound direction.

Each session has a default idle time-out interval. If no packets are received within this interval, the session is terminated and a new session must be initiated. These intervals are fixed and cannot be configured by the user.

The default idle time-out intervals for different sessions are:

- *ICMP and UDP sessions*— 30 seconds
- *TCP sessions*— 2 hours

6.4.1.2 Port ACLs

The switch supports Port ACLs on physical interfaces and inbound traffic only. The following Port ACLs are supported:

- *Standard IP ACL*— Uses a source IP address as matching criteria.

- *Extended IP ACL*— Uses a source IP address, destination IP address and IP protocol type as basic matching criteria. It can also include other parameters specific to a protocol type, like the source and destination ports for TCP/UDP protocols.
- *MAC Extended ACL*— Uses source and destination MAC addresses and VLAN ID. It optionally, also uses Ethertype information.

Port ACLs are also stateful and are not applied on every packet switched through the switch. Whenever a packet is received inbound, it is examined against existing sessions to determine if it belongs to an established session. ACLs are applied on the packet in the following manner:

1. If the packet matches an existing session, it is not matched against ACL rules and the session decides where to send the packet.
2. If no existing sessions match the packet, it is matched against ACL rules to determine whether to accept or reject it. If ACL rules accept the packet, a new session is created and all further packets belonging to that session are allowed. If ACL rules reject the packet, no session is established.

   A session is based on:

   - *Source IP address*
   - *Destination IP address*
   - *Source Port*
   - *Destination Port*
   - *ICMP identifier*
   - *Incoming interface index*
   - *IP Protocol*
   - *Source MAC*
   - *Destination MAC*
   - *Ethertype*
   - *VLAN-ID*
   - *802.1p bits*

   When a Port ACL is applied to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. With Port ACLs, you can filter:

   - *IP traffic by using IP ACL*
   - *Non-IP traffic by using MAC addresses.*

   Both 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.

   You cannot apply more than one IP ACL and one MAC ACL to a Layer 2 interface. If an IP ACL or MAC ACL is already configured on a Layer 2 interface and a new IP ACL or MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

6.4.1.3 Wireless LAN ACLs

Wireless LAN ACLs filter/mark packets based on the wireless LAN from which they arrive rather than filtering packets on Layer 2 ports.

In general, a Wireless-LAN ACL can be used to filter wireless to wireless, wireless to wired and wired to wireless traffic. Typical wired to wired traffic can be filtered using a Layer 2 port based ACL rather than a WLAN ACL.

Each WLAN is assumed to be a virtual Layer 2 port. Configure one IP and one MAC ACL on the virtual WLAN port. In contrast to Layer 2 ACLs, a WLAN ACL can be enforced on both the Inbound and Outbound direction.

6.4.1.4 ACL Actions

Every ACE within an ACL is made up of an action and matching criteria. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:

- *deny*— Instructs the ACL not to allow a packet to proceed to its destination.
- *permit*—Instructs the ACL to allows a packet to proceed to its destination.
- *mark*—Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.
  - VLAN 802.1p priority.
  - TOS/DSCP bits in the IP header.

NOTE: A Permit All ACL is not supported when using NTP. If a Permit All ACL is used with NTP, the client is not able to synchronize with the NTP server.

NOTE: Only a Port ACL supports a mark action. With Router ACLs, a mark is treated as a permit and the packet is allowed without modifications.

6.4.1.5 Precedence Order

The rules within an ACL are applied to packets based on their precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules's with the same precedence value.

Consider the following when adding rules:

- Every ACL entry in an ACL is associated with a precedence value unique for every entry. You cannot enter two different entries in an ACL with the same precedence value. This value can be between 1 and 5000. An ACE in an ACL is associated with a unique precedence value. No two ACE's can have the same precedence value.
- Specifying a precedence value with each ACL entry is not mandatory. If you do not want to specify one, the system automatically generates a precedence value starting with 10. Subsequent entries are added with precedence values of 20, 30 and so on. 10 is the default offset between any two rules in an ACL. However, if the user specifies a precedence value with an entry, that value overrides the default value. The user can also add an entry in between two subsequent entries (for example, in between 10 and 20).
- If an entry with a max precedence value of 5000 exists, you cannot add a new entry with a higher precedence value. In such a case, the system displays an error stating "Rule with max precedence value exists". Either delete the entry or add new entries with precedence values less than 5000. A user can add a maximum of 500 ACE's in an ACL.
- Rules within an ACL are displayed in an ascending order of precedence.

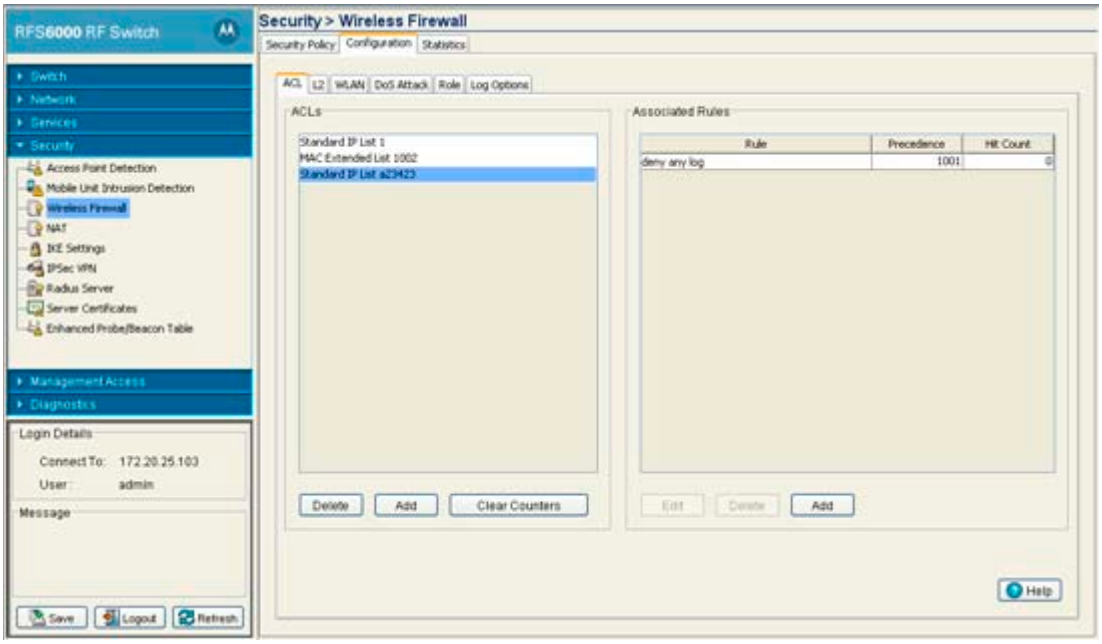
NOTE: ACEs with lower precedence are always applied first to packets. Therefore, it is advised to add more specific entries in the ACL first then the general ones. While displaying the ACL, the entries are displayed in an ascending order of precedence.

6.4.2 Configuring the Firewall

Configure the Firewall to create either standard/extended ip or extended MAC access control lists.

To configure the Firewall:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Select the **Configuration** tab.
3. Select the **ACL** tab.
4. Add a new ACL entry as explained in *Adding a New ACL on page 6-19*.
5. The Configuration tab consists of the following two fields:
   - *ACLs* - existing access lists
   - *Associated Rules* - allow/deny rules



The **ACLs** field displays the list of ACLs currently associated with the switch. An ACL contains an ordered list of ACEs. Each ACE specifies a permit or deny designation and a set of conditions the packet must satisfy to match the ACE. Because the switch stops testing conditions after the first match, the order of conditions in the list is critical.

6. If an existing ACL no longer satisfies switch access control requirements, select it from amongst the existing ACLs and click the **Delete** button.
7. Use the **Add** button (within the ACLs field) to add an additional ACL. For more information, see *Adding a New ACL on page 6-19*.
8. To reset the **Hit Count** number, click the **Clear** button.
9. Refer to the **Associated Rules** field to assess the rules and precedence associated with each ACL. If necessary, rules and can be added or existing rules modified. For more information, see *Adding a New ACL Rule on page 6-19*.

6.4.2.1 Adding a New ACL

When a packet is received by the switch, the switch compares the packet against the ACL to verify the packet has the required permissions to be forwarded. Often, ACLs need to be added as client permission changes during switch operation.

To create a new ACL:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click on the **ACL** tab to view the list of ACLs currently associated with the switch.
4. Click the **Add** button.

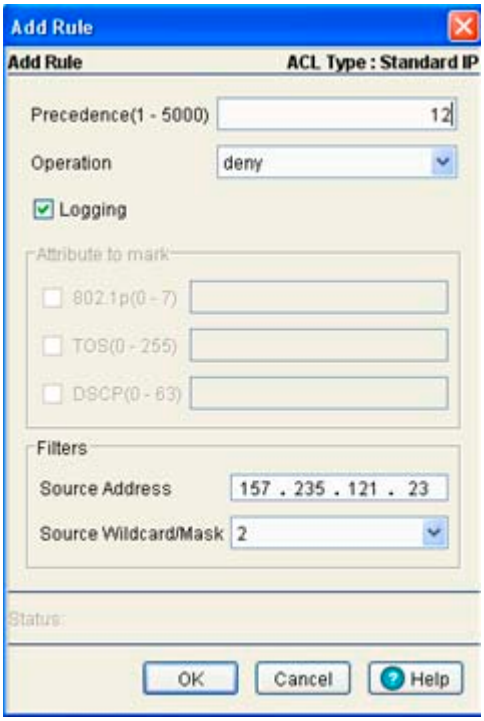
5. Select an **ACL Type** from the drop-down menu. The following options are available:
   - *Standard IP List* – Uses source IP addresses for matching operations.
   - *Extended IP List* – Uses source and destination IP addresses and optional protocol information for matching operations.
   - *MAC Extended List* – Uses source and destination MAC addresses, VLAN ID and optional protocol information.
6. Enter a numeric index name for the ACL in the **ACL ID** field.
7. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to use the changes to the running configuration and close the dialog.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.2.2 Adding a New ACL Rule

To add a new rule:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click the **ACL** tab.

4. Click the **Add** button within the Associated Rules field.



5. Use the **Precedence** field to enter a precedence (priority) value between 1 and 5000.

   The rules within an ACL will be applied to packets based on their precedence value. Rules with lower precedence are always applied first.

NOTE: If adding an access control entry to an ACL using the switch SNMP interface, **Precedence** is a required parameter.

6. Use the **Operation** drop-down menu to define a permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority.
7. Select the **Logging** checkbox to generate log messages when a packet has been forwarded, denied or marked based on the criteria specified in the access lists.
8. If **mark** is selected from within the **Operations** drop-down menu, the Attribute to mark field is enabled. Select the 802.1p (0 - 7) or TOS(0 - 255) or DSCP(0-63) checkbox and define the attribute receiving priority with this ACL mark designation.
9. From the **Filters** field, enter the **Source Address** where the packets are sourced.
10. Select a **Source Wildcard/Mask** from the drop-down menu.

    The **Source Wildcard/Mask** is the size of the network or host (in mask format). The mask length defines a match based on the Network / Host.
11. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
12. Click **OK** to use the changes to the running configuration and close the dialog.
13. Click **Cancel** to close the dialog without committing updates to the running configuration.

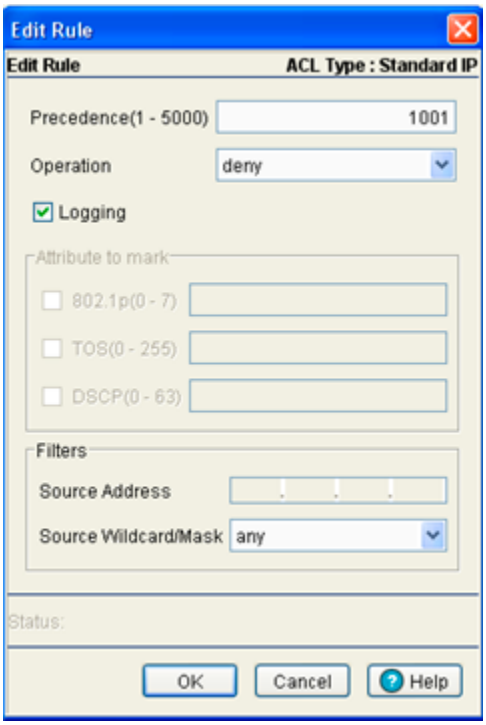
6.4.2.3 Editing an Existing Rule

As network and access permission requirements change, existing ACL rules need to be modified to be relevant with new client access requests.

To modify an existing ACL rule:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click the **ACL** tab.
4. Select an ACL from the ACLs field.

   The rules associated with the selected ACL display in the Associated Rules section.
5. Click the **Edit** button within the Associated Rules field.



6. Use the **Precedence** field to modify the precedence (priority) between 1 and 5000.

   The rules within an ACL are applied to packets based on their precedence value. Rules with lower precedence are always applied first.

NOTE: If adding an access control entry to an ACL using the switch SNMP interface, **Precedence** is a required parameter.

7. Use the **Operation** drop-down menu (if necessary) to modify the permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority.
8. Select the **Logging** checkbox to generate log messages when a packet has been forwarded, denied or marked based on the criteria specified in the access lists.
9. If mark is selected from within the **Operations** drop-down menu, the **Attribute to mark** field is enabled. Select the **802.1p (0 - 7)** or **TOS(0 - 255)** or **DSCP(0-63)** checkbox and define the attribute receiving priority with this ACL mark designation.

10.From the **Filters** field, enter the **Source Address** where the packets are sourced.

11.Select a **Source Wildcard/Mask** from the drop-down menu.

The **Source Wildcard/Mask** is the size of the network or host (in mask format). The mask length defines a match based on the Network / Host.

NOTE: If an Extended IP ACL is used, a Destination Wildcard/Mask and Destination Address are required.

12.Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

13.Click **OK** to use the changes to the running configuration and close the dialog.

14.Click **Cancel** to close the dialog without committing updates to the running configuration.

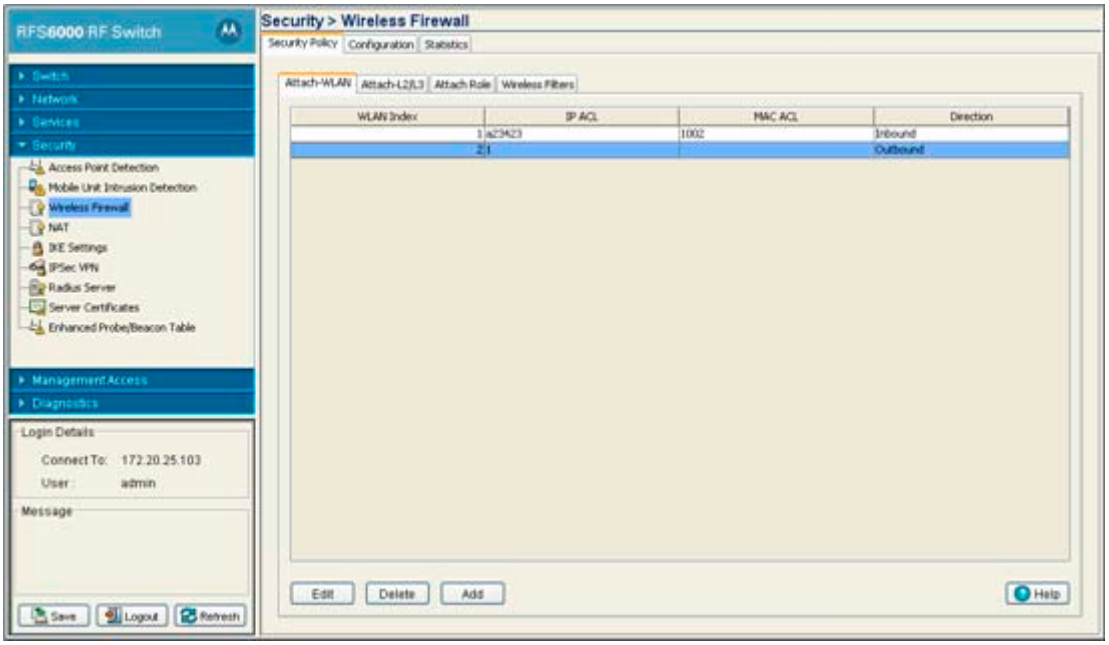
6.4.3 Attaching an ACL on a WLAN Interface/Port

Use the **Attach-WLAN** tab to view and assign an ACL to a WLAN on the switch. If a MAC ACL is being attached, create a ACL entry to allow an ARP with the least precedence.

NOTE: WLAN based ACLs allows users to enforce rules/ACLs on both the inbound and outbound direction, as opposed to Layer 2 ACLs, which just support the inbound direction.

To configure a WLAN ACL:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Select the **Security Policy** tab.
3. Select the **Attach-WLAN** tab.



4. Refer to the following information as displayed within the **Attach-WLAN** tab:

WLAN Index	Displays the list of WLANs attached with ACLs.
IP ACL	Displays the IP ACL configured.
MAC ACL	Displays the MAC ACL configured.
Direction	Displays whether the WLAN ACL is configured to work in an inbound or outbound direction.

5. Select a WLAN (by row) and click **Edit** to modify the WLAN Index, IP ACL and MAC ACL values.
6. Select a row and click the **Delete** button to delete the ACL from the list available (but not from the switch).
7. Click the **Add** button to add an ACL to a WLAN interface. For more information, see *Adding or Editing a New ACL WLAN Configuration on page 6-23*.

6.4.3.1 Adding or Editing a New ACL WLAN Configuration

After creating an ACL, it can be applied to one or more WLANs on the switch. To attach an ACL to a WLAN:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Security Policy** tab.
3. Click the **Attach-WLAN** tab.
4. Click the **Add** button to create a new ACL WLAN association or highlight an existing association and click the **Edit** button.

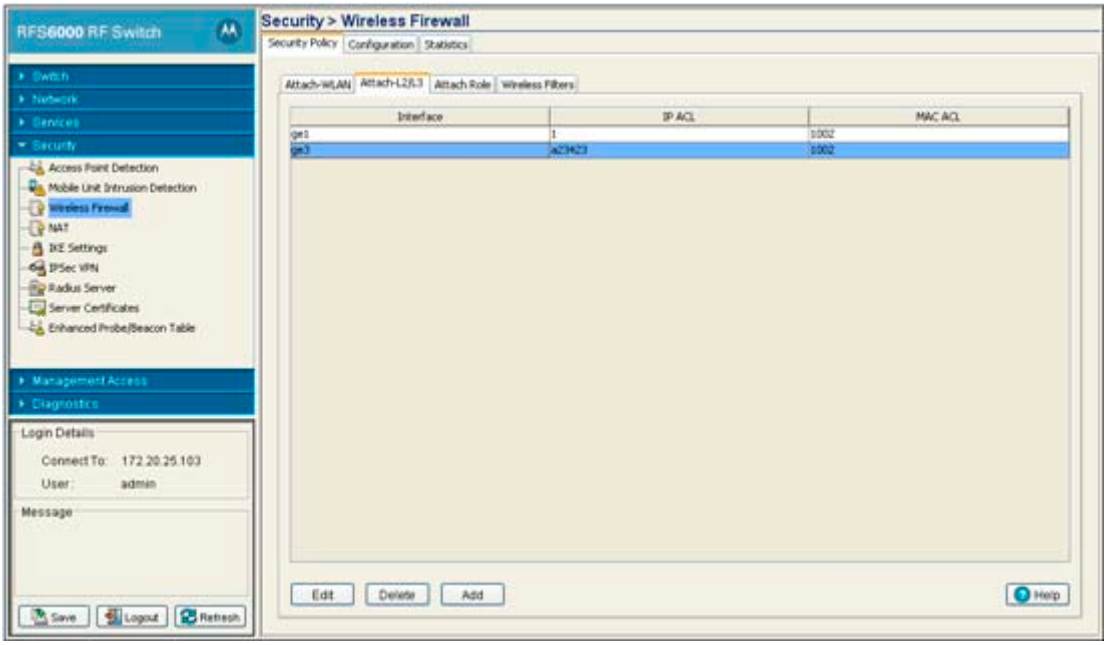
5. Define a **WLAN Index** between 1 and 32.
6. Use the **IP ACL** drop-down menu to select an IP ACL for the WLAN.
7. Use the **MAC ACL** drop-down menu to select the MAC ACL for the WLAN interface.
8. Select either the **Inbound** or **Outbound** radio button to define which direction the ACL applies.
9. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.4 Attaching an ACL Layer 2/Layer 3 Configuration

Use the **Attach-L2/L3** screen to view and assign the ACL to a physical interface or VLAN.

To attach an interface:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Security Policy** tab.
3. Click the **Attach-L2/L3** tab.



4. Refer to the following information as displayed within the Attach tab:

Interface	The interface to which the switch is configured. It can be one of the following: • *ge 1-8* • *up 1* • *vlan1* (or any additional VLANs that have been created)
IP ACL	Displays the IP ACL configured as the inbound IP for the layer 2 or layer 3 interface.
MAC ACL	Displays the MAC ACL to be configured as the MAC IP for the layer 2 interface.

5. Select an interface and click on **Edit** to modify the ACL interface, IP ACL and MAC ACL values.
6. Select an interface and click the **Delete** button to delete the interface configuration from the switch.
7. Click on **Add** button to add an physical or VLAN interface to the switch. For more information, see *Adding a New ACL Layer 2/Layer 3 Configuration on page 6-24*.

6.4.4.1 Adding a New ACL Layer 2/Layer 3 Configuration

After creating an ACL, it can be applied to one or more interfaces. On a Layer 3 interface/ Layer 2 interface, ACLs can be applied only in an inbound direction. To add an ACL interface to the switch:

1. Select **Security** > **Wireless Firewall** from the main menu tree.

2. Click the **Security Policy** tab.
3. Click the **Attach-L2/L3** tab.
4. Click the **Add** button.

5. Use the **Interface** drop-down menu to select the interface to configure on the switch. Available options include – ge 1-8, up 1, VLAN 1 (plus those VLANs created thus far) and Tunnel *n* (where *n* equals the name(s) of those tunnels created thus far).
6. Use the **IP ACL** drop-down menu to select an IP ACL used as the inbound IP for the layer 2 or layer 3 interface.
7. Use the **MAC ACL** drop-down menu to select an MAC ACL used as the MAC IP for the layer 2 interface.
8. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

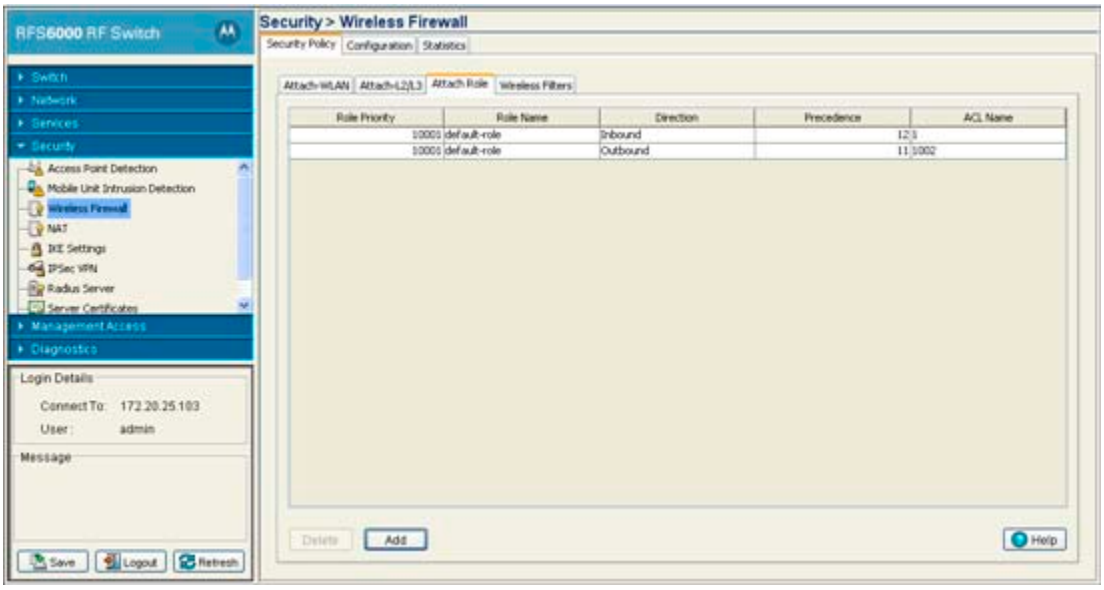
6.4.5 Configuring the Role Based Firewall

Use the **Attach Role** screen to view and assign an ACL to a role.

To attach a role:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Security Policy** tab.

3. Click the **Attach Role** tab.



4. Refer to the following information as displayed within the **Attach Role** tab:

Role Priority	Displays the priority assigned to the role as determined by the **Sequence Number** associated with the role.
Role Name	Displays the role name assigned to each role. Role names are assigned when they are added from the **Security** > **Wireless Firewall** > **Configuration** > **Role** tab.
Direction	Displays the direction which the role is associated with. The role can be associated in either the **Inbound** or **Outbound** direction.
Precedence	Displays the **ACL Precedence**. The ACL precedence range is 1-100.
ACL Name	Displays the name of the ACL associated with each role. ACLs can be configured on the ACL tab.

5. Click on **Add** button to add a new role.
6. Select an interface and click the **Delete** button to delete the interface configuration from the switch.

6.4.5.1 Creating a Role Based Firewall Rule

After creating an ACL, it can be applied to one or more Roles. On a role, acls can be applied in either an inbound or outbound direction.

To add an ACL interface to the switch:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Security Policy** tab.
3. Click the **Attach Role** tab.

4. Click the **Add** button.

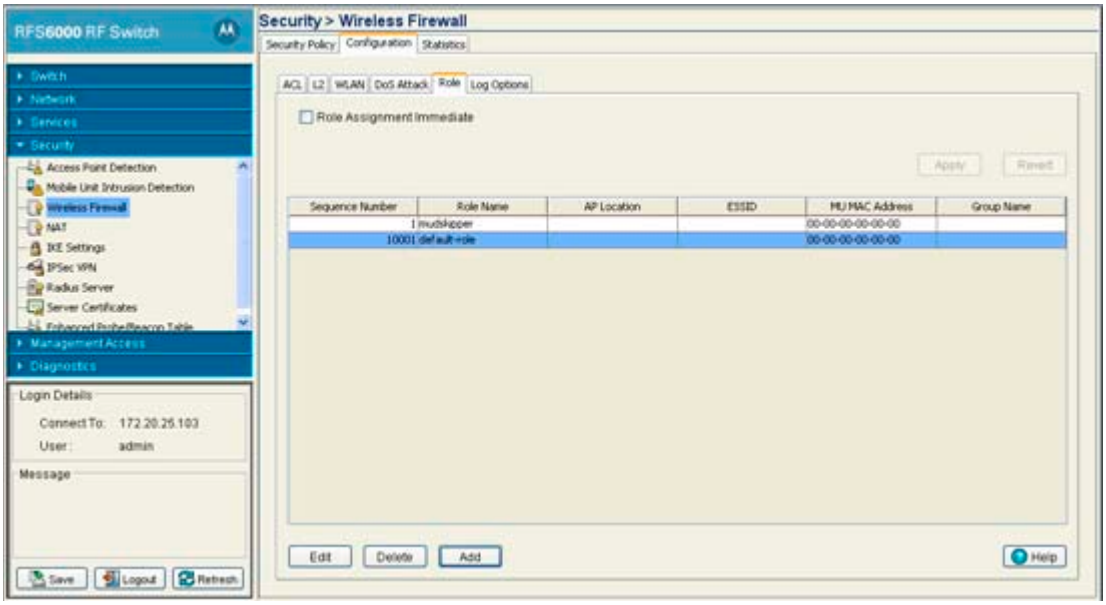
5. Select a **Role Name** from the drop-down menu. **Role Names** can be added in the **Configuration** > **Role** tab.
6. Use the **ACL** drop-down menu to select an ACL to associate with the **Role Name**.
7. Select **Inbound** or **Outbound** to apply the new role to the appropriate interface.
8. Set a **Precedence** level for the ACL. The valid range is between 1 and 100 with the lower the precedence numbers getting higher priority.
9. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.6 Configuring a Role

To view configured roles for a firewall:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.

3. Click the **Role** tab.



4. Role configuration screen displays the following information:

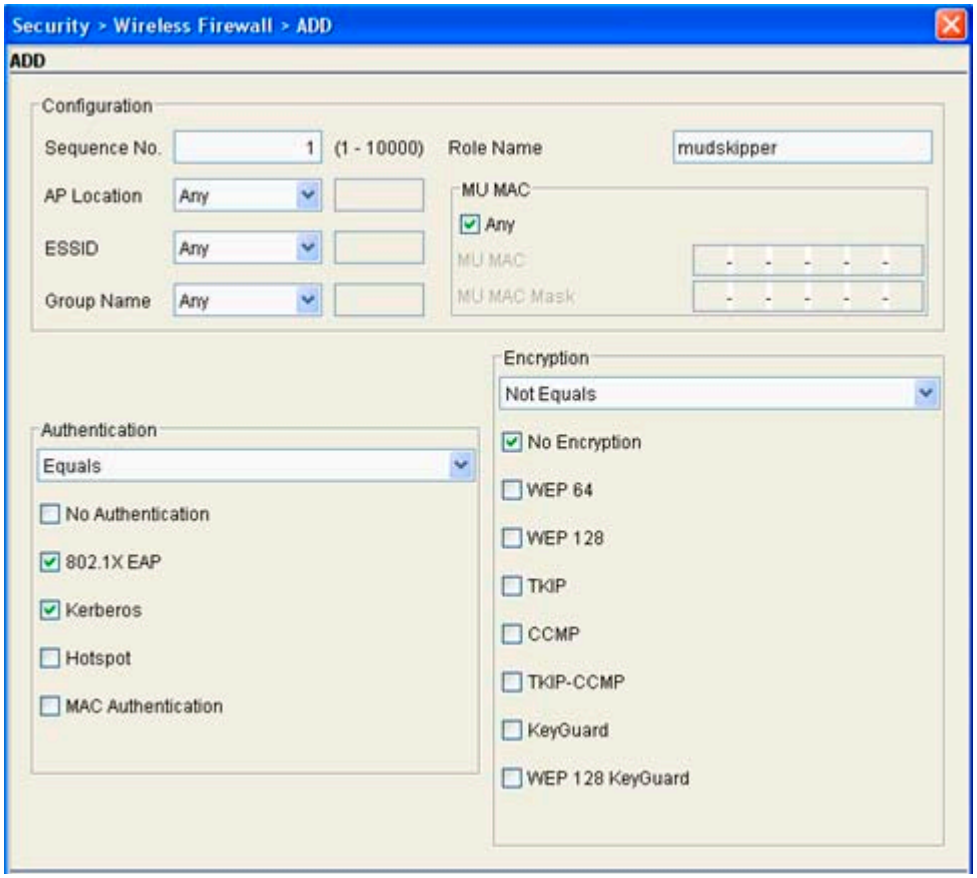
Sequence Number	Displays the sequence number associated with each role. Sequence numbers determine the order that role are applied. Roles with lower sequence numbers are applied before those with higher sequence numbers. Sequence numbers are assigned when a role is created and cannot be edited.
Role Name	Displays the name of each role. The role name is configured when the role is created and cannot be edited.
AP Location	Displays the AP Location filters, if any, applied to each role. The AP location filters can be set when the role is created or may be edited by selecting a role and clicking the **Edit** button.
ESSID	Displays the ESSID filters, if any, applied to each role. The ESSID location filters can be set when the role is created or may be edited by selecting a role and clicking the **Edit** button.
MU MAC Address	Displays the MU MAC Address filters, if any, applied to each role. The MU MAC Address filters can be set when the role is created or may be edited by selecting a role and clicking the **Edit** button.
Group Name	Displays the Radius Group name, if any, that is associated with each role.The Group Name filters can be set when the role is created or may be edited by selecting a role and clicking the **Edit** button.

5. To create a new role, click the **Add** button. For more information see *Creating a New Role on page 6-28*.
6. To edit an existing role, click the **Edit** button and modify the filter settings.
7. To remove a role, select that rule from the table and click the **Delete** button. A confirmation will be displayed before the rule is deleted from the switch.

6.4.6.1 Creating a New Role

To add new role:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click the **Role** tab.
4. Click the **Add** button.



5. To create a new role configure the following information:

Sequence Number — Enter a sequence number to be associated with each role. Sequence numbers determine the order that role are applied. Roles with lower sequence numbers are applied before those with higher sequence numbers. Sequence numbers are assigned when a role is created and cannot be edited.

Role Name — Enter a name for each role. The role name is configured when the role is created and cannot be edited.

AP Location — Select an AP Location filter, if any, to apply to the role.

Available AP Location filters are:

- *Exact*: The role will only be applied to APs with the exact location string specified in the role
- *Contains*: The role will be applied to APs whose location contains the location string specified in the role
- *Not Contains*: The role will be applied to APs whose location does not contain the location string specified in the role
- *Any*: The role will be applied to any AP Locations

ESSID	Select an ESSID filter, if any, to apply to the role. Available ESSID filters are: • *Exact*: The role will only be applied when the exact ESSID string specified in the role • *Contains*: The role will be applied when the ESSID contains the string specified in the role • *Not Contains*: The role will be applied when the ESSID does not contain the string specified in the role • *Any*: The role is applied to any ESSID
Group Name	Select a Group Name filter, if any, to apply to the role. Available Group Name filters are: • *Exact*: The role will only be applied when the exact Radius Group Name string specified in the role • *Contains*: The role will be applied when the Radius Group Name contains the string specified in the role • *Not Contains*: The role will be applied to when the Radius Group Name does not contain the string specified in the role • *Any*: The role will be applied to any Radius Group Name
MU MAC Address	Configure the MU MAC Address filters, if any, applied to each role. The MU MAC Address filter can be set to apply the role to any MU MAC Address or a specific MU MAC Address or a MU MAC Mask.
Authentication	Select an Authentication filter, if any, to apply to the role. Available Authentication filters are: • *Equals*: The role will only be applied when the Authentication type matches the exact Authentication method specified in the role • *Not Equals*: The role will only be applied when the Authentication type does not match the exact Authentication method specified in the role • *Any*: The role will be applied to any Authentication type
Encryption	Select an Encryption filter, if any, to apply to the role. Available Encryption filters are: • *Equals*: The role will only be applied when the Encryption type matches the exact Encryption method specified in the role • *Not Equals*: The role will only be applied when the Encryption type does not match the exact Encryption method specified in the role • *Any*: The role will be applied to any Encryption type

6. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to use the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

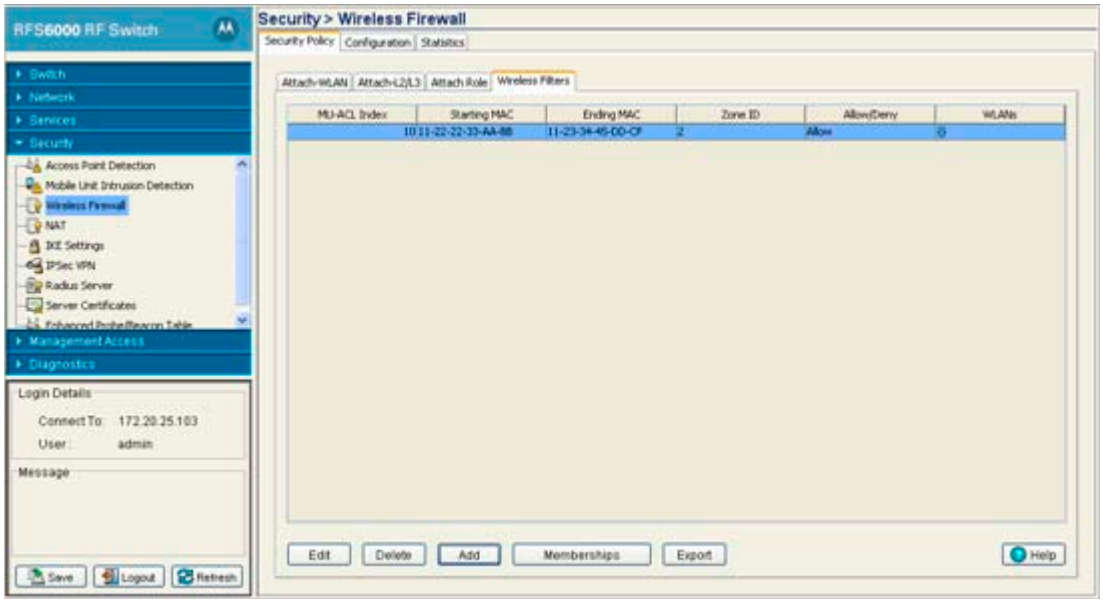
6.4.7 Configuring Wireless Filters

Use filters to either allow or deny a MAC address (or groups of MAC addresses) from associating with the switch. Refer to the **Wireless Filters** screen to review the properties of existing switch filters. A filter can

be selected from those available and edited or deleted. Additionally, a new filter can be added if an existing filter does not adequately express the MU's address range required.

To display the Wireless Filters main page:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click on the **Security Policy** tab.
3. Click on the **Wireless Filters** tab.
4. The **Wireless Filters** tab contains the following read-only information:



MU-ACL Index	Displays a numerical identifier used to associate a particular ACL to a range of MAC addresses (or a single MAC address) that are either allowed or denied access to the switch managed network.
Starting MAC	Displays the beginning MAC Address (for this specific Index) either allowed or denied access to the switch managed network.
Ending MAC	Displays the ending MAC Address (for this specific Index) either allowed or denied access to the switch managed network.
Zone ID	Displays a Zone ID associated with each Wireless Filter. Zone ID can be between 1 and 48. Zones allows you to associate firewall policies to each zone. All members of the same zone will have the same firewall policies applied to them.
Allow/Deny	States whether this particular ACL Index and MAC address range has been allowed or denied access to the switch managed network.
WLANs	Displays the WLANs associated with each Wireless Filter.

5. If the properties of an existing filter fulfill to your needs but still require modification to better filter devices, select the **Edit** button. For more information see, *Editing an Existing Wireless Filter on page 6-32*.
6. If an existing filter is now obsolete, select it from those listed and click the **Delete** button.

7. Click the **Add** button to create a new filter. For more information, see *Adding a new Wireless Filter on page 6-33*.
8. Click the **Memberships** button to display a screen wherein a selected index can be added to one or more existing WLANs. For more information see, *Associating an ACL with a WLAN on page 6-34*
9. Click on the **Export** button to export the contents of the table to a *Comma Separated Values* file (CSV).

6.4.8 Editing an Existing Wireless Filter

Use the **Edit** screen to modify the properties of an existing filter. This is recommended if an existing filter contains adequate device address information, but the allow/deny permissions need to be changed or if only minor changes are required to the starting and ending MAC addresses. If significant changes are required to a usable filter, consider creating a new one.

To edit an existing filter:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click on the **Security Policy** tab.
3. Click on the **Wireless Filters** tab.
4. Select one of the existing ACLs from the filters list.
5. Click the **Edit** button at the bottom of the screen to launch a screen for editing an ACL.

   The user can modify an ACL Index (numerical identifier) for the ACL, and edit the starting an ending MAC address range for the devices allowed or denied access to the switch managed network.

6. The **MU-ACL Index** is used as an identifier for a MAC Address range and allow/deny ACL designation. The available index range is 1 - 1000. However, the index is not editable, only its starting/ending MAC range and allow/deny designation. If a new index is needed, create a new filter.
7. Modify the existing **Starting MAC** for the target Index or leave the **Starting MAC** value as is and just modify the **Ending MAC** Address or **Allow**/**Deny** designation.
8. Modify the existing **Ending MAC** for the target Index. Enter the same Starting MAC address within the **Ending MAC** field to use only the **Starting MAC** address as either allowed or denied access to the switch managed network.

9. To associate a zone with the ACL select a **Zone ID** from the drop-down menu. Zone numbers range from 1 to 48. Creating zones allows you to associate firewall policies to each zone. All members of the same zone will have the same firewall policies applied to them. It should be set to an ID only if locationing is enabled, otherwise it should be set to *not in use*.
10. Use the drop-down menu to select **Allow** or **Deny**.

    This rule applies to MUs within the specified Starting and Ending MAC Address range. For example, if the adoption rule is to Allow, access is granted for all MUs within the specified range.
11. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
12. Click **OK** to use the changes to the running configuration and close the dialog.
13. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.9 Adding a new Wireless Filter

Use the **Add** screen to create a new index and define a new address permission range. Once created, an allow or deny designation can be applied to the new filter ACL.

To create a new filter ACL:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Select the **Security Policy** tab.
3. Select the **Wireless Filters** tab.
4. Click the **Add** button at the bottom of the screen to launch a new dialogue for creating an ACL.

   Define an Index (numerical identifier) for the ACL and the starting and ending MAC address range for devices allowed/denied access to the switch managed network.

5. Enter an Index numerical value (1 -1000) in the **MU-ACL Index** field.

   The MU-ACL Index is a numerical identifier used to associate a particular ACL to a range of MAC addresses (or a single MAC address) either allowed or denied access to the switch managed network. Enter a new Index to define a new MAC Address range and allow/deny ACL Index designation.
6. Enter the a hex value for the **Starting MAC** address.

   This is the beginning MAC address either allowed or denied access to the switch managed network.

7. Enter the a hex value for the **Ending MAC** address. Enter the same Starting MAC address within the **Ending MAC** field to use only the **Starting MAC** address as either allowed or denied access to the switch managed network.
8. To modify the zone associated with the ACL select a **Zone ID** from the drop-down menu. Zone numbers range from 1 to 48. Creating zones allows you to associate firewall policies to each zone. All members of the same zone will have the same firewall policies applied to them.
9. Use the drop-down menu to select **Allow** or **Deny**.

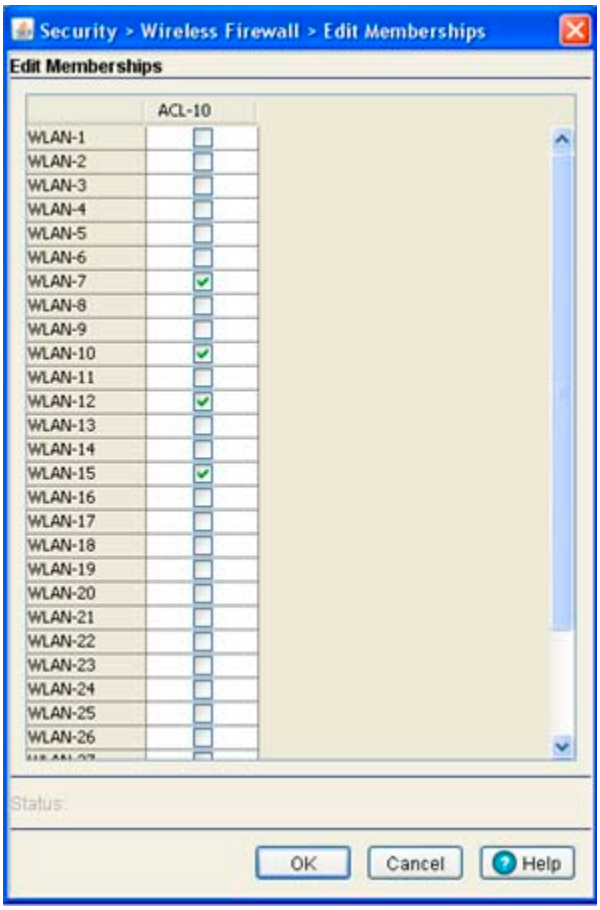
   This rule applies to MUs within the specified Starting and Ending MAC Address range. For example, if the adoption rule is to Allow, access is granted for all MUs within the specified range.
10. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
11. Click **OK** to use the changes to the running configuration and close the dialog.
12. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.10 Associating an ACL with a WLAN

Use the **Membership** screen to define a name for the ACL index and map the index to WLANs (1-32) requiring membership permission restrictions.

To associate a filter ACL index with a WLAN:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Security Policy** tab.
3. Click the **Wireless Filters** tab.
4. Select one or more of the existing ACLs from the filters list.
5. Click the **Memberships** button.



6. Select the box to the right of each WLAN you want associated with the ACL.

   Selecting a WLAN maps it the MAC address range and allow or deny designation assigned to it. Consequently, be sure you are not restricting MU traffic for a WLAN that requires those MAC addresses to interact with the switch.

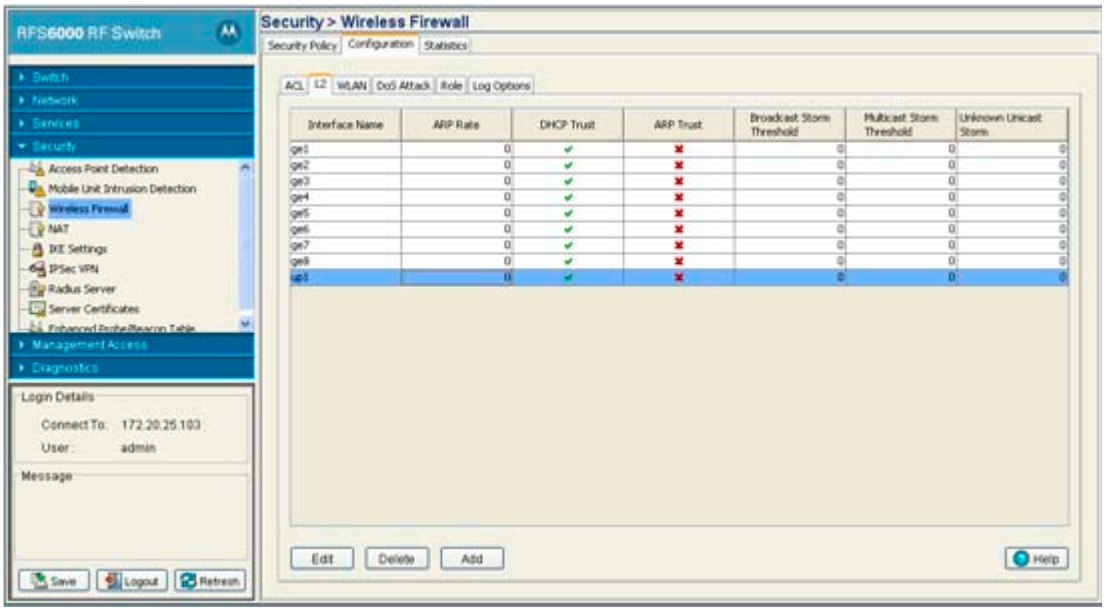
7. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to use the changes to the running configuration and close the dialog.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.11 L2 Level Attack Detection and Mitigation

To review Layer 2 firewall rules:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Select the **Configuration** tab.
3. Click the **L2** tab.

4. The **L2** tab contains the following information:



Interface Name — Displays the interface associated with the Layer 2 firewall. Available Layer 2 interfaces are ge 1-8 and up1.

ARP Rate — Displays the *Address Resolution Protocol* (ARP) rate. Rates can be between 1 and 1000000

DHCP Trust — Displays whether or not the DHCP servers configured on the switch are trusted by the Layer 2 firewall. If DHCP is trusted, DHCP traffic will not be subjected to the Layer 2 firewall rules. When the DHCP servers is trusted a green checkmark will be displayed. When the DHCP servers are not trusted a red "X" will be displayed.

ARP Trust — Displays whether or not the ARP is trusted by the Layer 2 firewall. If ARP is trusted, ARP traffic will not be subjected to the Layer 2 firewall rules. When the ARP interface is trusted a green checkmark will be displayed. When the ARP interface is not trusted a red "X" will be displayed.

Broadcast Storm Threshold — Displays the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

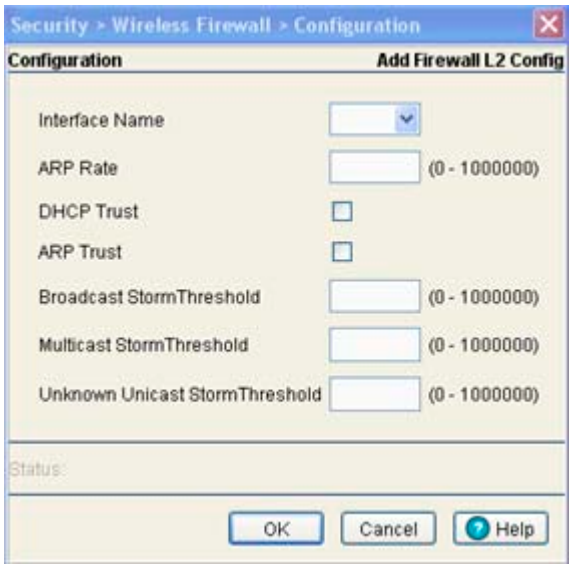
Multicast Storm Threshold — Displays the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

Unknown Unicast Storm — Displays the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

6.4.11.1 Port Level Configuration

To configure new Layer 2 firewall rules:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click the **L2** tab.
4. Click the **Add** button.



5. Configure the following values for each new Layer 2 configuration:

Interface Name	Assign the interface to be associated with the Layer 2 firewall. Available Layer 2 interfaces are ge 1-8 and up1.
ARP Rate	Specify the *Address Resolution Protocol* (ARP) rate. Rates can be between 1 and 1000000.
DHCP Trust	Configure whether or not the DHCP Servers connected to the switch are trusted by the Layer 2 Firewall. To set DHCP as trusted, check the box marked **DHCP Trust**.
ARP Trust	Configure whether or not the ARP is trusted by the Layer 2 firewall. If ARP is trusted, ARP traffic will not be subjected to the Layer 2 firewall rules. To set ARP as trusted, check the box marked **ARP Trust**.
Broadcast Storm Threshold	Configure the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

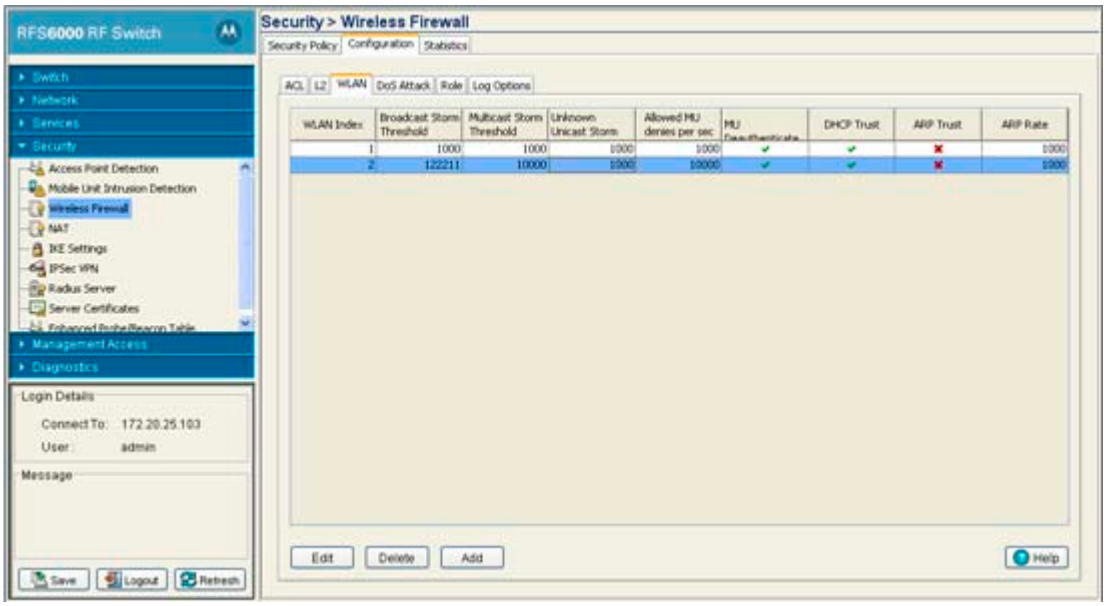
Multicast Storm Threshold	Configure the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.
Unknown Unicast Storm	Configure the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

6. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to use the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.12 Configuring WLAN Firewall Rules

To review WLAN firewall rules:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click the **WLAN** tab.
4. The **WLAN** tab contains the following information:



WLAN Index — Displays the WLAN index number. This number is configured on the wireless LAN configuration page.

Broadcast Storm Threshold — Displays the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.

Multicast Storm Threshold — Displays the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.

Unknown Unicast Storm — Displays the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.

Allowed MU denies per sec — Displays the permissible number of denied packets per second that a mobile unit on this WLAN may send before it is deauthenticated. The threshold range is 0-1000000 packets per second.

MU Deauthenticate — Displays whether or not mobile unit deauthentication is enabled for each WLAN. If **MU Deauthenticate** is enabled any associated mobile unit which hit the thresholds configured for Allowed MU denies per second will be deauthenticated. If MU Deauthenticate is enabled a green checkmark will be displayed. When it is disabled a red "X" will be displayed.

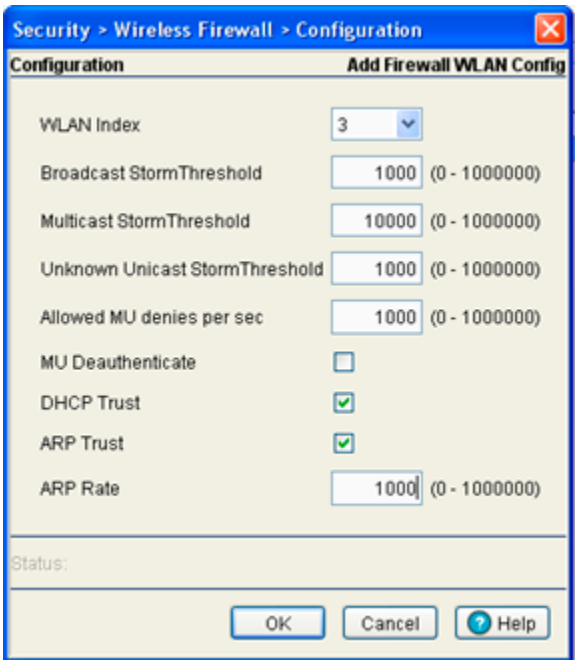
DHCP Trust	Displays whether the Interface is DHCP trusted or not, If the interface is DHCP trusted then the DHCP Request will forward to the External DHCP Server otherwise it will not. Always the Internal DHCP servers are trusted in nature. When ever the interface is DHCP trusted, then it is marked as GREEN and if it not DHCP trusted it will mark in RED "X".
ARP Trust	Displays whether or not the ARP is trusted by the Layer 2 firewall. If ARP is trusted, ARP traffic will not be subjected to the Layer 2 firewall rules. When the ARP interface is trusted a green checkmark will be displayed. When the ARP interface is not trusted a red "X" will be displayed.
ARP Rate	Displays the ARP rate threshold. The ARP threshold determines the number of ARP packets permissible per second. Rates can be between 0 and 1000000

5. If the properties of an existing WLAN firewall setting fulfill to your needs but still require modification to better filter traffic, select the WLAN and click the **Edit** button.
6. If an existing WLAN firewall rule is now obsolete, select it from those listed and click the **Delete** button.
7. Click the **Add** button to create a new WLAN firewall rule. For more information, see *WLAN Level Configuration on page 6-40*.

6.4.12.1 WLAN Level Configuration

To add new WLAN firewall rules:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click the **WLAN** tab.
4. Click the **Add** button.



5. To create a new WLAN Firewall rule configure the following information:

WLAN Index	Select a WLAN index number from the drop-down menu. This number is configured on the wireless LAN configuration page.
Broadcast Storm Threshold	Enter the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The valid threshold range is 0-1000000 packets per second.
Multicast Storm Threshold	Enter the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The valid threshold range is 0-1000000 packets per second.
Unknown Unicast Storm	Enter the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.
Allowed MU denies per sec	Configure the permissible number of denied packets per second that a mobile unit on this WLAN may send before it is deauthenticated. The threshold range is 0-1000000 packets per second.
MU Deauthenticate	Configure whether or not mobile unit deauthentication is enabled for each WLAN. If **MU Deauthenticate** is enabled any associated mobile unit which hit the thresholds configured for storm traffic will be deauthenticated. To enable deauthentication, check the box.
DHCP Trust	Displays whether the Interface is DHCP trusted or not, If the interface is DHCP trusted then the DHCP Request will forward to the External DHCP Server otherwise it will not. Always the Internal DHCP servers are trusted in nature. When ever the interface is DHCP trusted, then it is marked as GREEN and if it not DHCP trusted it will mark in RED "X". To enable DHCP trust, check the box.
ARP Trust	Configure whether or not ARP is trusted by the Layer 2 firewall. If ARP is trusted, ARP traffic is not subjected to Layer 2 firewall rules. To enable ARP trust, check the box.
ARP Rate	Enter the ARP threshold.The ARP threshold determines the number of ARP packets permissible per second. Rates can be between 0 and 1000000

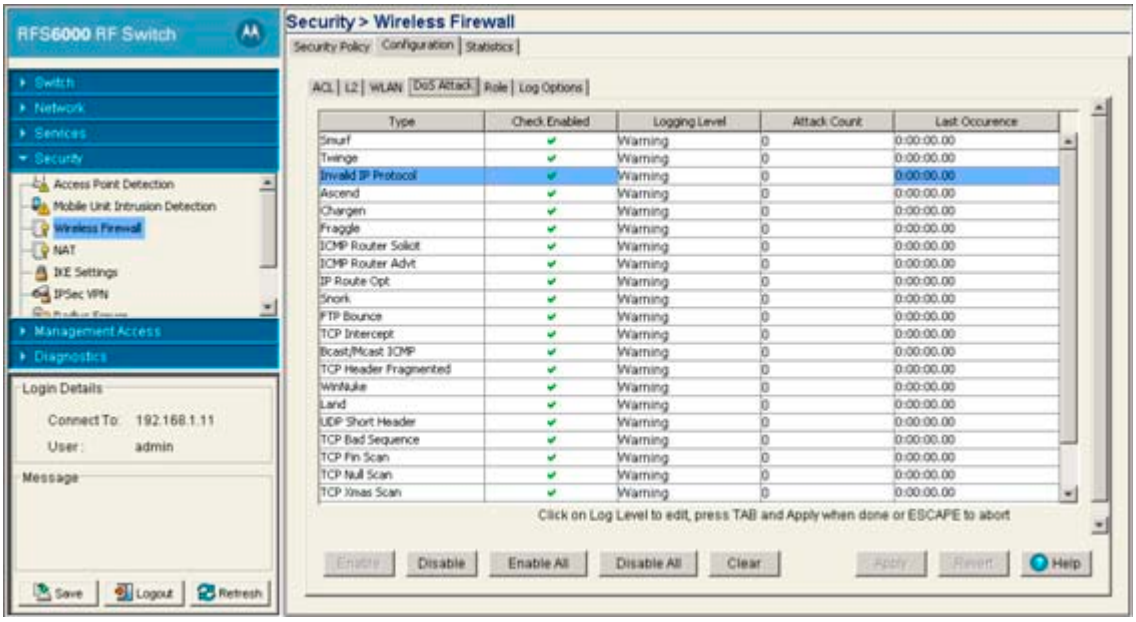
6. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to use the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.4.13 Configuring Denial of Service (DoS) Attack Firewall Rules

To review Denial of Service Attack firewall rules:

1. Select **Security** > **Wireless Firewall** from the main tree menu.

2. Click the **Configuration** tab.
3. Click the **DoS Attack** tab.
4. The **DoS Attack** tab contains the following information:



Type — Displays the Denial of Service attack type. The switch currently supports enabling or disabling 28 types of DoS attack filters.

Check Enabled — This field will show a green checkmark next to the Denial of Service Attack filters that are enabled on the switch firewall. When a DoS Attack filter is disabled a red "X" will be shown in this column.

Logging Level — The Logging Level field displays the level of Syslog logging enabled for each DoS Attack filter. The logging level uses standard Syslog levels of:

- *Emergency*
- *Alert*
- *Critical*
- *Error*
- *Warning*
- *Notice*
- *Info*
- *Debug*
- *None*

To change the logging level, click on the specific field and choose the logging level from the drop-down menu.

Attack Count	Displays the number of times that each DoS attack have been observed by the switch firewall. Clicking the **Clear Stats** button on this page will reset all **Attack Counts** to 0.
Last Occurrence	Displays the amount of time since each DoS attack has been observed by the switch firewall. Clicking the **Clear Stats** button on this page will reset all **Last Occurrence** timers to 0:00:00.00.

5. To enable a Denial of Service Attack filter, select a disabled rule from the table and click the **Enable** button.The **Check Enabled** field will show a green checkmark next to the Denial of Service Attack filters that are enabled on the switch firewall.
6. To disable a Denial of Service Attack filter, select an enabled rule from the table and click the **Disable** button. When a DoS Attack filter is disabled a red "X" will be shown in the **Check Enabled** column.

NOTE: Of the 28 DoS Attack filters supported by the switch, 10 can be disabled individually. Those filters are:

- *Smurf*
- *Twinge*
- *Invalid IP protocol*
- *ICMP router advertisement*
- *Src ip route*
- *Echo ports*
- *Snork*
- *FTP bounce*
- *TCP intercept*
- *Bcast Mcast ICMP*

7. To enable all Denial of Service Attack filters, click on the **Enable All** button.The **Check Enabled** field will show a green checkmark next to the Denial of Service Attack filters that are enabled on the switch firewall.
8. To disable all Denial of Service Attack filters, click on the **Disable All** button. When a DoS Attack filter is disabled a red "X" will be shown in the **Check Enabled** column.
9. To clear statistics for Denial of Service Attacks, click the **Clear** button. This will reset all **Attack Counts** to 0 and all **Last Occurrence** times to 0:00:00.00.
10. Click the **Apply** button to save the changes made within the DoS Attach screen.
11. Click the **Revert** button to cancel any changes made within the DoS Attach screen and revert back to the last saved configuration.

6.4.14 Configuring Firewall Logging Options

To view firewall logging rules:

1. Select **Security** > **Wireless Firewall** from the main tree menu.
2. Click the **Configuration** tab.
3. Click the **Log Options** tab.

4. Select the Syslog logging levels for each of the following log types:

ARP Log

The **ARP Log** field displays the level of Syslog logging enabled for excessive ARP on an interface. The logging level uses standard Syslog levels of:

- *Emergency*
- *Alert*
- *Critical*
- *Error*
- *Warning*
- *Notice*
- *Info*
- *Debug*
- *None*

To change the logging level, click on the specific field and choose the logging level from the drop-down menu.

Broadcast Log

The **Broadcast Log** field displays the level of syslog logging enabled for excessive broadcasts on an interface. The logging level uses the same standard Syslog levels.

To change the logging level, click on the specific field and choose the logging level from the drop-down menu.

Multicast Log	The **Multicast Log** field displays the level of syslog logging enabled for excessive multicast on an interface. The logging level uses the same standard Syslog levels. To change the logging level, click on the specific field and choose the logging level from the drop-down menu.
Unknown Unicast Log	The **Unknown Unicast Log** field displays the level of syslog logging enabled for excessive unknown unicasts on an interface. The logging level uses the same standard Syslog levels. To change the logging level, click on the specific field and choose the logging level from the drop-down menu.

5. When all logging options have been modified, click the **Apply** button to commit those changes to the switch.
6. To undo any changes and go back to the previously saved logging options, click the **Revert** button.

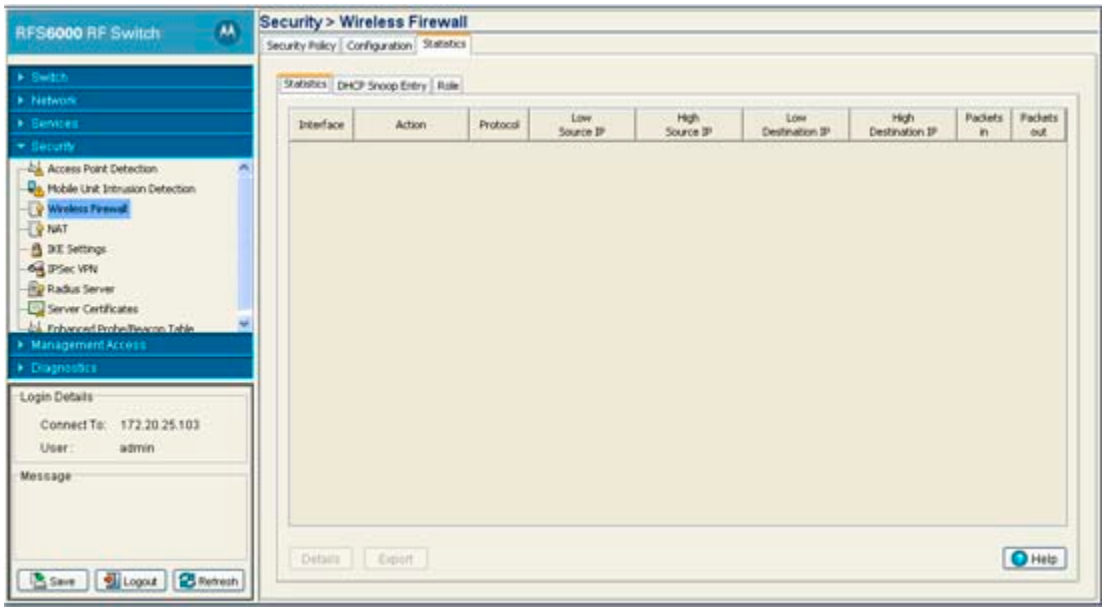
6.4.15 Reviewing Firewall and ACL Statistics

Use the **Statistics** tab to view set of statistics for **ACL**, **DHCP Snoop Entry** and **Role** based firewalls.

6.4.15.1 Reviewing ACL Statistics

To review ACL statistics:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Statistics** tab.
3. From the **Statistics** section select the **Statistics** tab.



4. Refer to the following information as displayed within the **Statistics** tab:

Interface	Interface displays the physical/virtual interfaces used to add the ACL association to the switch.
Action	Displays the permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority.

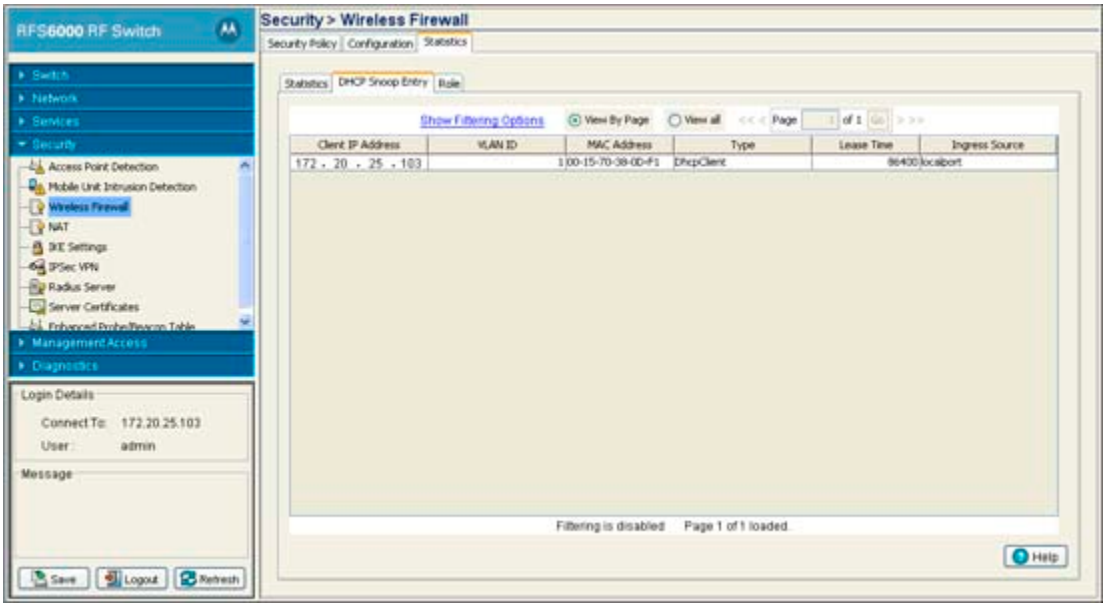
Protocol	Displays the permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority or *type of service*.
Low Source IP	Displays the Low Source IP Address from where the packets are sourced.
High Source IP	Displays the High Source (highest address in available range) IP Address from where the packets are sourced.
Low Destination IP	Displays the Low Destination (lowest address in available range) IP Address.
High Destination IP	Displays the High Destination IP Address.
Packets In	Displays the number of packets (in bytes) transmitted over the ACL.
Packets Out	Displays the number of instances this ACL has been used. Periodically review to determine whether specific ACLs should be deleted or modified to make relevant.

5. Select an interface and click the **Details** button to display a more robust set of statistics for the selected interface.
6. Click the **Export** to export the selected ACL attribute to a user specified location.

6.4.15.2 Viewing DHCP Snoop Entry Statistics

To review DHCP Snoop Entry statistics:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Statistics** tab.
3. Select the **DHCP Snoop Entry** tab.



4. Refer to the following information as displayed within the **DHCP Snoop Entry** tab:

Client IP Address	Displays the DHCP Client IP Address for each entry.
VLAN ID	Displays the VLAN ID number, if any, for each entry in the DHCP Snoop Entry table.

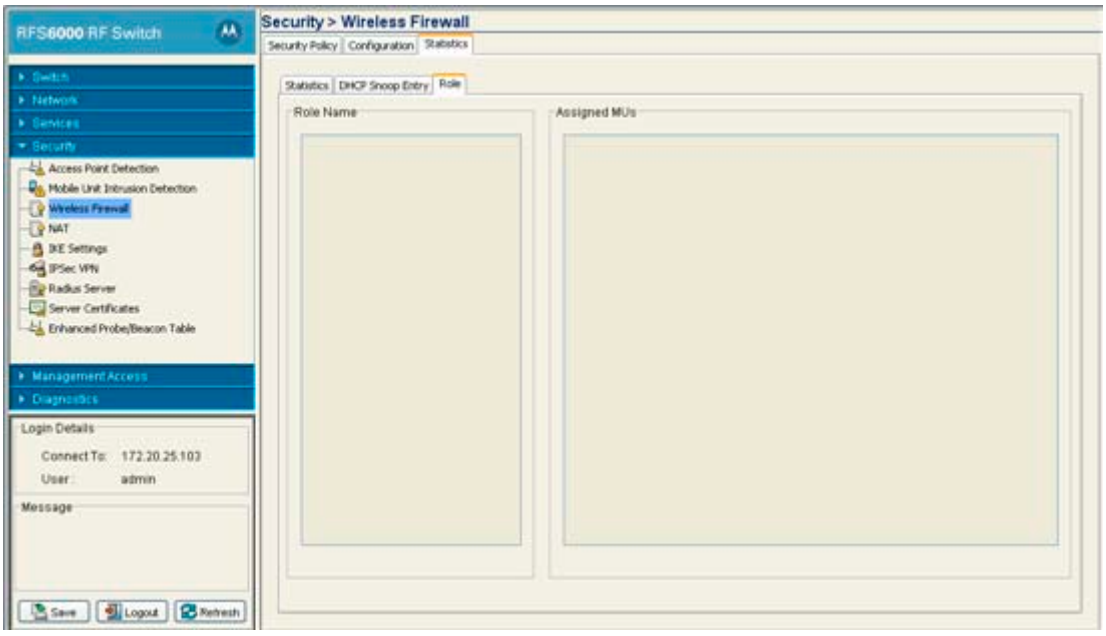
MAC Address	Displays the MAC Address of each DHCP Client, DHCP Server or Router in the table.
Type	Displays the type for each DHCP Snoop Entry. Available entry types include: • *DHCP Client* • *DHCP Server* • *Router* • *DHCP Server Router* • *DHCP Client Router*
Lease Time	Displays the DHCP remaining Lease Time for each entry in the table.
Ingress Source	Displays the MU port number for each entry in the table.

6.4.15.3 Viewing Role Based Firewall Statistics

The Role Based Firewall statistics information displays a list of mobile units associated with each role name.

To review Role Based Firewall statistics:

1. Select **Security** > **Wireless Firewall** from the main menu tree.
2. Click the **Statistics** tab.
3. From the **Statistics** section select the **Role** tab.



4. Refer to the following information as displayed within the **Role** tab:

Role Name	Displays the **Role Names** for all roles that are active and have mobile units associated with them.
Assigned MUs	Clicking on a **Role Name** will display all mobile units that are associated with the selected role.

6.5 Configuring NAT Information

Network Address Translation NAT provides the translation of an *Internet Protocol* (IP) address within one network to a different, known IP address within another network. One network is designated as the private network, while the other is public. NAT provides a layer of security by translating private (local) network addresses to one or more public IP addresses. For example, when an administrator wants to allow individuals on the WAN side access to a particular FTP or Web server located on one of the LAN subnets but does not want to permit any other access, NAT is the appropriate solution.

Using NAT, a user can mark one or more interfaces as inside or outside. When a user creates a NAT rule for inside or outside application, it is applied on all the interfaces marked as inside or outside respectively. NAT operates on the switch to connect two networks together. An inside network is assigned addresses requiring conversion into valid addresses before packets can be forwarded to an outside network. The translation process operates in parallel with packet routing.

NAT enables network administrators to move a Web or FTP Server to another host without having to troubleshoot broken links. Change the inbound mapping with the new inside local address to reflect the new host. Configure changes to your internal network seemlessly since the only external IP address either belongs to the switch or from a pool of global addresses.

The switch NAT configuration process is divided into the following configuration activities:

- *Defining Dynamic NAT Translations*
- *Defining Static NAT Translations*
- *Configuring NAT Interfaces*
- *Viewing NAT Status*

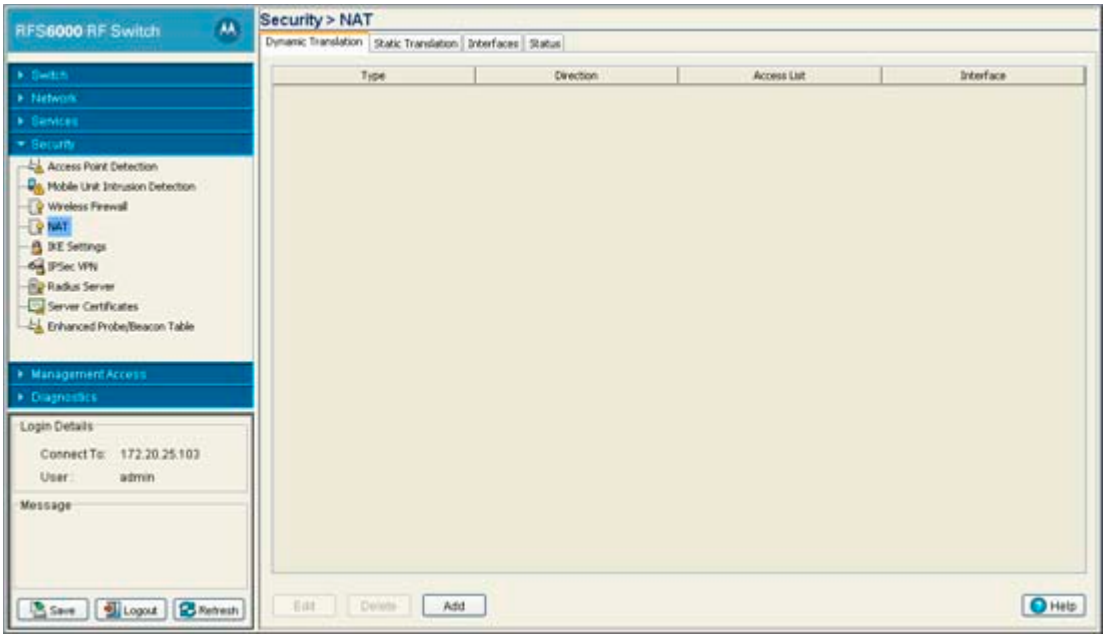
6.5.1 Defining Dynamic NAT Translations

Dynamic NAT translates the IP address of packets going out from one interface to another interface based on the conditions configured in the list. Dynamic NAT requires packets to be switched through the NAT router to generate translations in the switch translation table.

Refer to the NAT screen's **Dynamic Translation** tab to view existing dynamic NAT configurations available to switch.

To view and add/edit a dynamic NAT configuration:

1. Select **Security** > **NAT** from the main menu tree.
2. Click on the **Dynamic Translation** tab.



3. Refer to the following information as displayed within the **Dynamic Translation** tab.

Type	Displays the NAT type as either: • *Inside* - Applies NAT on packets arriving on interfaces marked as inside. These interfaces should be private networks not accessible from outside (public) networks. • *Outside* - Applies NAT on packets coming in on interfaces marked as outside. These switch interfaces should be public or outside networks accessible from anywhere on the Internet.
Direction	Displays the direction as either: • *Source* - 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. • *Destination* - Packets passing through the NAT on the way back to the switch managed LAN are searched against 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 switch managed network.
Access List	Defines the packet selection criteria for NAT. NAT is applied only on packets which match a rule defined in the access-list. Only the Standard IP and Extended IP Access List can be used.
Interface	Defines the interface through which packets are routed. The source IP address and source port number (only if IP protocol is TCP or UDP) of packets is changed to the interface IP address and a random port number.

4. Select an existing NAT configuration and click the **Edit** button to modify the settings of this existing NAT configuration. The fields within the Edit screen are similar to those displayed when adding a new NAT configuration.
5. Select an existing NAT configuration and click the **Delete** button to remove it from the list of available configurations.

6. Click the **Add** button to display a screen to create a new NAT configuration and add it to the list of available configurations. For more information, see *Adding a New Dynamic NAT Configuration on page 6-50*.

6.5.1.1 Adding a New Dynamic NAT Configuration

If the existing NAT configurations displayed with the Configuration prove unsuitable for translation, consider creating a new one.

To define a new NAT configuration:

1. Select **Security** > **NAT** from the main menu tree.
2. Click on the **Dynamic Translation** tab.
3. Click the **Add** button.

4. Define the NAT **Type** from the drop-down menu. Options include:
   - *Inside* - The set of networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world.
   - *Outside* - All other addresses. Usually these are valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network.
5. Define the NAT **Direction** from the drop-down menu. Options include:
   - *Source* - 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.
   - *Destination* - Packets passing through the NAT on the way back to the switch managed LAN are searched against to 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 switch managed network.
6. Use the **Access List** drop-down menu to select the list of addresses used during NAT translation. These addresses (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination
7. Use the **Interface** drop-down menu to select the VLAN 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.
8. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel** to close the dialog without committing updates to the running configuration.

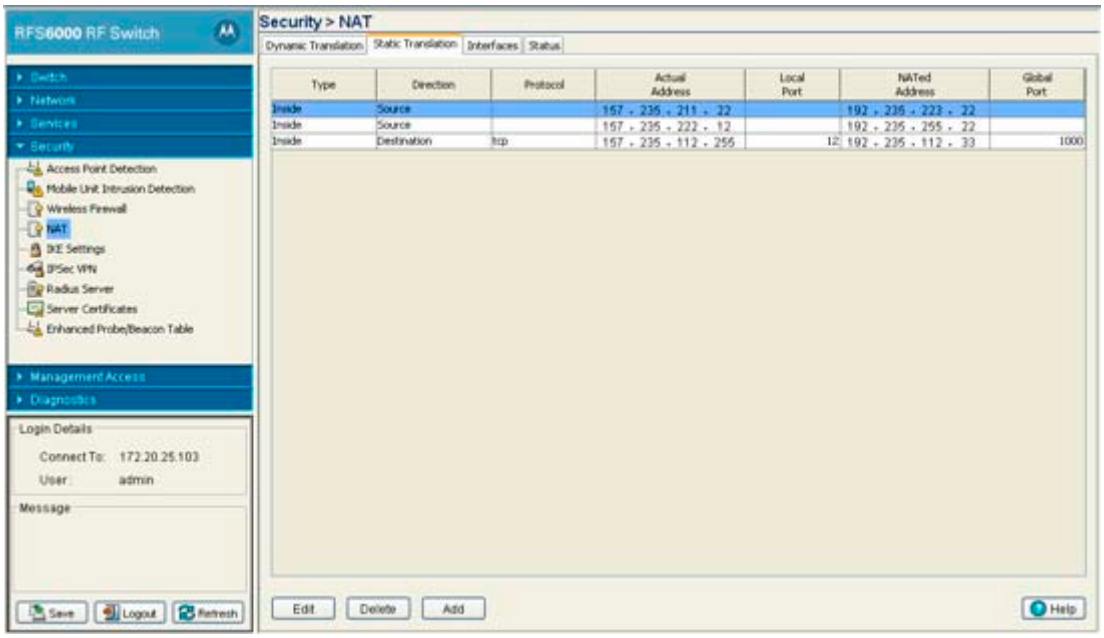
6.5.2 Defining Static NAT Translations

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.

Refer to the NAT screen's **Static Translation** tab to view existing static NAT configurations available to switch.

To view and add/edit a dynamic NAT configuration:

1. Select **Security** > **NAT** from the main menu tree.
2. Click the **Static Translation** tab.



3. Refer to the following information as displayed within the **Static Translation** tab.

Type	Displays the NAT type as either: • *Inside* - The set of networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world. • *Outside* - All other addresses. Usually valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network.
Direction	Displays the Direction as either: • *Source* - 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. • *Destination* - Packets passing through the NAT on the way back to the switch managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address to reach the LAN over the switch managed network.
Protocol	Displays the tcp or udp option selected for use with the static translation.
Actual Address	Displays 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.
Local Port	Applies NAT on packets matching the specified port number. The port number matched can be either source or destination based on the direction specified. This option is valid only if the direction specified is **destination**.
NATed Address	Modifies 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.
Global Port	Modifies the port number of the matching packet to the specified value. This option is valid only if the direction specified is **destination.**

4. Select an existing NAT configuration and click the **Edit** button to display screen to modify the settings of this existing NAT configuration. The fields within the Edit screen are similar to those displayed when adding a new NAT configuration.
5. Select an existing NAT configuration and click the **Delete** button to remove it from the list of available configurations displayed.
6. Click the **Add** button to display screen to create a new NAT configuration and add it to the list of available configurations. For more information, see *Adding a New Dynamic NAT Configuration on page 6-50*.

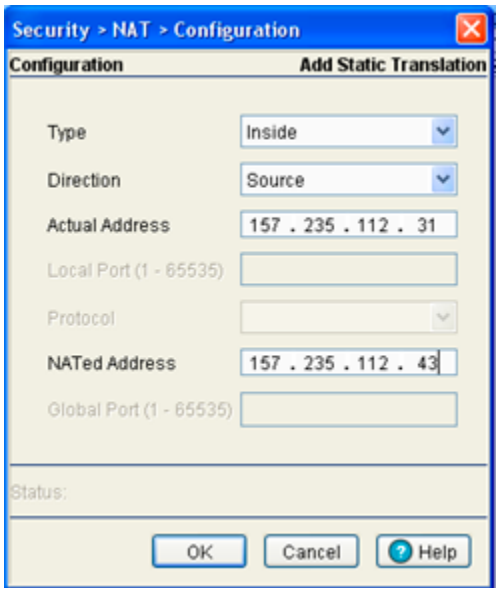
6.5.2.1 Adding a New Static NAT Configuration

If existing NAT configurations prove unsuitable for translation, consider creating a new one.

To define a new NAT configuration:

1. Select **Security** > **NAT** from the main menu tree.
2. Click on the **Static Translation** tab.

3. Click the **Add** button.



4. Define the NAT **Type** from the drop-down menu. Options include:
   - *Inside* - The set of networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world.
   - *Outside* - All other addresses (usually valid addresses located on the Internet). Outside addresses pose no risk if exposed over a publicly accessible network.
5. Define the NAT **Direction** from the drop-down menu. Options include:
   - Source - 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.
   - Destination - Packets passing through the NAT on the way back to the switch managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address to reach the LAN over the switch managed network.
6. Enter the **Actual Address** used at the local (source) end of the 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.
7. Enter the **Local Port (1 - 65535)** used to for the translation between the switch and its NAT destination.
8. Use the **Protocol** drop-down menu to select either **TCP** or **UDP** as the protocol

NOTE: After selecting (and saving) a protocol type of TCP or UDP (using the Web UI), the switch CLI will not display the selected protocol type or provide an option to configure it. Ensure both the protocol and port are defined using the Web UI.

9. Enter the **Global Address** to assign to a host in the outside network. This should be interpreted as a secure address.
10. Displays the **Global Port** used to for the translation between the switch and its NAT destination.
11. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something is wrong in the transaction between the applet and the switch.
12. Click **OK** to use the changes to the running configuration and close the dialog.

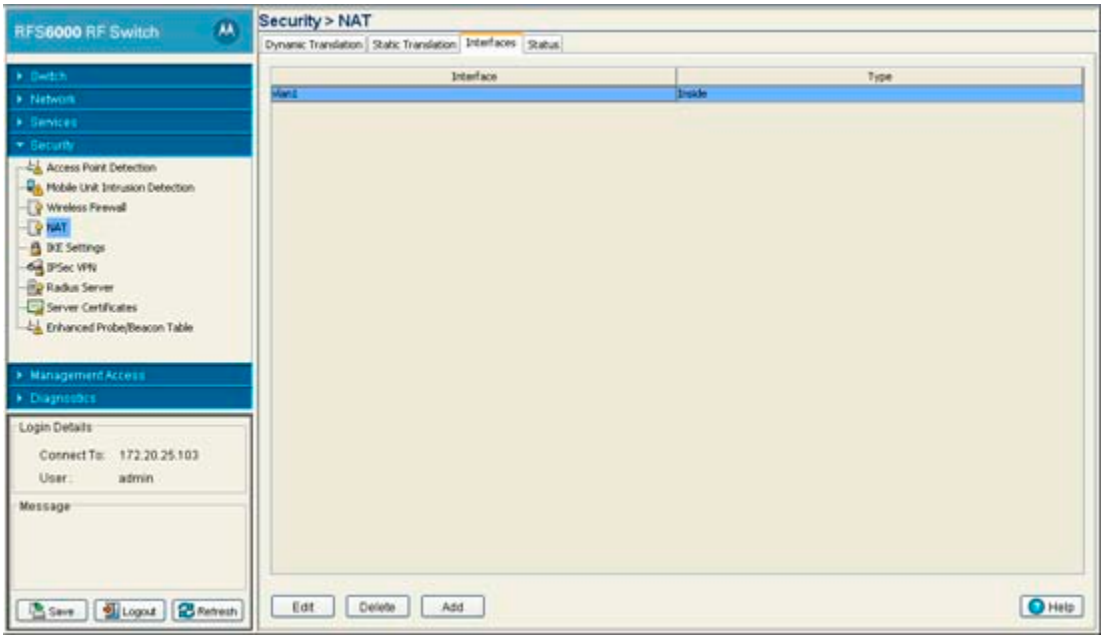
13.Click **Cancel** to close the dialog without committing updates to the running configuration.

6.5.3 Configuring NAT Interfaces

The NAT Interface is the VLAN used to route switch data traffic between the source and destination address locations within the switch-managed network. Any of the default VLANs is available as the NAT interface, in addition to any other VLANs created. In addition to selecting the VLAN, specify the Inside or Outside NAT type.

To view and configure a NAT interface:

1. Select **Security** > **NAT** from the main menu tree.
2. Click on the **Interfaces** tab.



3. Refer to the following information as displayed within the **Interface** tab:

Interface	Displays the VLAN used as the inside or outside NAT type. All defined VLANs are available from the drop-down menu for use as the interface.
Type	Displays the NAT type as either: • *Inside* - The set of switch-managed networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world. • *Outside* - All other addresses. Usually these are valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network.

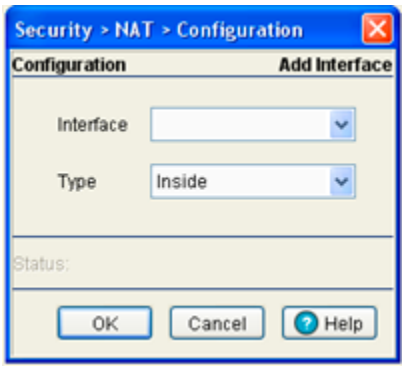
4. To Edit an existing interface, select it from the list of available interfaces and click the **Edit** button.

   An Edit Interface screen displays allowing the user to modify the VLAN and interface type (inside or outside).

5. If an interface is obsolete or of no use to the NAT translation process, select it and click the **Delete** button to remove it from the list of interfaces available

6. If modifying an existing interface is not a valid option, consider configuring a new interface. To define a new NAT interface:

   a. Click the **Add** button from within the Interfaces tab.



   b. Use the **Interface** drop-down menu to select the VLAN used as the communication medium between the switch managed network and its destination (within the insecure outside world).

   c. Use the **Type** drop-down menu to specific the Inside or Outside designation as follows:

   - *Inside* - The set of switch-managed networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world.
   - *Outside* - All other addresses. Usually these are valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network.

   d. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

   e. Click **OK** to use the changes to the running configuration and close the dialog.

   f. Click **Cancel** to close the dialog without committing updates to the running configuration.

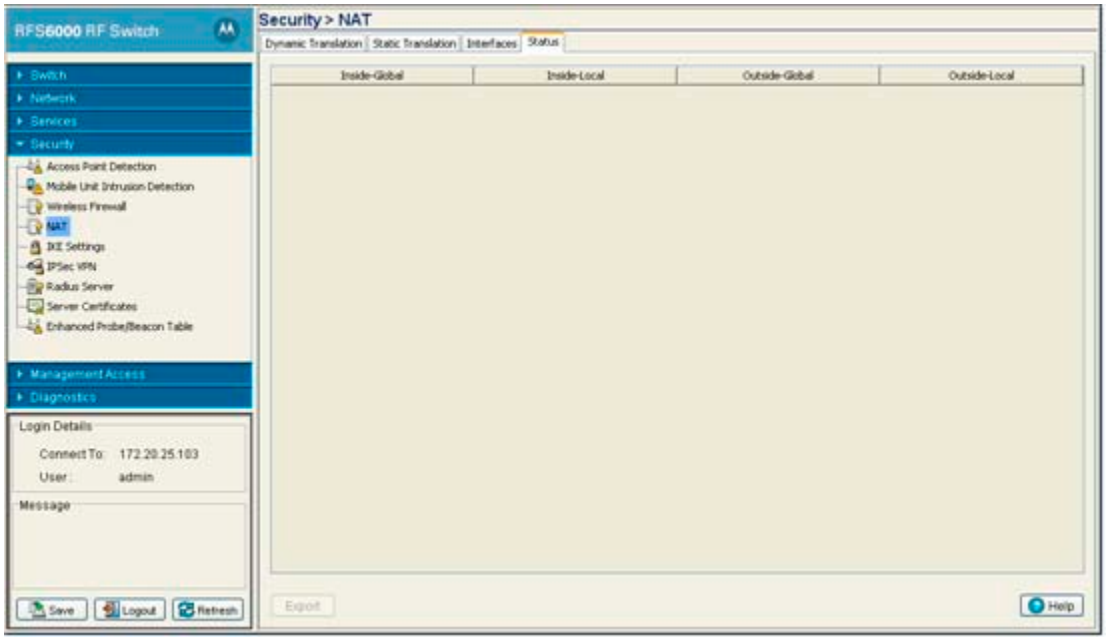
6.5.4 Viewing NAT Status

Use the **Status** tab to review the NAT translations configured thus far for the switch. The Status tab displays the inside and outside local and global IP addresses.

To view and configure a NAT interface:

1. Select **Security** > **NAT** from the main menu tree.

2. Click on the **Status** tab.



3. Refer to the following to assess the validity and total NAT translation configurations available to the switch.

Inside-Global	Displays the internal global pool of addresses (allocated out of the switch's private address space but relevant to the outside) you are trying to prevent from being exposed to the outside world.
Inside Local	Displays the internal local pool of addresses (addresses internal to the switch) you are trying to prevent from being exposed to the outside world.
Outside-Global	The IP address of an outside host as it appears to the inside network.
Outside-Local	The configured IP address assigned to a host in the outside network.

4. Click on the **Export** button to export the contents of the table to a *Comma Separated Values* file (CSV).

6.6 Configuring IKE Settings

IKE (also known as ISAKMP) is the negotiation protocol enabling two hosts to agree on how to build an IPSec security association. To configure the security appliance for virtual private networks, set global IKE parameters that apply system wide and define IKE policies peers negotiate to establish a VPN tunnel.

IKE protocol is an IPSec standard protocol used to ensure security for VPN negotiation, and remote host or network access. IKE provides an automatic means of negotiation and authentication for communication between two or more parties. IKE manages IPSec keys automatically.

The IKE configuration is defined by the following:

- *Defining the IKE Configuration*
- *Setting IKE Policies*
- *Viewing SA Statistics*

NOTE: By default, the IKE feature is enabled. Motorola does not support disabling the IKE server.

NOTE: The default isakmp policy will not be picked up for IKE negotiation if another crypto isakmp policy is created. For the default isakmp policy to be picked up for AAP adoption you must first create the default isakmp policy as a new policy with default parameters. This needs to be done if multiple crypto isakmp policies are needed in the switch configuration.

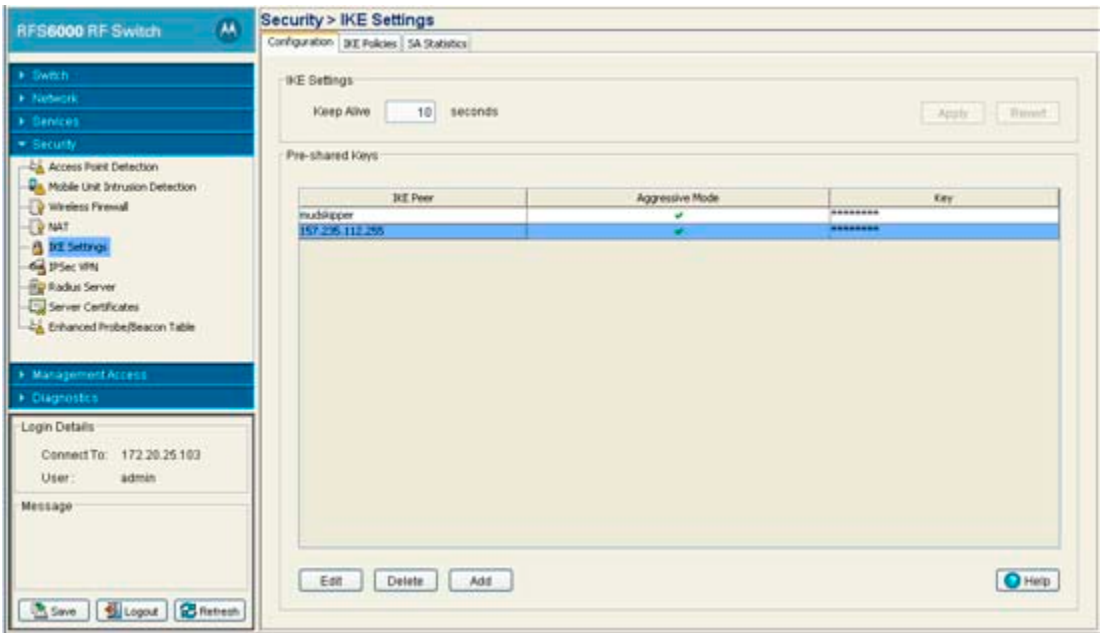
6.6.1 Defining the IKE Configuration

Refer to the **Configuration** tab to enable (or disable) IKE and define the IKE identity (for exchanging identities) and aggressive mode. Aggressive mode reduces messages exchanged when establishing IKE SAs (used in phase 2).

Use IKE to specify IPSec tunnel attributes for an IPSec peer and initiate an IKE aggressive mode negotiation with the tunnel attributes. This feature is best implemented in a crypto hub scenario. Users initiate IKE aggressive mode negotiation with the switch using pre-shared keys specified as tunnel attributes. This scenario is scalable since the keys are kept at a central repository (the Radius server) and more than one switch and application can use the information.

To view the current set of IKE configurations:

1. Select **Security** > **IKE Settings** from the main menu tree.
2. Click the **Configurations** tab.



During IKE negotiations, peers must identify themselves to one another. Thus, the configuration you define is the identification medium for device recognition.

3. Set a **Keep Alive** interval (in seconds) the switch uses for monitoring the continued presence of a peer and report of the client's continued presence. The client notifies you when the peer is no longer present. The default interval is 10 seconds.
4. Click the **Apply** button (within the IKE Settings field) to save the configuration.
5. Click the **Revert** (within the IKE Settings field) to rollback to the previous configuration.
6. Refer to the **Pre-shared Keys** field to review the following information:

IKE Peer	Use this address to associate an IP address with the specific tunnel used by a group of peers.
Aggressive Mode	Displays whether aggressive mode is enabled for this IP address and key string. A green check mark defines aggressive mode as enabled. A red "X" denotes the mode as disabled.
Key	Displays the string ID a remote peer uses to look up pre-shared keys.

NOTE: Please note that RSA keys are not supported for IKE negotiation on this switch.

7. Highlight an existing set of pre-shared Keys and click the **Edit** button to revise the existing peer IP address, key and aggressive mode designation.
8. Select an existing entry and click the **Delete** button to remove it.

9. If the properties of an existing peer IP address, key and aggressive mode designation are no longer relevant and cannot be edited, click the **Add** button to create a new pre-shared key

   a. Select the **Peer IP Address checkbox** to associate an IP address with the specific tunnel used by a group of peers or, select the **Distinguished Name** checkbox to configure the switch to restrict access to those peers with the same distinguished name, or select the **Hostname** checkbox to allow shared-key messages between corresponding hostnames.

   b. Define the **Key** (string ID) a remote peer uses to look up the pre-shared to interact securely with peers within the tunnel.

   c. Select the **Aggressive Mode** checkbox (if required). Aggressive mode enables you to configure IKE pre-shared keys as Radius tunnel attributes for IP Security (IPSec) peers.

   d. Refer to the **Status** field for the current state of requests made from applet. This field displays error messages if something is wrong in the transaction between the applet and the switch.

   e. Click **OK** to use the changes to the running configuration and close the dialog.

   f. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.6.2 Setting IKE Policies

Each IKE negotiation is divided into two phases. Phase 1 creates the first tunnel (protecting later IKE negotiation messages) and phase 2 creates the tunnel protecting the data. To define the terms of the IKE negotiation, create one or more IKE policies. Include the following:

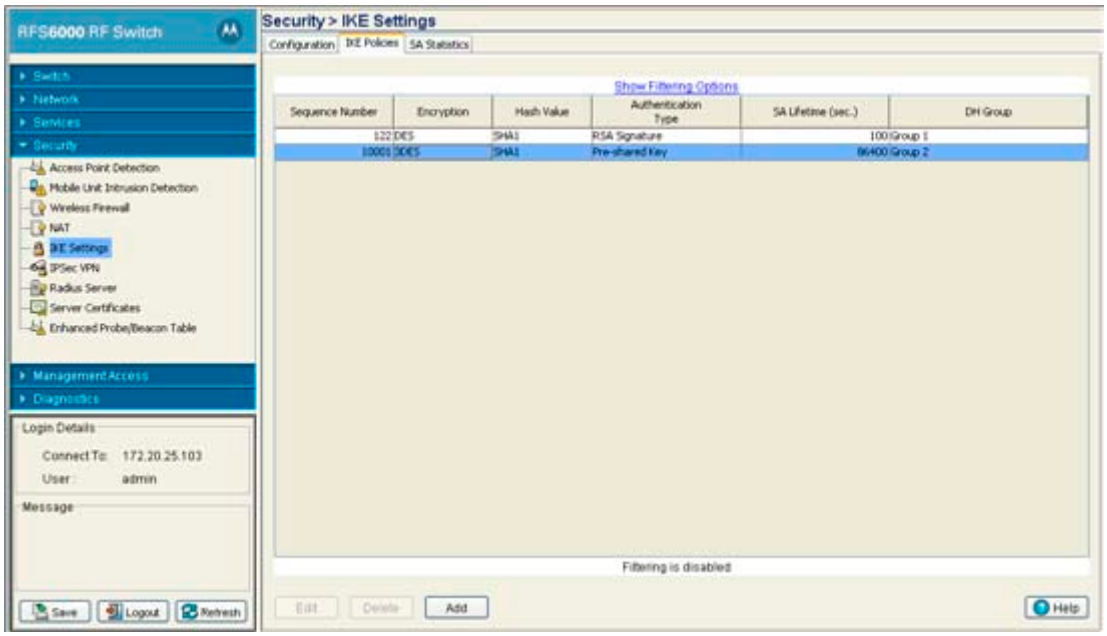
- An authentication scheme to ensure the credentials of the peers
- An encryption scheme to protect the data
- A HMAC method to ensure the identity of the sender, and validate a message has not been altered
- A Diffie-Hellman group establishing the strength of the of the encryption-key algorithm.
- A time limit for how long the encryption key is used before it is replaced.

If IKE policies are not defined, the switch uses the default policy (with a default priority of 10001) and contains the default values. When IKE negotiations begin, the peer initiating the negotiation sends its policies to the remote peer. The remote peer searches for a match with its own policies using the defined priority scheme.

A IKE policy matches when they have the same encryption, hash, authentication and Diffie-Hellman settings. The SA lifetime must also be less than or equal to the lifetime in the policy sent. If the lifetimes do not match, the shorter lifetime applies. If no match exists, IKE refuses negotiation.

To view the current set of IKE policies:

1. Select **Security** > **IKE Settings** from the main menu tree.
2. Click the **IKE Policies** tab.



3. Refer to the values displayed within the IKE Policies tab to determine if an existing policy requires revision, removal or a new policy requires creation.

Sequence Number — Displays the sequence number for the IKE policy. The available range is from 1 to 10,000, with 1 being the highest priority value.

Encryption — Displays the encryption method protecting data transmitted between peers. Options include:

- *DES 56-bit DES-CBC*. The default value.
- *3DES* - 168-bit Triple DES.
- *AES* - 128-bit AES.
- *AES 192* - 192-bit AES.
- *AES 256* - 256-bit AES.

Hash Value — Displays the hash algorithm used to ensure data integrity. The hash value validates a packet comes from its intended destination, and has not been modified in transit. Options include:

- *SHA* - The default value.
- *MD5* - MD5 has a smaller digest and is somewhat faster than SHA-1.

Authentication Type	Displays the authentication scheme used to validate the identity of each peer. Pre-shared keys do not scale accurately with a growing network but are easier to maintain in a small network. Options include: • *Pre-shared Key* - Uses pre-shared keys. • *RSA Signature* - Uses a digital certificate with keys generated by the RSA signatures algorithm.
SA Lifetime (sec.)	Displays an integer for the SA lifetime. The default is 60 seconds. With longer lifetimes, security defines future IPSec security associations quickly. Encryption strength is great enough to ensure security without using fast rekey times. Motorola recommends using the default value.
DH Group	Displays the *Diffie-Hellman* (DH) group identifier. IPSec peers use the defined value to derive a shared secret without transmitting it to one another.

NOTE: 192-bit AES and 256-bit AES are not supported for manual IPSec sa configurations.

4. Highlight an existing policy and click the **Edit** button to revise the policy's existing encryption scheme, hash value, authentication type, SA lifetime and DH group.

   The sequence number cannot be revised.

5. Select an existing policy and click the **Delete** button to remove it from the table.

6. If the properties of an existing policy are no longer relevant and cannot be edited to be useful, click the **Add** button to define a new policy.

a. Configure a set of attributes for the new IKE policy:

Sequence Number — Define the sequence number for the IKE policy. The available range is from 1 to 10,000 with 1 being the highest priority value.

Encryption — Set the encryption method used to protect the data transmitted between peers. Options include:

- *DES 56-bit DES-CBC*. The default value.
- *3DES* - 168-bit Triple DES.
- *AES* - 128-bit AES.
- *AES 192* - 192-bit AES.
- *AES 256* - 256-bit AES.

Hash Value — Define the hash algorithm used to ensure data integrity. The hash value validates a packet comes from its intended source and has not been modified in transit. Options include:

- *SHA* - The default value.
- *MD5* - MD5 has a smaller digest and is somewhat faster than SHA-1.

Authentication Type — Set the authentication scheme used to validate the identity of each peer. Pre-shared keys do not scale accurately with a growing network but are easier to maintain in a small network. Options include:

- *Pre-shared Key* - Uses pre-shared keys.
- *RSA Signature* - Uses a digital certificate with keys generated by the RSA signatures algorithm.

SA Lifetime — Define an integer for the SA lifetime. The default is 60 seconds. With longer lifetimes, security defines future IPSec security associations quickly. Encryption strength is great enough to ensure security without using fast rekey times. Motorola recommends using the default value.

DH Group — Set the Diffie-Hellman group identifier. IPSec peers use the defined value to derive a shared secret without transmitting it to one another.

b. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

c. Click **OK** to use the changes to the running configuration and close the dialog.

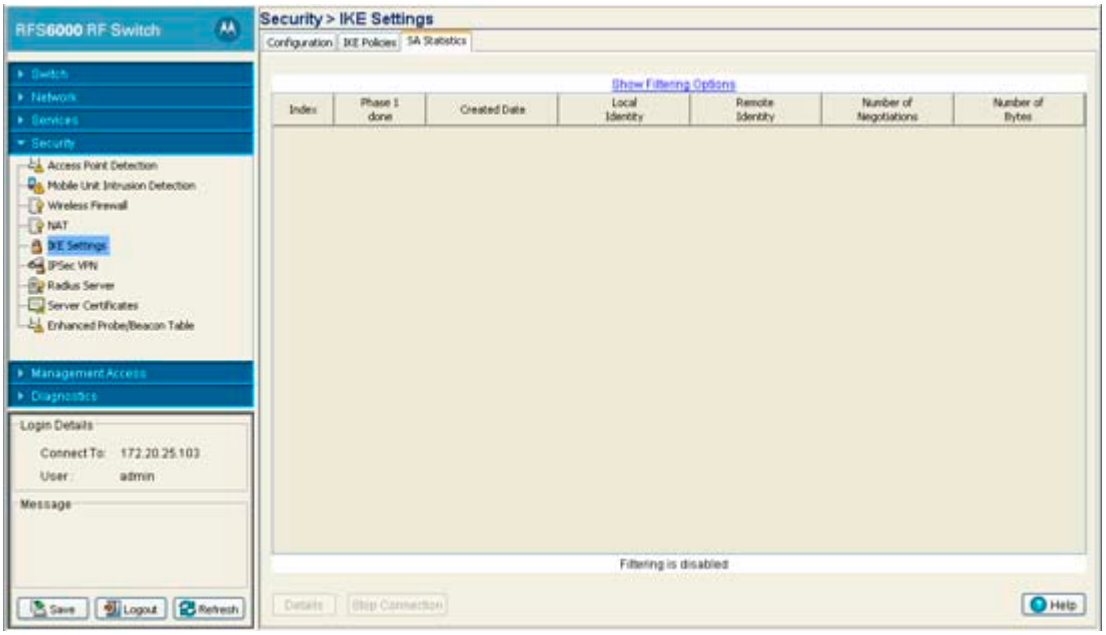
d. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.6.3 Viewing SA Statistics

A *security association* (SA) is a description of how two peers employ a security to interoperate securely. IKE requires SAs to identify connection attributes. IKE can negotiate and establish its own SA. An IKE SA is used by IKE only, and is bi-directional.

To view SA statistics:

1. Select **Security** > **IKE Settings** from the main menu tree.
2. Click the **SA Statistics** tab.



3. Refer to the information displayed within SA Statistics tab to discern the following:

Index	Displays the alpha-numeric name (index) used to identify individual SAs.
Phase 1 done	Displays whether this index is completed with the phase 1 (authentication) credential exchanged between peers.
Created Date	Displays the exact date the SA was configured for each index displayed.
Local Identity	Specifies the address the local IKE peer uses to identify itself to the remote peer.
Remote Identity	Specifies the address the remote IKE peer uses to identify itself to a local peer.
Number of Negotiations	During IKE negotiations the peers must identify themselves to each other. This value is helpful in determining the network address information used to validate peers.
Number of Bytes	Displays the number of bytes passed between the peers for the specified index.

4. Select an index and click the **Details** button to display a more robust set of statistics for the selected index.

   Use this information to discern whether changes to an existing IKE configuration is warranted or if a new configuration is required.

5. Click the **Stop Connection** button to terminate the statistic collection of the selected IKE peer.

6.7 Configuring IPSec VPN

Use IPSec *Virtual Private Network* (VPN) to define secure tunnels between two peers. Configure which packets are sensitive and should be sent through secure tunnels, and what should be used to protect these sensitive packets. Once configured, an IPsec peer creates a secure tunnel and sends the packet through the tunnel to the remote peer.

IPSec tunnels are sets of security associations (SA) established between two peers. The security associations define which protocols and algorithms are applied to sensitive packets, and what keying material is used by the two peers. Security associations are unidirectional and established per security protocol.

To configure IPSec security associations, Motorola uses the Crypto Map entries. Crypto Map entries created for IPSec pull together the various parts used to set up IPSec security associations. Crypto Map entries include transform sets. A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IPSec protected traffic.

The Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with the IPSec standard. IKE automatically negotiates IPSec security associations and enables IPSec secure communications without costly manual configuration. To support IPSec VPN functionality, the following configuration activities are required:

- *Configure a DHCP Sever to assign public IP address*

  An IPSec client needs an IP address before it can connect to the VPN Server and create an IPSec tunnel. A DHCP Server needs to be configured on the interface to distribute public IP addresses to the IPSec clients.

- *Configure a Crypto policy (IKE)*

  IKE automatically negotiates IPSec security associations and enables IPSec secure communications without costly manual pre-configuration. IKE eliminates the need to manually specify all the IPSec security parameters in the Crypto Maps at both peers, allows you to specify a lifetime for the IPSec security association, allows encryption keys to change during IPSec sessions and permits *Certification Authority* (CA) support for a manageable, scalable IPSec implementation. If you do not want IKE with your IPSec implementation, disable it for IPSec peers. You cannot have a mix of IKE-enabled and IKE-disabled peers within your IPSec network.

- *Configure security associations parameters*

  The use of manual security associations is a result of a prior arrangement between switch users and the IPSec peer. If IKE is not used for establishing security associations, there is no negotiation of security associations. The configuration information in both systems must be the same for traffic to be processed successfully by IPSec.

- *Define transform sets*

  A transform set represents a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a particular transform set for protecting data flow.

With manually established security associations, there is no negotiation with the peer. Both sides must specify the same transform set. If you change a transform set definition, the change is only applied to Crypto Map entries that reference the transform set. The change is not applied to existing security associations, but is used in subsequent negotiations to establish new security associations.

- *Create Crypto Map entries*

  When IKE is used to establish security associations, the IPSec peers can negotiate the settings they use for the new security associations. Therefore, specify lists (such as lists of acceptable transforms) within the Crypto Map entry.

- *Apply Crypto Map sets to Interfaces*

  Assign a Crypto Map set to each interface through which IPSec traffic flows. The security appliance supports IPSec on all interfaces. Assigning the Crypto Map set to an interface instructs the security appliance to evaluate all the traffic against the Crypto Map set and use the specified policy during connection or SA negotiation. Assigning a Crypto Map to an interface also initializes run-time data structures (such as the SA database and the security policy database). Reassigning a modified Crypto Map to the interface resynchronizes the run-time data structures with the Crypto Map configuration. With the switch, a Crypto Map cannot get applied to more than one interface at a time.

- *Monitor and maintain IPSec tunnels*

  New configuration changes only take effect when negotiating subsequent security associations. If you want the new settings to take immediate effect, clear the existing security associations so they will be re-established with the changed configuration.

  For manually established security associations, clear and reinitialize the security associations or the changes will not take effect.

NOTE: Though the switch can adopt an AP-7131 model access point, an AP-7131 cannot provide IPSec support and should not be used in IPSec supported configurations.

For more information on configuring IPSec VPN, refer to the following:

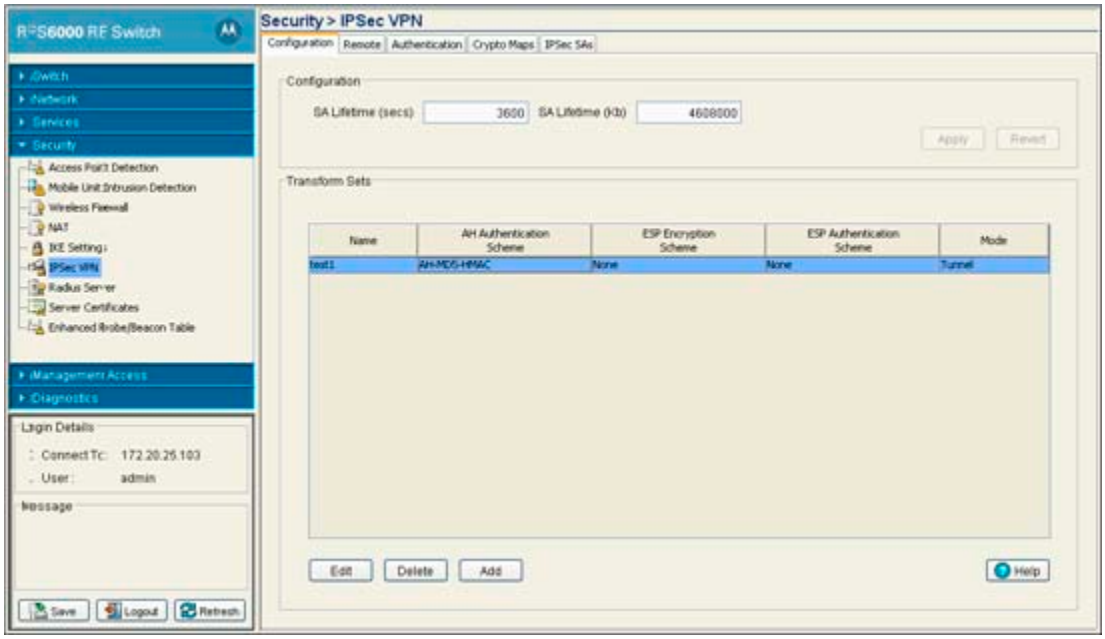
- *Defining the IPSec Configuration*
- *Defining the IPSec VPN Remote Configuration*
- *Configuring IPSEC VPN Authentication*
- *Configuring Crypto Maps*
- *Viewing IPSec Security Associations*

6.7.1 Defining the IPSec Configuration

Use the IPSec VPN **Configuration** tab to view the attributes of existing VPN tunnels and modify the security association lifetime and keep alive intervals used to maintain the sessions between VPN peers. From the Configuration tab, transform sets can be created as existing sets, modified or deleted.

1. Select **Security** > **IPSec VPN** from the main menu tree.

2. Click the **Configuration** tab.



3. Refer to the **Configuration** field to define the following:

SA Lifetime (secs)	For IKE based security associations, define a SA Lifetime (in seconds) forcing the periodic expiration and re-negotiation of peer credentials. Thus, continually validating the peer relationship. The default value is 3600 seconds.
SA Lifetime (Kb)	Causes the security association to time out after the specified amount of traffic (in kilobytes) have passed through the IPSec tunnel using the security association. The default value is 4608000 Kb.
Apply	Click **Apply** to save any updates you may have made to the screen.
Revert	Click the **Revert** button to disregard any changes you have made and revert back to the last saved configuration.

4. Refer to the **Transform Sets** field to view the following data:

Name	Displays a transform set identifier used to differentiate transform sets. The index is helpful when transform sets with similar attributes need to be revised or discarded.
AH Authentication Scheme	Displays the AH Transform Authentication scheme used with the index. Options include: • *None* - No AH authentication is used. • *AH-MD5-HMAC* - AH with the MD5 (HMAC variant) authentication algorithm. • *AH-SHA-HMAC* - AH with the SHA (HMAC variant) authentication algorithm.

ESP Encryption Scheme	Displays the ESP Encryption Transform used with the index. Options include: • *None* - No ESP encryption is used with the transform set. • *ESP-DES* - ESP with the 56-bit DES encryption algorithm. • *ESP-3DES* - ESP with 3DES, ESP with AES. • *ESP-AES* - ESP with 3DES, ESP with AES (128 bit key). • *ESP-AES 192* - ESP with 3DES, ESP with AES (192 bit key). • *ESP-AES 256* - ESP with 3DES, ESP with AES (256 bit key)
ESP Authentication Scheme	Displays the ESP Authentication Transform used with the index. Options include: • *None* - No ESP authentication is used with the transform set. • *MD5-HMAC* - AH with the MD5 (HMAC variant) authentication algorithm. • *SHA-HMAC* - AH with the SHA (HMAC variant) authentication algorithm.
Mode	Displays the current mode used with the transform set. The mode is either Tunnel or Transport.

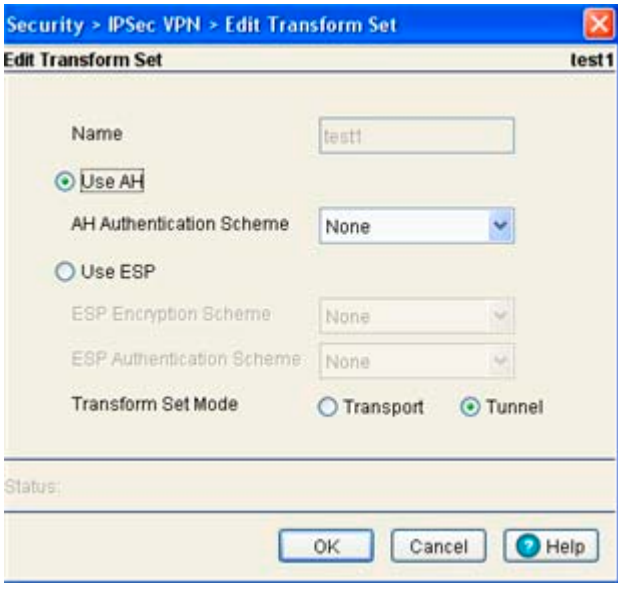
5. Select an IPSec VPN transform set (by its index) and click the **Edit** button to modify its properties. For more information, see *Editing an Existing Transform Set on page 6-67*.
6. Select an index and click the **Delete** button to remove it from the table.
7. If none of the transform sets displayed appear useful, click the **Add** button to create a new one. For more information, see *Adding a New Transform Set on page 6-68*.

6.7.1.1 Editing an Existing Transform Set

If the attributes of an existing transform set no longer lend themselves useful, consider editing the transform set to be relevant with the needs of existing VPN peers.

To edit the attributes of an existing transform set:

1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Configuration** tab.
3. Select an existing transform set and click the **Edit** button.



4. Revise the following information as required to render the existing transform set useful.

Name	The name is read-only and cannot be modified unless a new transform set is created.
AH Authentication Scheme	Select the **Use AH** checkbox (if necessary) to modify the AH Transform Authentication scheme. Options include: • *None* - No AH authentication is used. • *AH-MD5-HMAC* - AH with the MD5 (HMAC variant) authentication algorithm. • *AH-SHA-HMAC* - AH with the SHA (HMAC variant) authentication algorithm.
ESP Encryption Scheme	Select the **Use ESP** checkbox (if necessary) to modify the ESP Encryption Scheme. Options include: • *None* - No ESP encryption is used with the transform set. • *ESP-DES* - ESP with the 56-bit DES encryption algorithm. • *ESP-3DES* - ESP with 3DES, ESP with AES. • *ESP-AES* - ESP with 3DES, ESP with AES (128 bit key). • *ESP-AES 192* - ESP with 3DES, ESP with AES (192 bit key). • *ESP-AES 256* - ESP with 3DES, ESP with AES (256 bit key).
ESP Authentication Scheme	Select the **Use ESP** checkbox (if necessary) to modify the ESP Authentication Scheme. Options include: • *None* - No ESP authentication is used with the transform set. • *MD5-HMAC* - AH with the MD5 (HMAC variant) authentication algorithm. • *SHA-HMAC* - AH with the SHA (HMAC variant) authentication algorithm.
Mode	Modify (if necessary) the current mode used with the transform set. The mode is either Tunnel or Transport.

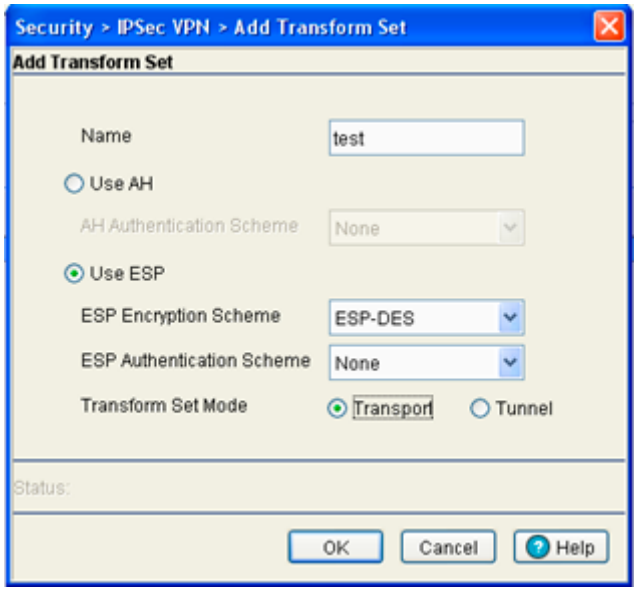
5. Refer to the **Status** field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.7.1.2 Adding a New Transform Set

A transform set represents a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a particular transform set for protecting data flow. If the attributes of an existing transform set no longer lend themselves useful, and an existing transform set is not required, create a new transform set to meet the needs of your network.

To edit the attributes of an existing transform set:

1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Configuration** tab.
3. Click the **Add** button.



4. Define the following information as required for the new transform set.

Name	Create a name describing this new transform set.
AH Authentication Scheme	Select the **Use AH** checkbox to define the AH Transform Authentication scheme. Options include: • *None* - No AH authentication is used. • *AH-MD5-HMAC* - AH with the MD5 (HMAC variant) authentication algorithm. • *AH-SHA-HMAC* - AH with the SHA (HMAC variant) authentication algorithm.
ESP Encryption Scheme	Select the **Use ESP** checkbox to define the ESP Encryption Scheme. Options include: • *None* - No ESP encryption is used with the transform set. • *ESP-DES* - ESP with the 56-bit DES encryption algorithm. • *ESP-3DES* - ESP with 3DES, ESP with AES. • *ESP-AES* - ESP with 3DES, ESP with AES (128 bit key). • *ESP-AES 192* - ESP with 3DES, ESP with AES (192 bit key). • *ESP-AES 256* - ESP with 3DES, ESP with AES (256 bit key).
ESP Authentication Scheme	Select the **Use ESP** checkbox to define the ESP Authentication Scheme. Options include: • *None* - No ESP authentication is used with the transform set. • *MD5-HMAC* - AH with the MD5 (HMAC variant) authentication algorithm. • *SHA-HMAC* - AH with the SHA (HMAC variant) authentication algorithm.
Mode	Define the current mode used with the transform set. The mode is either Tunnel or Transport.

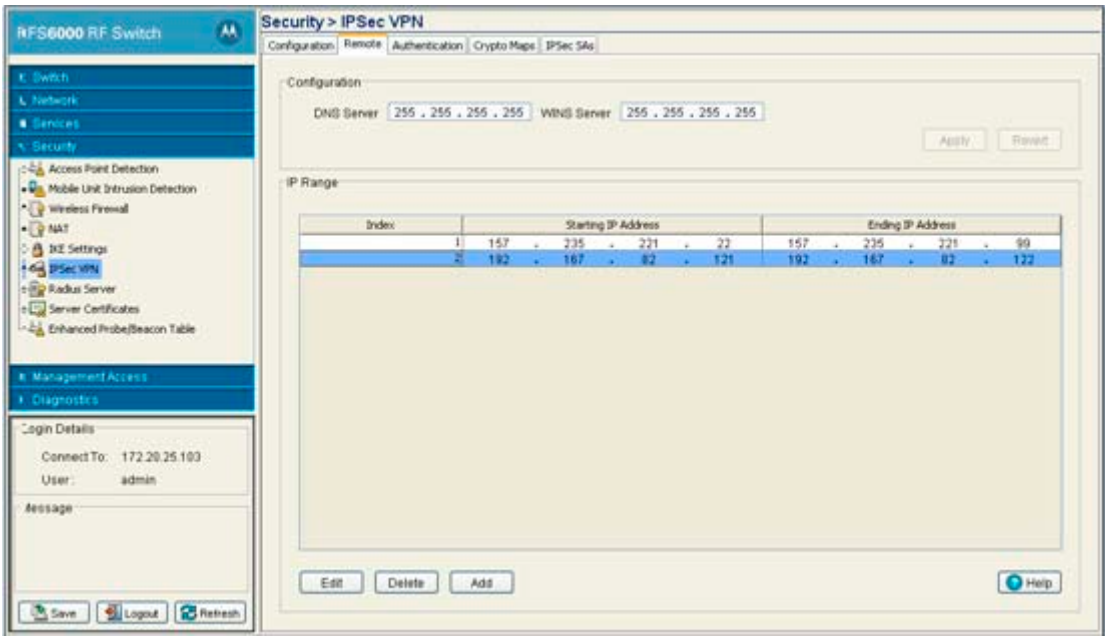
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.7.2 Defining the IPSec VPN Remote Configuration

Use the **IPSec VPN Remote** tab to configure the DNS and/or WINS Servers used to route packets to the remote end of the IPSec VPN tunnel. The Remote tab is also used for defining the IP address range used within the IPSec VPN tunnel and configuring the authentication scheme for user permissions within the IPSec VPN tunnel.

To define the IPSEc VPN's remote configuration:

1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Remote** tab.



3. Refer to the **Configuration** field to define the following:

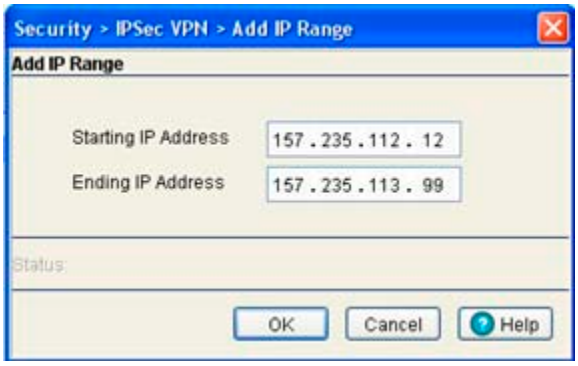
DNS Server	Enter the numerical IP address of the DNS Server used to route information to the remote destination of the IPSec VPN.
WINS Server	Enter the numerical IP address of the WINS Server used to route information to the remote destination of the IPSec VPN.
Apply	Click **Apply** to save any updates made to the screen.
Revert	Click the **Revert** button to disregard changes and revert back to the last saved configuration.

4. Click the **IP Range** tab to view the following:.

Index	Enter the index assigned to the range of IP addresses displayed in the Starting and Ending IP Address ranges. This index is used to differentiate the index from others with similar IP addresses.

Starting IP Address	Enter the numerical IP address used as the starting address for the range defined. If the Ending IP address is left blank, only the starting address is used for the remote destination.
Ending IP Address	Enter a numerical IP address to complete the range. If the Ending IP address is blank, only the starting address is used as the destination address.

5. Click the **Edit** button (within the IP Range tab) to modify the range of existing IP addresses displayed.
6. Select an IP address range index and click the **Delete** button to remove this range from those available within the IP Range tab.
7. To add a new range of IP addresses, click the **Add** button (within the IP Range tab) and define the range in the fields provided. Click **OK** when completed to save the changes.



8. Click **Cancel** to disregard the changes and revert to the last saved configuration.

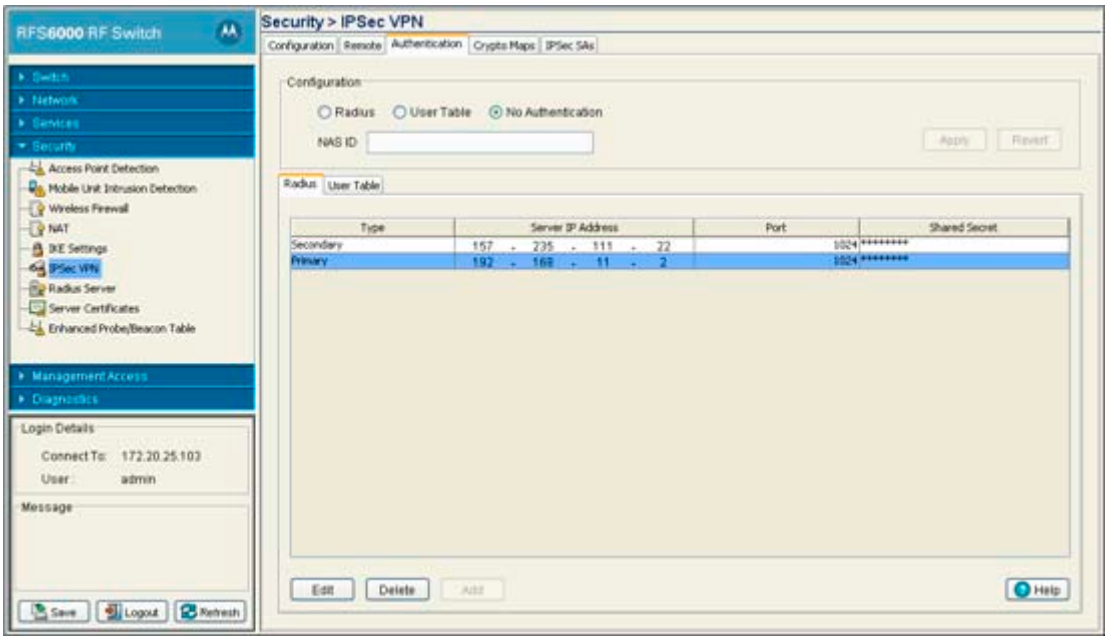
6.7.3 Configuring IPSEC VPN Authentication

If IKE is not used for establishing security associations, there is no negotiation of security associations. Consequently, the configuration information in both systems must be the same for traffic to be processed successfully by the IPSec resource. Select the **Authentication** tab to define the credential verification mechanisms used with the IPSEC VPN configuration.

To define the IPSEc VPN authentication configuration:

1. Select **Security** > **IPSec VPN** from the main menu tree.

2. Select the **Authentication** tab.



3. Define whether IPSec VPN user authentication is conducted using a Radius Server (by selecting the **Radius** radio button), by a user-defined set of names and password (by selecting the **User Table** radio button) or if no authentication is used for credential verification (by selecting the **No Authentication** radio button).
4. Enter a **NAS ID** for the NAS port.

   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 switch authorizes users, it queries the user profile database using a username representative of the physical NAS port making the connection.
5. If the **Radius Server** radio button is selected, the following server information displays within the Radius tab:

Type	Displays whether this target server is a Primary or Secondary Radius Server.
Server IP Address	Displays the IP address of the server acting as the data source for the Radius server.
Port	Displays the TCP/IP port number for the server acting as a data source for the Radius. The default port is 1812.
Shared Secret	Displays a shared secret used for each host or subnet authenticating against the Radius server. The shared secret can be up to 7 characters in length.

6. Select an existing Radius Server and click the **Edit** button to modify its designation as a primary or secondary Radius Server, IP address, port, NAS ID and shared secret password.

   Motorola recommends only modifying an existing Radius Server when its current configuration is no longer viable for providing user authentication. Otherwise, define a new Radius Server.
7. Select an existing server and click the **Delete** button to remove it from list of available Radius Servers. Only delete a server if its configuration does not provide a valid authentication medium.

8. If you require a new Radius Server be configured, click the **Add** button.

   Set this server's designation as a primary or secondary Radius Server (using the checkboxes), define the server IP address, port and shared secret password. Click **OK** when completed to save the changes.

9. If the **User Table** checkbox was selected from within the Configuration field, select the User Table tab to review the User Name and Passwords defined for use.

10. Click the **Add** button to display a screen used to add a new User and Password. Enter a User Name and Password and confirm. Click **OK** to save the changes.

11. To change an existing user's password, select the user from within the User Table and click the **Change Password** button. Change and confirm the updated password.

12. If necessary, select an existing user and click the **Delete** button to remove that user from the list available within the User Table.

6.7.4 Configuring Crypto Maps

Crypto Maps allow you to set restrictions preventing peers with specific certificates (especially certificates with particular DNs) from accessing selected encrypted interfaces. If restricting access, specify a fewer number of Crypto Maps (referring to large identity sections) instead of specifying a large number of Crypto Maps (referring to small identity sections).

To define the Crypto Map configuration:

1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Crypto Maps** tab.

   The Crypto Maps screen is divided into 5 tabs, each serving a unique function in the overall Crypto Map configuration. Refer to the following:

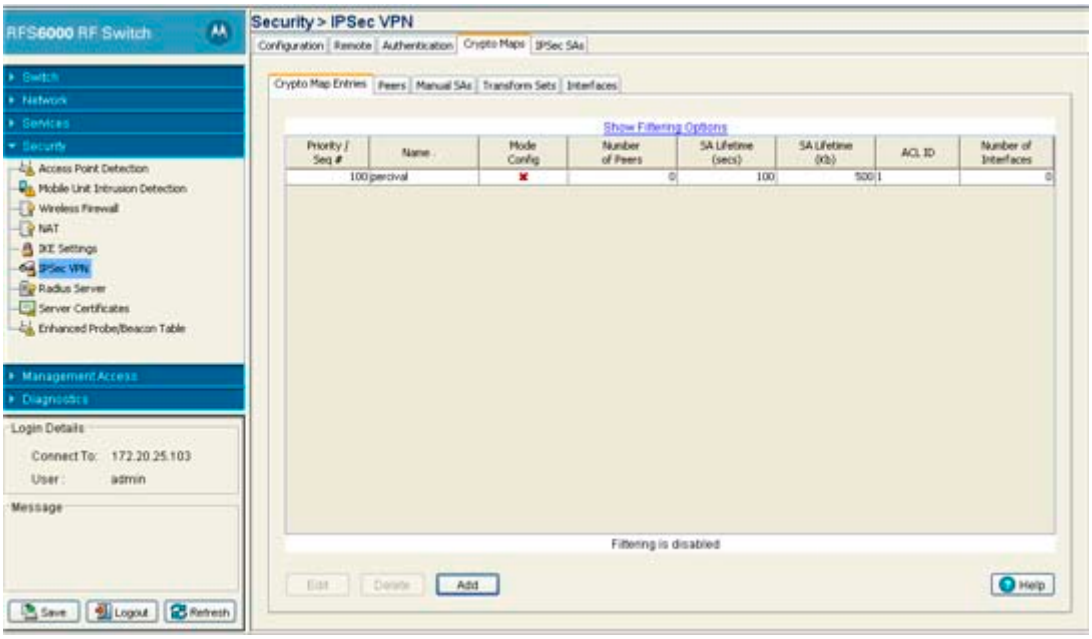
   - *Crypto Map Entries*
   - *Crypto Map Peers*
   - *Crypto Map Manual SAs*
   - *Crypto Map Transform Sets*
   - *Crypto Map Interfaces*

6.7.4.1 Crypto Map Entries

To review, revise or add Crypto Map entries:

1. Select **Security** > **IPSec VPN** from the main menu tree.

2. Click the **Crypto Maps** tab and select **Crypto Map Entries**.



3. Review the following Crypto Map attributes to determine if an existing Crypto Map requires revision, deletion or if a new Crypto Map needs to be created.

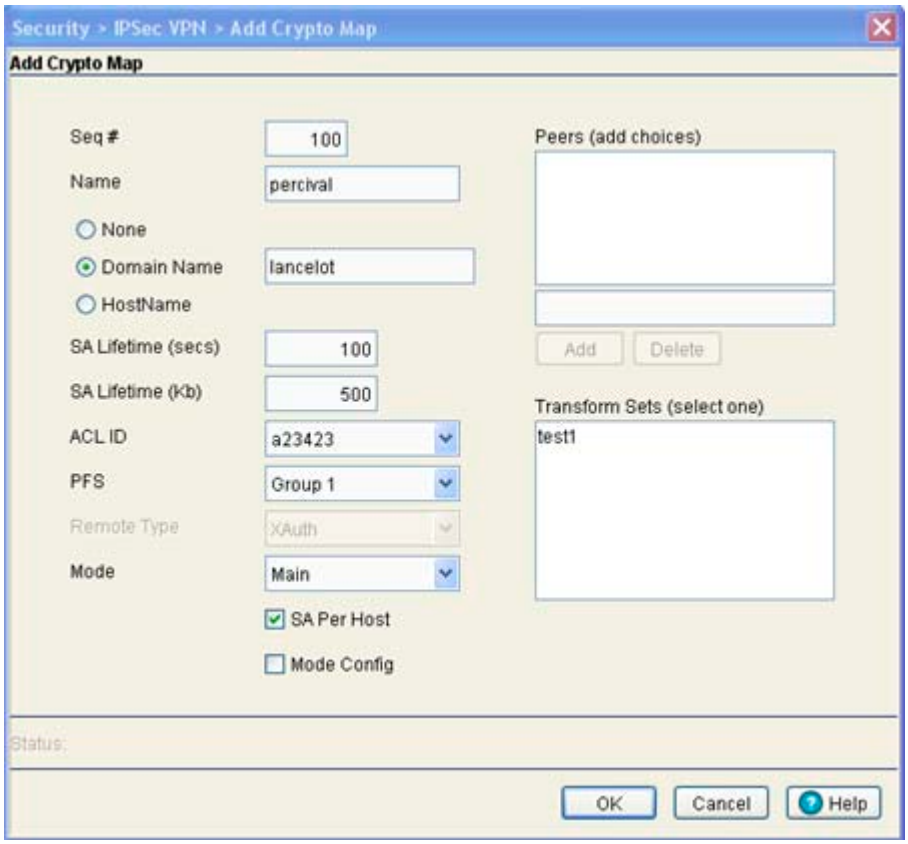
Priority / Seq	Displays the numerical priority assigned to each Crypto Map.
Name	Displays the user-assigned name for this specific Crypto Map. This name can be modified using the **Edit** function or a new Crypto Map can be created by clicking the **Add** button.
Mode Config	Displays a green checkmark for the Crypto Map used with the current interface. A "X" is displayed next to other Crypto Maps not currently being used.
Number of Peers	Displays the number of peers used by each Crypto Map displayed.
SA Lifetime (secs)	Displays a SA Lifetime (in seconds) that forces the periodical expiration and re-negotiation of peer credentials. Thus, continually validating the peer relationship.
SA Lifetime (Kb)	Causes the security association to time out after the specified amount of traffic (in kilobytes) has passed through the IPSec tunnel (using the security association).
ACL ID	Displays the name of the ACL ID used for each Crypto Map.
Number of Interfaces	Displays the number of interfaces each specific Crypto Map is used with.

4. Select an existing Crypto Map and click the Edit button to modify the Crypto Map's attributes. If an entire Crypto Map requires revision, consider deleting the Crypto Map and creating a new one using the **Add** function.

   Refer to the definitions supplied for the **Add Crypto Map** screen (on the next page) to ascertain the requirements for editing a Crypto Map.

5. Select an existing Crypto Map and click the **Delete** button to remove it from the list of available.

6. Click the **Add** button to define the attributes of a new Crypto Map.



a. Assign a **Seq #** (sequence number) to distinguish one Crypto Map from the another.

b. Assign the Crypto Map a **Name** to differentiate from others with similar configurations.

c. Use the **None, Domain Name** or **Host Name** radio buttons to select and enter the *fully qualified domain name* (FQDN) or host name of the host exchanging identity information.

d. Define a **SA Lifetime (secs)** to define an interval (in seconds) that (when expired) forces a new association negotiation.

e. Define a **SA Lifetime (Kb)** to time out the security association after the specified traffic (in kilobytes) has passed through the IPSec tunnel using the security association.

f. Use the **ACL ID** drop-down menu to permit a Crypto Map data flow using the permissions within the selected ACL.

g. Use the **PFS** drop-down menu to specify a group to require *perfect forward secrecy* (PFS) in requests received from the peer.

h. Use the **Remote Type** drop-down menu to specify a remote type (either **XAuth** or **L2TP**).

i. Use the **Mode** drop-down menu to specify a mode of **Main** or **Aggressive**. Aggressive mode enables you to configure pre-shared keys as Radius tunnel attributes for IP Security (IPSec) peers.

j. Optionally select the **SA Per Host** checkbox to specify that separate IPSec SAs should be requested for each source/destination host pair.

k. Optionally select the **Mode Config** checkbox to allow the new Crypto Map to be implemented using the aggressive mode (if selected from the Mode drop-down menu).

l. Refer to the **Peers (add choices)** field and use the Add and Delete functions as necessary to add or remove existing peers. For information on adding or modifying peers, see *Crypto Map Peers on page 6-76*.

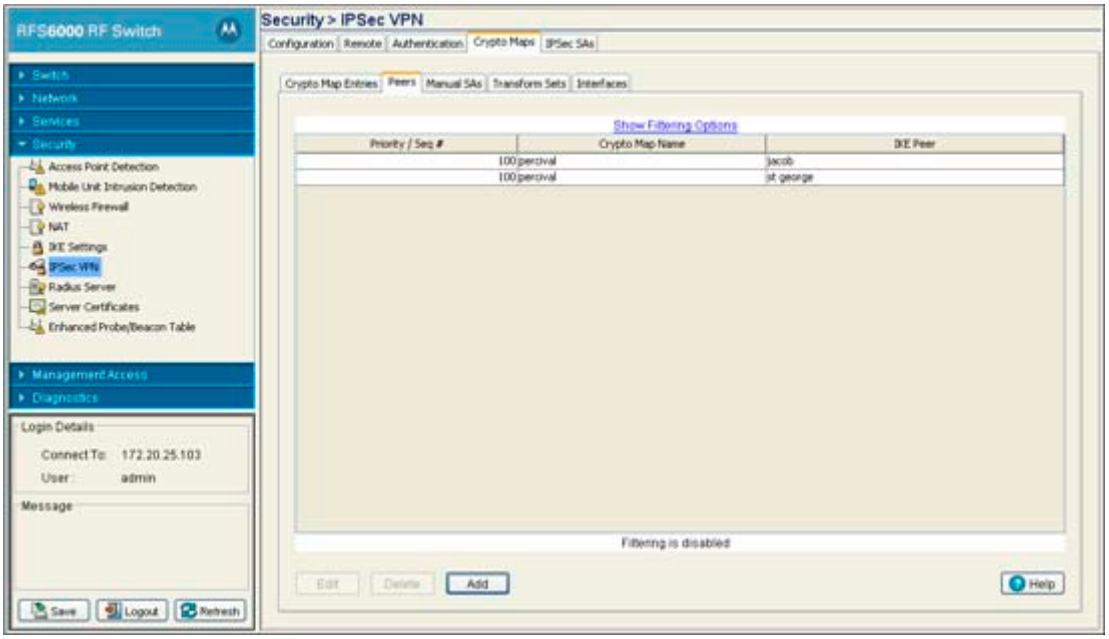
m. Refer to the **Transform Sets (select one)** field to select and assign a transform set for v with Crypto Map. Again, a transform set represents a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a particular transform set for protecting data flow.

7. Click **OK** to save the new Crypto Map and display it within the Crypto Map tab.

6.7.4.2 Crypto Map Peers

To review, revise or add Crypto Map peers:

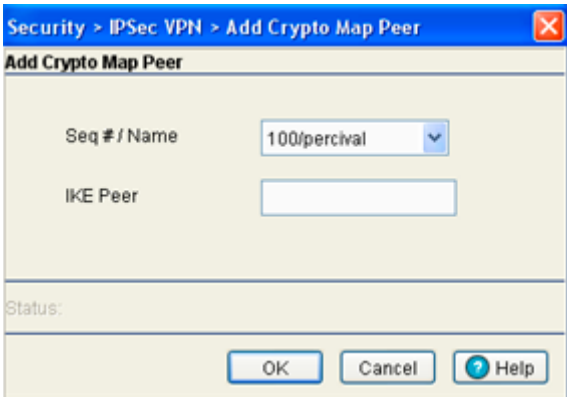
1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Crypto Maps** tab and select **Peers**.



3. Refer to the read-only information displayed within the **Peers** tab to determine whether a peer configuration (among those listed) requires modification or a new peer requires creation.

Priority / Seq #	Displays each peer's Seq # (sequence number) to distinguish one from the other.
Crypto Map Name	Displays the name assigned to the peer to differentiate it from others with similar configurations.
IKE Peer	Displays the IKE peer used with the Crypto Map to build an IPSec security association.

4. If a Crypto Map Seq # or IKE peer requires revision, select it from amongst those displayed and click the **Edit** button.
5. Select an existing Crypto Map and click the Delete button to remove it from the list of those available to the switch.
6. If a new peer requires creation, click the **Add** button.



a. Define the **Seq # /Name** for the new peer.

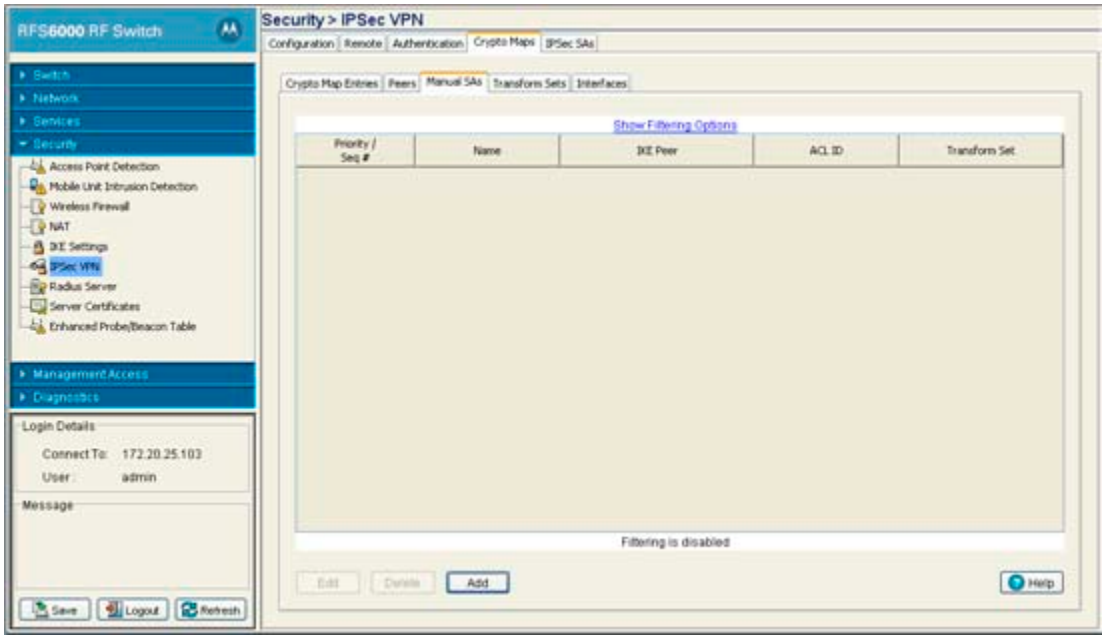
b. Enter the name of the **IKE Peer** used with the Crypto Map to build an IPSec security association.

7. Click **OK** to save the configuration of the new Crypto Map peer.

6.7.4.3 Crypto Map Manual SAs

To review, revise or add a Crypto Map using a manually defined security association:

1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Crypto Maps** tab and select **Manual SAs**.

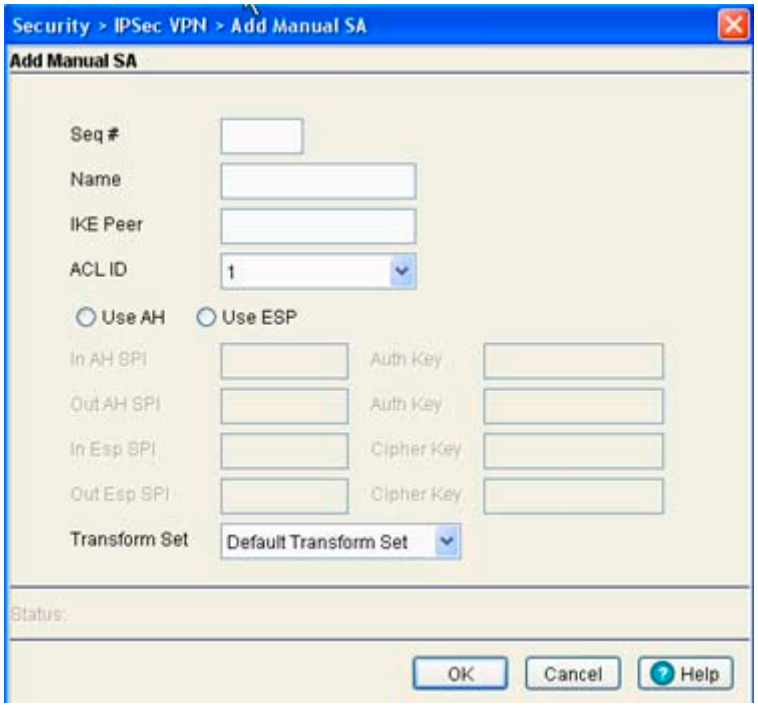


3. Refer to the read-only information displayed within the **Manual SAs** tab to determine whether a Crypto Map (with a manually defined security association) requires modification or if a new one requires creation.

Priority / Seq #	Displays the Seq # (sequence number) used to determine priority. the lower the number the higher the priority.
Name	Displays the name assigned to the security association.

IKE Peer	Displays the IKE peer used with the Crypto Map to build an IPSec security association.
ACL ID	Displays the ACL ID the Crypto Map's data flow uses to establish access permissions.
Transform Set	Displays the transform set representing a combination of security protocols and algorithms. During the security association negotiation, peers agree to use a particular transform set for protecting the data flow.

4. If a Crypto Map with a manual security association requires revision, select it from amongst those displayed and click the **Edit** button to revise its Seq #, IKE Peer, ACL ID and security protocol.
5. Select an existing table entry and click the **Delete** button to remove it from the list of those available to the switch.
6. If a new Crypto Map manual security association requires creation, click the **Add** button



a. Define the **Seq #**. The sequence number determines priority among Crypto Maps. The lower the number, the higher the priority.

b. Provide a unique **Name** for this Crypto Map to differentiate it from others with similar configurations.

c. Enter the name of the **IKE Peer** used to build an IPSec security association.

d. Use the **ACL ID** drop-down menu to permit a Crypto Map data flow using the unique permissions within the selected ACL.

e. Select either the **AH** or **ESP** radio button to define whether the Crypto Map's manual security association is an *AH Transform Authentication* scheme or an *ESP Encryption Transform* scheme. The AH SPI *or* ESP SPI fields become enabled depending on the radio button selected.

f. Define the **In AH SPI** and **Auth Keys** *or* **In Esp** and **Cipher Keys** depending on which option has been selected.

g. Use the **Transform Set** drop-down menu to select the transform set representing a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use the transform set for protecting the data flow. A new manual security association cannot be generated without the selection of a transform set. A default transform set is available (if none are defined).

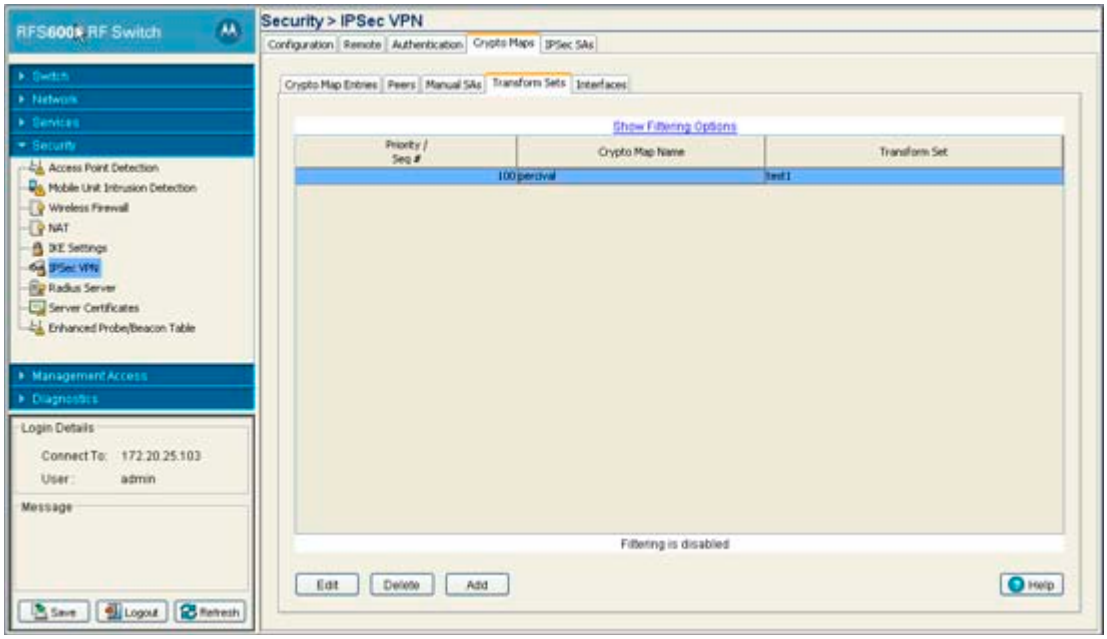
7. Click **OK** when completed to save the configuration of the Crypto Map security association.

6.7.4.4 Crypto Map Transform Sets

A transform set is a combination of security protocols and algorithms defining how the switch protects data.

To review, revise or add a Crypto Map transform set:

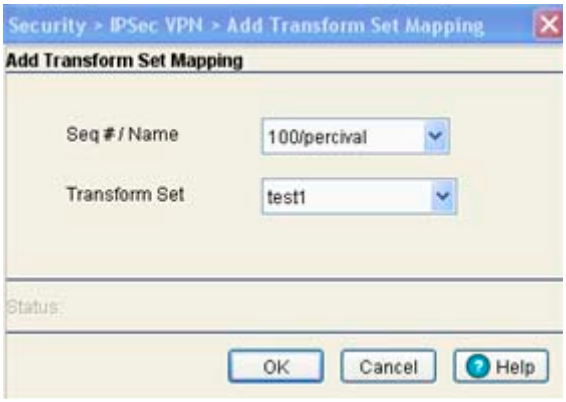
1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Crypto Maps** tab and select **Transform Sets**.



3. Refer to the read-only information displayed within the **Transform Sets** tab to determine whether a Crypto Map transform set requires modification or a new one requires creation.

Priority / Seq #	Displays the Seq # (sequence number) used to determine priority.
Name	Displays the name assigned to the Crypto Map that's using the transform set.
Transform Set	Displays the transform set representing a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use the transform set for protecting the data flow.

4. Select an existing Crypto Map and click the **Edit** button to revise its Seq #, Name and Transform Set.
5. Select an existing entry from the table and click the **Delete** button to remove it from the list.
6. If a new Crypto Map transform set requires creation, click the **Add** button.



a. Select the **Seq #/Name**.

b. Enter the name of the **Transform set** used with the Crypto Map.

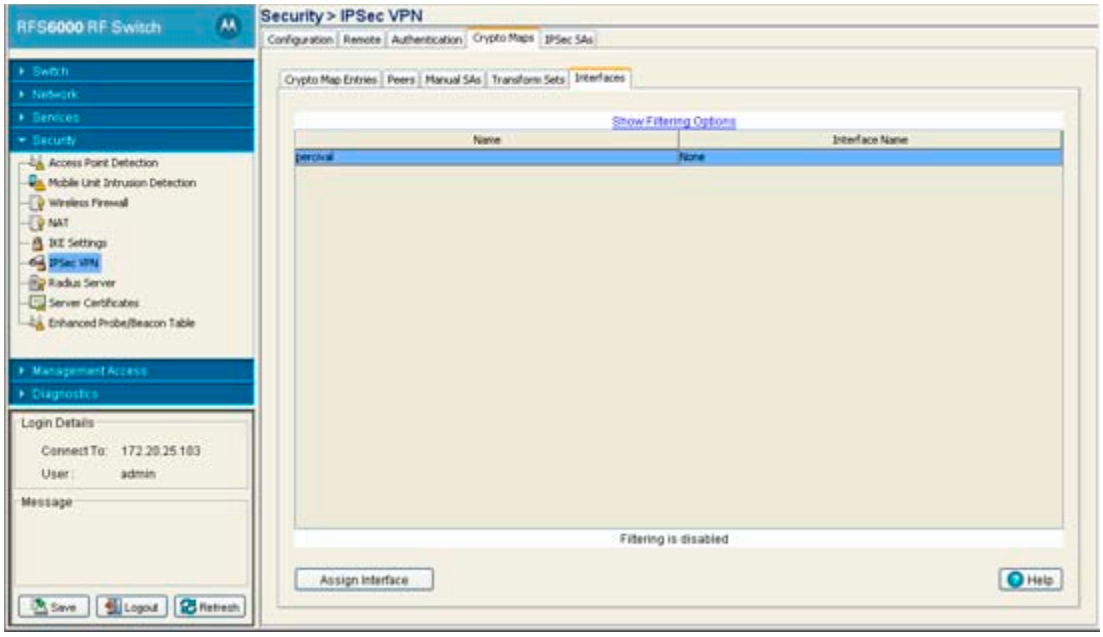
7. Click **OK** when completed to save the configuration of the Crypto Map transform set.

6.7.4.5 Crypto Map Interfaces

To review the interfaces currently available to the Crypto Maps or assign an interface:

NOTE: A Crypto Map cannot get applied to more than one interface at a time. To apply the same Crypto Map settings to multiple interfaces, create a unique Crypto Map for each interface.

1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Crypto Maps** tab and select **Interfaces**.



3. Refer to the following read-only information displayed within the **Interfaces** tab.

Name	Lists the name of the Crypto Maps available for the interface.
Interface Name	Displays the name of the interface through which IPSec traffic flows. Applying the Crypto Map set to an interface instructs the switch to evaluate all the interface's traffic against the Crypto Map set and to use the specified policy during connection or security association negotiation on behalf of traffic protected by crypto (either CET or IPSec).

4. Click the **Assign Interface** button to assign a Crypto Map to each interface through which IPSec traffic flows.

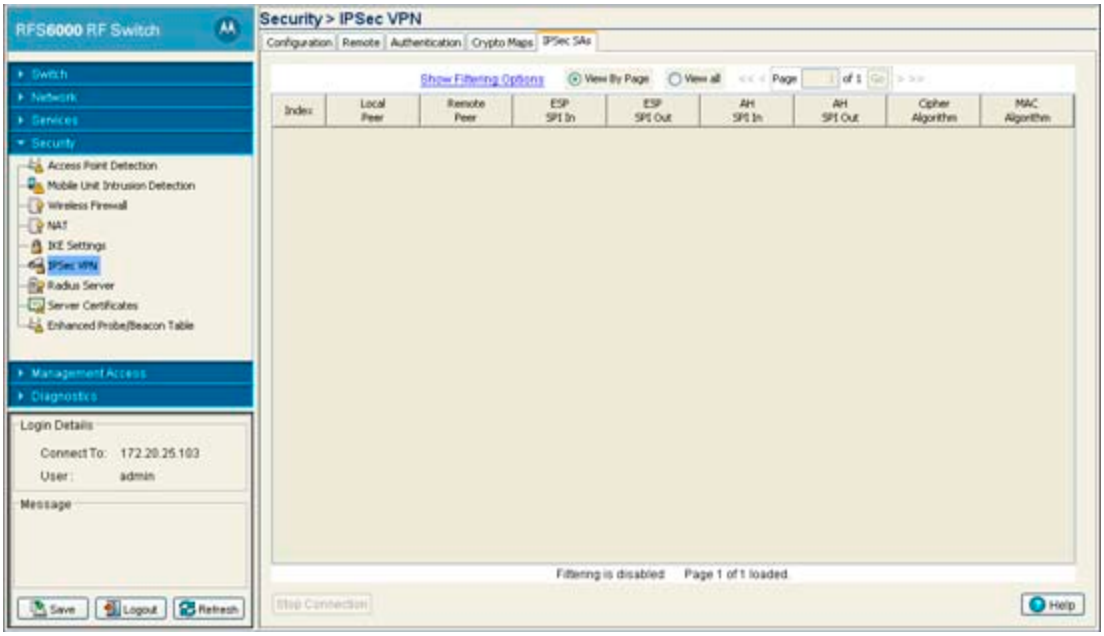
   Assigning the Crypto Map set to an interface instructs the security appliance to evaluate all the traffic against the Crypto Map set and use the specified policy during connection or SA negotiation. Assigning a Crypto Map to an interface also initializes run-time data structures (such as the SA database and the security policy database). Reassigning a modified Crypto Map to the interface resynchronizes the run-time data structures with the Crypto Map configuration. Also, adding new peers through the new sequence numbers and reassigning the Crypto Map does not break existing connections.

6.7.5 Viewing IPSec Security Associations

Refer to the **IPSec SAs** tab to review the various *security associations* (SAs) between the local and remote peers comprising an IPSec VPN connection. The IPSec SA tab displays the authentication and encryption schemes used between the VPN peers as well other device address information.

To display IPSec VPN security associations:

1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **IPSec SAs** tab.



3. Refer to the following security association data:

Index	Displays the numerical (if defined) ID for the security association. Use the index to differentiate the index from others with similar configurations.
Local Peer	Displays the name of the local peer at the near side of the VPN connection.
Remote Peer	Displays the name of the remote peer at the far side of the VPN connection.
ESP SPI In	SPI specified in the *Encapsulating Security Payload* (ESP) inbound header.
ESP SPI Out	SPI specified in the *Encapsulating Security Payload* (ESP) outbound header.
AH SPI In	Displays the inbound *Authentication Header* (AH).
AH SPI Out	Displays the outbound *Authentication Header* (AH).
Cipher Algorithm	Displays the algorithm used with the ESP cipher.
MAC Algorithm	Displays the algorithm used with the security association.

4. Use the page navigation facility (found on top of the table next to the **Show Filtering Options** link) to view the list of security associations.

   The switch can display a maximum of 600 security associations. To enable a search through the list, the **Security** > **IPSec VPN** screen provides a page navigation facility. Up to 30 security associations display per page.

   The following navigation and pagination options are available:

View All	Displays all SAs in one screen.
View By Page	Use this option to split the list into pages and view them one page at a time.

The following controls are enabled when the **View By Page** option is selected.

<<	Use this control to navigate to the first page.
<	Use this control to navigate to the previous page.
Page	Use this text box to enter the page number to jump directly to. This value cannot exceed the total number of pages.
Go	Use the Go button to jump to the page specified in the Page text box.
>	Use this control to navigate to the next page.
>>	Use this control to navigate to the last page.

5. If necessary, select a security association from those displayed and click the **Stop Connection** button to stop the security association.

6.8 Configuring the Radius Server

Remote Authentication Dial-In User Service (Radius) is a client/server protocol and software enabling remote access servers to communicate with the switch to authenticate users and authorize their access to the switch managed network. For an overview on the switch's Radius deployment, see *Radius Overview on page 6-83*.

Setting up Radius on the switch entails the following configuration activities:

- *Defining the Radius Configuration*
- *Configuring Radius Authentication and Accounting*
- *Configuring Radius Users*
- *Configuring Radius User Groups*
- *Viewing Radius Accounting Logs*

NOTE: For hotspot deployment, Motorola recommends using the switch's onboard Radius server and built-in user database. This is the easiest setup option and offers a high degree of security and accountability.

6.8.1 Radius Overview

Radius enables centralized management of switch authentication data (usernames and passwords). When a MU attempts to associate to the Radius supported switch, the switch sends the authentication request to the Radius server. The communications between the switch and server are authenticated and encrypted through the use of a shared secret password (not transmitted over the network).

The switch's local Radius server stores the authentication data locally, but can also be configured to use a remote user database. A Radius server as the centralized authentication server is an excellent choice for performing accounting. Radius can significantly increase security by centralizing password management.

NOTE: The switch can be configured to use its own local Radius server or an external Radius server you define and configure. For information on the benefits and risks of using the switch's resident Radius Server (as opposed to an external Radius Server), see *Using the Switch's Radius Server Versus an External Radius on page 6-85*.

CAUTION: When restarting or rebooting the switch, the Radius server is restarted regardless of its state before the reboot.

The Radius server defines authentication and authorization schemes for granting the access to wireless clients. Radius is also used for authenticating hotspot and remote VPN Xauth. The switch can be configured to use 802.1x EAP for authenticating wireless clients with a Radius server. The following EAP authentication types are supported by the switch's onboard Radius server:

- *TLS*
- *TLS and MD5*
- *TTLS and PAP*
- *TTLS and MSCHAPv2*
- *PEAP and GTC*
- *PEAP and MSCHAPv2*

Apart from EAP authentication, the switch allows the enforcement of user-based policies. User-based policies include dynamic VLAN assignment and access based on time of day.

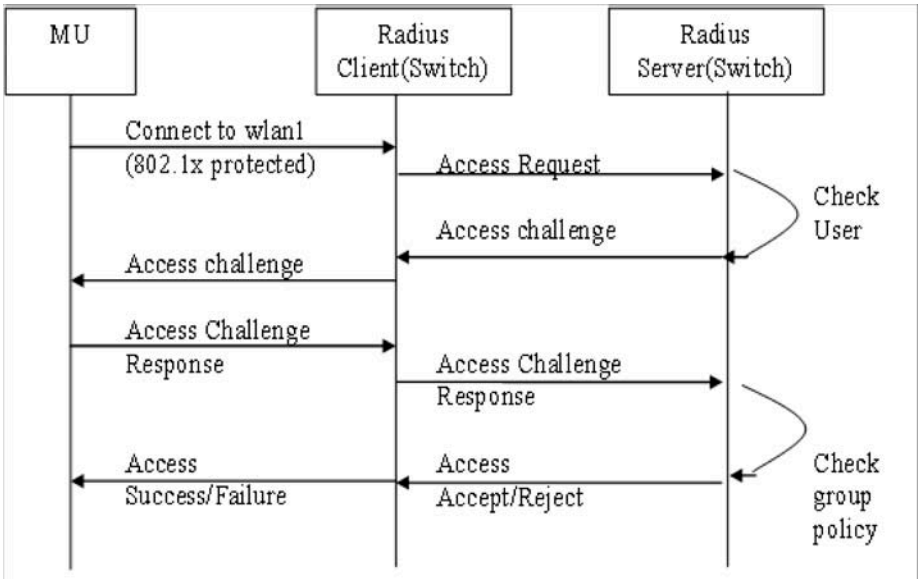
The switch uses a default trustpoint. A certificate is required for EAP TTLS,PEAP and TLS Radius authentication (configured with the Radius service).

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.

NOTE: For a Radius supported VLAN to function properly, the **Dynamic Assignment** checkbox must be enabled for the WLAN supporting the VLAN. For more information, see *Editing the WLAN Configuration on page 4-26*.

For 802.1x EAP authentication, the switch initiates the authentication process by sending an EAPoL message to the Access Port only after the wireless client joins the wireless network. The Radius client in the switch processes the EAP messages it receives. It encapsulates them to Radius access requests and sends them to the configured Radius server (in this case the switch's local Radius server).

The Radius server validates the user's credentials and challenge information received in the Radius access request frames. If the user is authorized and authenticated, the client is granted access by sending a Radius access accept frame. The frame is transmitted to the client in an EAPoL frame format.



6.8.1.1 User Database

User group names and associated users (in each group) can be created in the local database. The User ID in the received access request is mapped to the associated wireless group for authentication. The switch supports the creation of 500 users and 100 groups within its local database. Each group can have a maximum of 500 users.

6.8.1.2 Authentication of Terminal/Management User(s)

The local Radius server can be used to authenticate users. A normal user (with a password) should be created in the local database. These users should not be a part of any group.

6.8.1.3 Access Policy

Access policies are defined for a group created in the local database. Each user is authorized based on the access policies defined for the groups to which the user belongs. Access policies allow the administrator to control access to a set of users based on the WLANs (ESSID).

Group to WLAN access is controlled using a "Time of the day" access policy.

Consider User1 (part of Group 1), which is mapped to WLAN1 (ESSID of WLAN1). When the user tries to connect to WLAN1, the user is prompted to enter his/her credentials. Once the authentication and authorization phases are successful, only User1 is able to access WLAN1 for the allowed duration (but not any other WLAN). Each user group can be configured to be a part of one VLAN. All the users in that group are assigned the same VLAN ID if dynamic VLAN authorization has been enabled on the WLAN.

6.8.1.4 Proxy to External Radius Server

Proxy realms are configured on the switch, which has the details of the external Radius server to which the corresponding realm users are to be proxied. The obtained user ID is parsed in a (user@realm, realm/user, user%realm, user/realm) format to determine which proxy Radius server is to be used.

6.8.1.5 LDAP

An external data source based on LDAP can be used to authorize users. The Radius server looks for user credentials in the configured external LDAP server and authorizes users. The switch supports two LDAP server configurations.

6.8.1.6 Accounting

Accounting should be initiated by the Radius client. Once the Local/Onboard Radius server is started, it listens for both authentication and accounting records.

6.8.2 Using the Switch's Radius Server Versus an External Radius

The switch ships with a default configuration defining the local Radius Server as the primary authentication source (default users are admin with superuser privileges and operator with monitor privileges). No secondary authentication source is specified. However, Motorola recommends using an external Radius Server as the primary authentication source and the local switch Radius Server as the secondary user authentication source. For information on configuring an external Radius Server, see *Configuring External Radius Server Support on page 4-49*. For instructions on how to configure the switch's local Radius Server, see *Defining the Radius Configuration on page 6-86*.

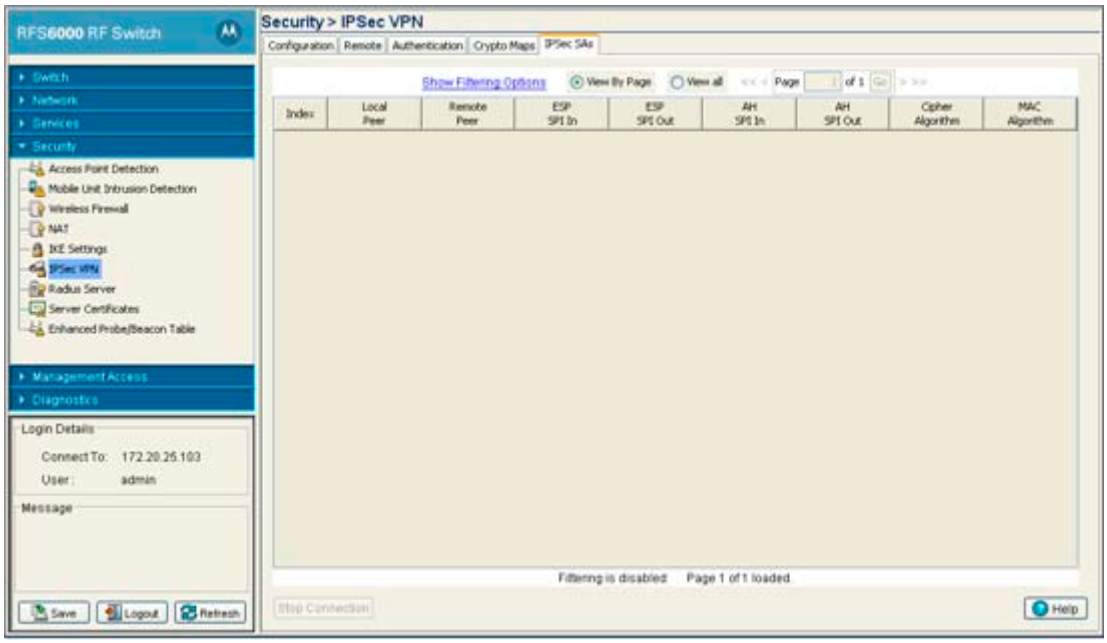
If an external Radius server is configured as the switch's primary user authentication source and the switch's local Radius Server is defined as an alternate method, the switch first tries to authenticate users using the external Radius Server. If an external Radius Server is unreachable, the switch reverts to the local Server's user database to authenticate users. However, if the external Radius server is reachable but rejects the user or if the user is not found in the external Server's database, the switch will not revert to the local Radius Server and the authentication attempt fails.

If the switch's local Radius Server is configured as the primary authentication method and an external Radius Server is configured as an alternate method, the alternate external Radius Server will not be used as an authentication source if a user does not exist in the local Server's database, since the primary method has rejected the authentication attempt.

6.8.3 Defining the Radius Configuration

To configure Radius support on the switch:

1. Select **Security** > **Radius Server** from the main menu.
2. Ensure the **Configuration** tab is selected.



3. Click the Start **the RADIUS server** link to use the switch's own Radius server to authenticate users accessing the switch managed network. Again, this is recommended as the secondary means of authenticating users.
4. Set a **Timeout** interval (between 5 and 10 seconds) to define how long the switch waits for a reply to a Radius request before retransmitting the request. The default value is 5.

   Ensure the value is set long enough to compensate for the heaviest periods of data traffic within the switch managed network.
5. Set a **Retires** value (between 3and 6) to define the number of times the switch transmits each Radius request to the server before giving up. The default value is 3.
6. Click the **Apply** button to save the changes made to within the Global Settings field.
7. Click the **Revert** button to cancel any changes made within the Global Settings field and revert back to the last saved configuration.

NOTE: The appearance of the bottom portion of the Configuration tab differs depending on whether **Clients** or **Proxy Servers** is selected. Select the **Clients** tab to display the IP Address and Subnet Mask of existing Radius clients. Existing clients can be modified or new clients added. For more information, see *Radius Client Configuration on page 6-87*. Select the **Proxy Servers** tab to display the ID suffix, IP address and Port Number of existing Radius proxy servers. Existing servers can be modified or new proxy servers added. For more information, see *Radius Proxy Server Configuration on page 6-87*.

6.8.3.1 Radius Client Configuration

A Radius client implements a client/server mechanism enabling the switch to communicate with a central server to authenticate users and authorize access to the switch managed network. A Radius client is often an embedded device since it alleviates the need to store detailed user information locally.

To configure Radius client support:

1. Select **Security** > **Radius Server** from the main menu.
2. Ensure the **Configuration** tab is selected.
3. Select the **Clients** tab from the bottom portion of the Configuration tab.

   The Clients tab displays the IP address and subnet mask of existing Radius clients.
4. To edit an existing Radius client configuration, select it from the table and click the **Edit** button.

   The Edit screen displays the Radius client's existing IP address, subnet mask and shared secret password used for credential verification. Modify these settings as required.
5. To remove an existing Radius client configuration from the table of configurations available to the switch, select a configuration and click the **Delete** button.
6. To create a new Radius client configuration, click the **Add** button at the bottom of the screen.

   a. Specify the **IP Address/Mask** of the subnet or host authenticating with the Radius client.

   b. Specify a Radius **Shared Secret** for authenticating the RADIUS client.
   Shared secrets used to verify Radius messages (with the exception of the Access-Request message) are sent by a Radius -enabled device configured with the same shared secret. The shared secret is a case-sensitive string that can include letters, numbers, or symbols. Make the shared secret at least 31 characters to protect the Radius server from brute-force attacks.

   c. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something is wrong in the transaction between the applet and the switch.

   d. Click **OK** to use the changes to the running configuration and close the dialog.

   e. Click **Cancel** to close the dialog without committing updates to the running configuration

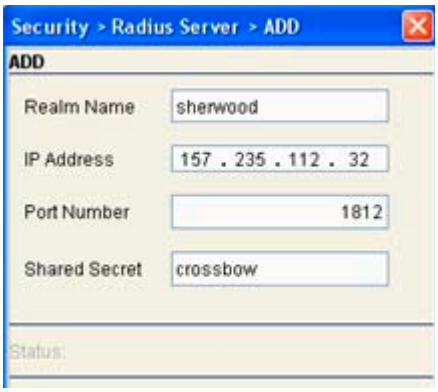
6.8.3.2 Radius Proxy Server Configuration

The switch can be configured to send Radius requests to a proxy radius server. A user's access request is sent to a proxy server if it cannot be authenticated by a local server. The proxy server forwards the access request to a proxy server that can authenticate the user. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy target server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

To configure Radius proxy server support:

1. Select **Security** > **Radius Server** from the main menu.
2. Ensure the **Configuration** tab is selected.
3. Select the **Proxy Servers** tab from the bottom of the Configuration tab.

   The Proxy Servers tab displays the user ID suffix (index), IP address and port number of the switch's existing proxy server configurations.
4. To remove an existing Radius proxy server configuration from the table of configurations available to the switch, select the configuration and click the **Delete** button.
5. Click the **Add** button at the bottom of the screen to create a new Radius proxy server configuration.



   a. Create a new **Realm Name** as an abbreviation to differentiate the configuration from others with similar attributes.

   b. Specify the **IP Address** of the new Radius proxy server.

   c. Enter the TCP/IP **Port Number** used by the proxy Radius server.

   d. Specify a Radius **Shared Secret** for authenticating the Radius client.

      The shared secret is used to verify Radius messages. It is a case-sensitive string that can include letters, numbers, or symbols. Make the shared secret at least 31 characters long to protect the Radius server from brute-force attacks.

   e. Shared secrets verify Radius messages (with the exception of the Access-Request message) are sent by a Radius-enabled device configured with the same shared secret.

      The shared secret is a case-sensitive string that can include letters, numbers, or symbols. Make the shared secret at least 22 characters long to protect the Radius server from brute-force attacks. The max length of the shared secret is 31 characters.

   f. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

   g. Click **OK** to use the changes to the running configuration and close the dialog.

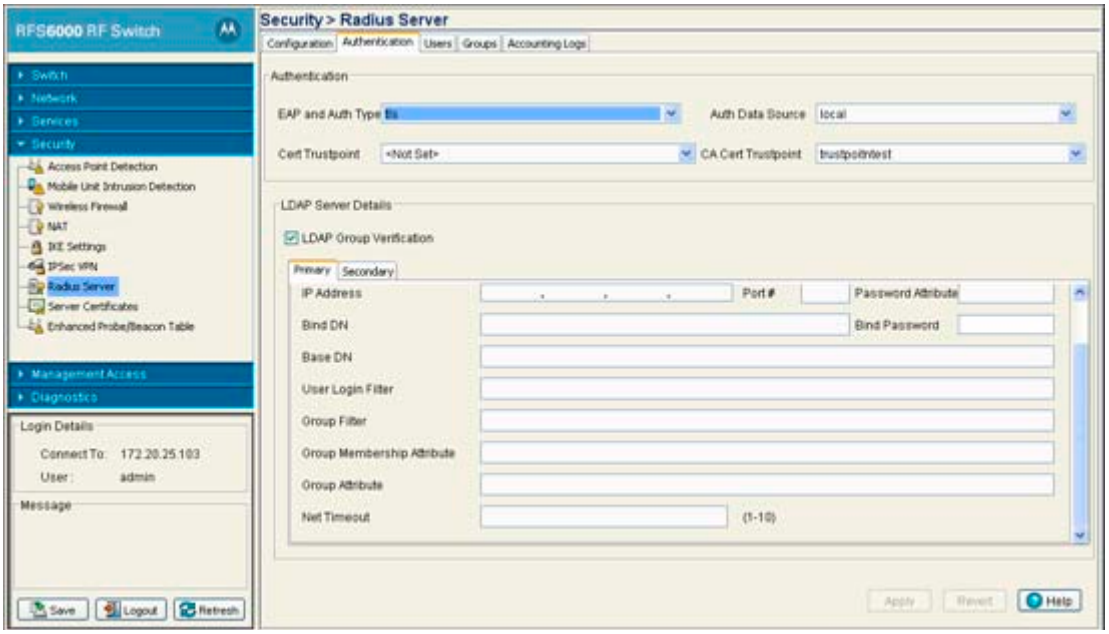
   h. Click **Cancel** to close the dialog without committing updates to the running configuration

6.8.4 Configuring Radius Authentication and Accounting

Deploy one or more Radius servers to manage security and retrieve accounting information from the switch managed network. Radius accounting supplies administrators with user data as Radius sessions are started and terminated.

To define the Radius authentication and accounting configuration:

1. Select **Security** > **Radius Server** from the main menu.
2. Select the **Authentication** tab.



3. Refer to the **Authentication** field to define the following Radius authentication information:

EAP and Auth Type Specify the EAP type for the Radius server.

- *PEAP* uses a TLS layer on top of EAP as a carrier for other EAP modules. PEAP is an ideal choice for networks using legacy EAP authentication methods.
- *TTLS* is similar to EAP-TLS, but the client authentication portion of the protocol is not performed until after a secure transport tunnel has been established. This allows EAP-TTLS to protect legacy authentication methods used by some Radius servers.

Auth Data Source Use **Auth Data Source** drop-down menu to select the data source for the local Radius server.

- If *Local* is selected, the switch's internal user database serves as the data source for user authentication. Refer to the **Users** and **Groups** tabs to define user and group permissions for the switch's local Radius server.
- If *LDAP* is selected, the switch uses the data within an LDAP server.

Cert Trustpoint	Click the **View/Change** button to specify the trustpoint from which the Radius server automatically grants certificate enrollment requests. A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. If the server certificate trustpoint is not used, the default trustpoint is used instead.
CA Cert Trustpoint	Click the **View/Change** button to specify the CA certificate trustpoint from which the Radius server automatically grants certificate enrollment requests. A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. If a CA trustpoint is not specified, the "default trustpoint's CA certificate is used as a CA certificate. If the "Default trustpoint" does not have a CA certificate, the server certificate is used as the CA certificate.

NOTE: EAP-TLS will not work with a default trustpoint. Proper CA and Server trustpoints must be configured for EAP-TLS. For information on configuring certificates for the switch, see *Creating Server Certificates on page 6-97*.

4. Refer to the **LDAP Server Details** field to define the primary and secondary Radius LDAP server configuration providing access to an external database used with the local Radius server.

IP Address	Enter the IP address of the external LDAP server acting as the data source for the Radius server. This server must be accessible from an active switch subnet.
Port	Enter the TCP/IP port number for the LDAP server acting as the data source.
Password Attribute	Enter the password attribute used by the LDAP server for authentication.
Bind DN	Specify the distinguished name to bind with the LDAP server.
Bind Password	Enter a valid password for the LDAP server.
Base DN	Specify a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.
User Login Filter	Enter the login used by the LDAP server for authentication.
Group Filter	Specify the group filters used by the LDAP server.
Group Membership Attribute	Specify the Group Member Attribute sent to the LDAP server when authenticating users.
Group Attribute	Specify the group attribute used by the LDAP server.
Net Timeout	Enter a timeout value (between 1-10 seconds) the system uses to terminate the connection to the Radius Server if no activity is detected.

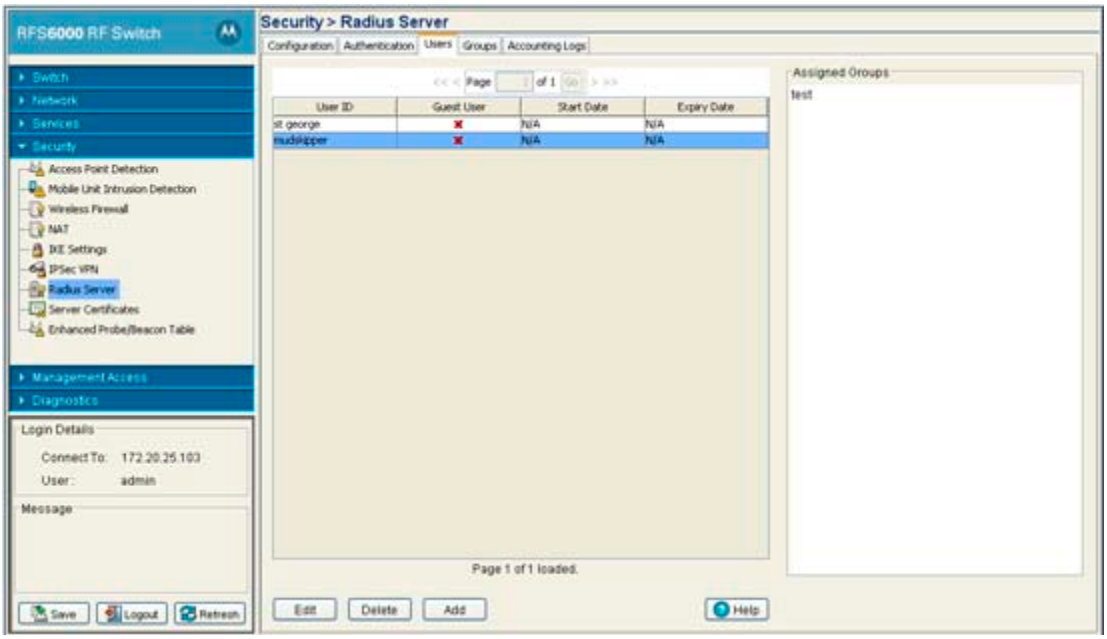
5. Click the **Apply** button to save the changes made to within the screen.
6. Click the **Revert** button to cancel any changes made within the screen and revert back to the last saved configuration.

6.8.5 Configuring Radius Users

Refer to the **Users** tab to view the current set of users and groups assigned for the Radius server. The Users tab is employed when **Local** is selected as the Auth Data Source within the **Authentication & Accounting** tab. The user information is ignored if an LDAP server is used for authentication.

To define the Radius user permissions for switch access:

1. Select **Security** > **Radius Server** from the main menu.
2. Select the **Users** tab.



3. Refer to the following to assess whether an existing user can be used with the local Radius server as is, requires modification or if a new user is required.

User ID	Displays the username for this specific user. The name assigned should reflect the user's identity and perhaps their status within the switch managed network (guest versus secure user).
Guest User	Displays whether a specific user has been defined as a guest user (with a green check) or has been configured as permanent user. Guest users have temporary access.
Group Name	Lists the group name that was assigned to the Radius User ID and Group.
Start Date	Defines the time when Guest User's privileges commence.
Expiry Date	If the user has been assigned guest privileges, they were also assigned a date when their Radius privileges expire.

4. Refer to the **Available Groups** field to view the memberships for existing users.

   If the group assignment is insufficient, use the **Edit** or **Add** functions to modify/create users or modify their existing group assignments. For guest users, only the password is editable. For normal (non-guest) users, the password and group association can be modified.
   To modify the attributes of an existing user, select the user from the list and click the **Edit** button.

Modify the existing user's guest designation, password, expiry date and group assignments as required to reflect the user's current local Radius authentication requirements.

5. If an existing user is no longer needed, select the user from those displayed and click the **Delete** button to permanently remove the user.
6. To create a new user for use with the local Radius server, click the **Add** button and provide the following information.

CAUTION: If password encryption is not enabled, Radius user passwords are stored in the running configuration file in clear text. The user passwords are shown as encrypted if the global password encryption is enabled. The maximum for the file is 5000 users, 100 groups, 25 clients, 5 realms and 2 LDAP servers.

User ID	Define a unique user ID that differentiates this user from others with similar attributes.
Guest User	Select the **Guest User** checkbox to assign this particular user temporary access to the local Radius server, thus restricting their authentication period to a user defined interval.
Password	Enter the password that adds the user to the list of approved users displayed within the Users tab.
Confirm Password	Re-enter (confirm) the password used to add the user to the list of approved users displayed within the Users tab.
Current Switch Date	Displays the read only switch time. This is the time used for expiry data and time.sers tab.
Start Date & Time	Defines the start date and time (in dd:MM:yyyy-hh:mm format) to login guest users defined with temporary (guest) permissions.
Expiry Date & Time	Defines the date and time (in dd:MM:yyyy-hh:mm format) to timeout guest users defined with temporary (guest) permissions.
Available Groups	Use the Available Groups **Add ->** and **Remove <-** functions to map groups (for inclusion) for this specific user.
Configured Group	Displays existing groups available for the user.

a. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

b. Click **OK** to use the changes to the running configuration and close the dialog.

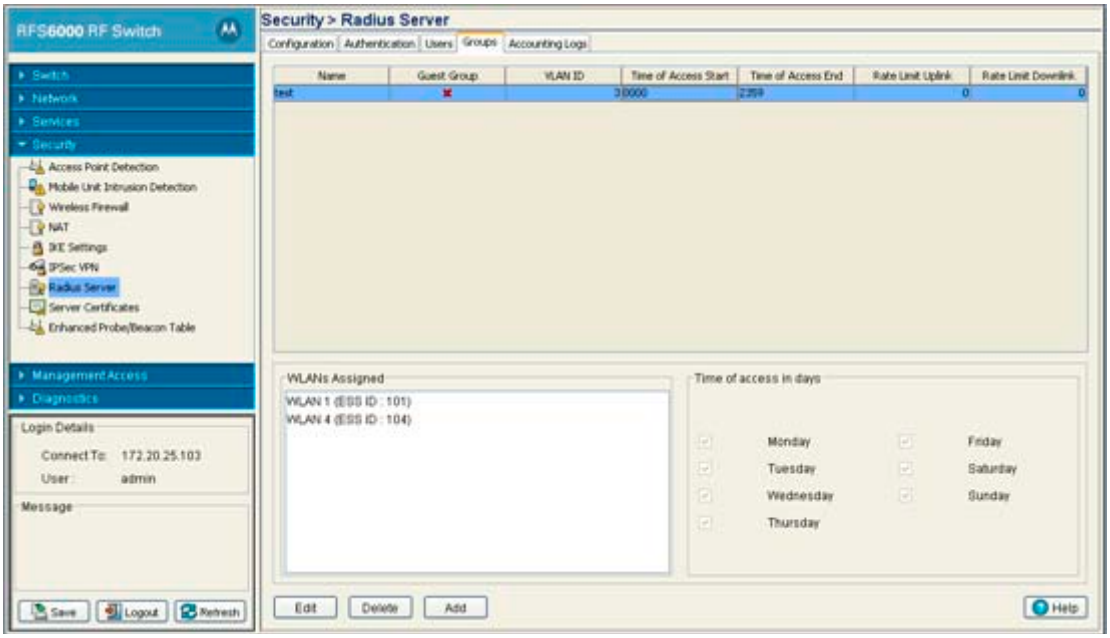
c. Click **Cancel** to close the dialog without committing updates to the running configuration

6.8.6 Configuring Radius User Groups

The **Groups** tab displays a list of all groups in the local Radius server's database. The groups are listed in the order added. The existing configuration for each group is displayed to provide the administrator the option of using a group as is, modifying an existing group's properties or creating a new group.

To access the configuration of existing user groups:

1. Select **Security** > **Radius Server** from the main menu.
2. Select the **Groups** tab.



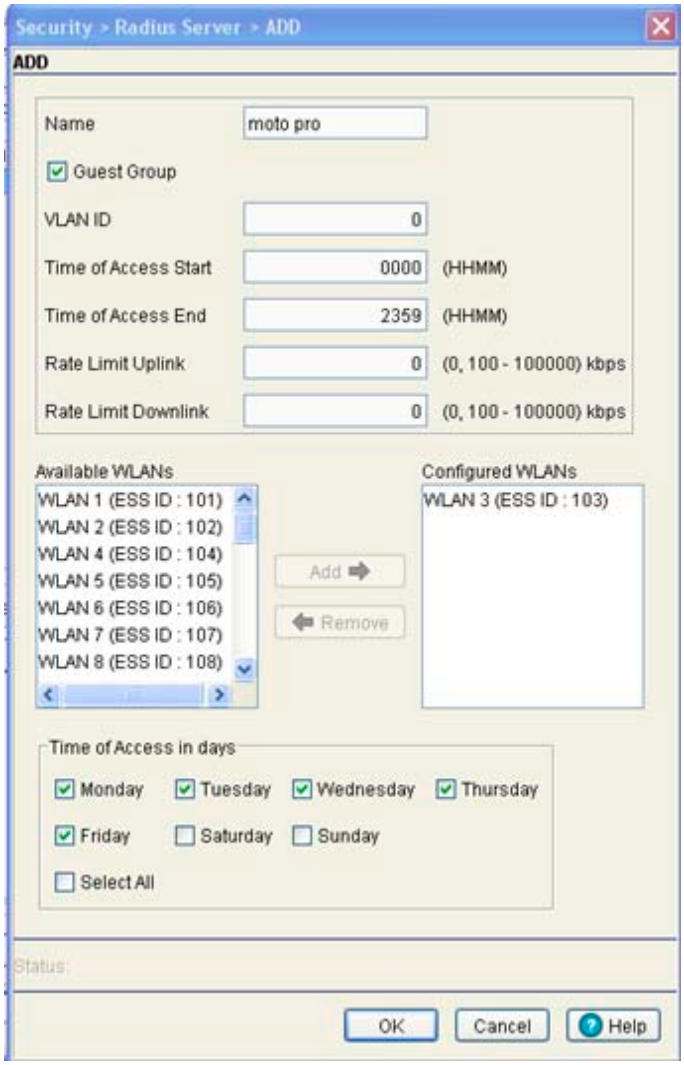
3. Refer to the user groups listed to review the following read-only attributes for each group:

Name	Displays the unique name assigned to each group. The group name should be indicative of the user population within and their shared activity within the switch managed network.
Guest Group	Displays whether a specific group has been defined as a guest group (indicated with a green check mark) or has been configured as permanent group (indicated with a red X). Guest users have temporary Radius server access.
VLAN ID	Display the VLAN ID(s) used by each group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate with one another within the switch managed network (once authenticated by the local Radius server).
Time of Access Start	Displays the time each group is authenticated to interoperate within the switch managed network. Each user within the group is authenticated with the local Radius server. Group members successfully authenticated are allowed access to the switch managed network under the restrictions defined for that group.
Time of Access End	Displays the time each group's user base will loose access privileges. After this time, users within this group will not be authenticated by the local Radius server. However, if a user is part of a different group that has not exceeded their access interval, then the user may still interoperate with the switch (remain authenticated) as part of that group.
Rate Limit Uplink	Displays the data (in kbps) allowed for this group (in the uplink direction from clients) when the group was created or edited.
Rate Limit Downlink	Displays the data (in kbps) allowed for this group (in the downlink direction from clients) when the group was created or edited.

4. Refer to the **WLANs Assigned** area of the Groups tab to review which switch WLANs are available for use with configured groups.

5. Refer to the **Time of access in days** field to assess the intervals (which days) the group has been assigned access to the switch managed network (after each user has been authenticated). At least one day is required.

   This value is read-only within the Groups tab. Click **Edit** to modify the access assignments of an existing group or click **Add** to create a new group with unique access assignments.



6. To modify the attributes of an existing group, select the group from the list of groups displayed and click the **Edit** button.

   Modify the existing group's guest designation, VLAN ID, access period(s) and WLAN assignment(s).

7. If an existing group is no longer needed (perhaps obsolete in function), select the group and click the **Delete** button to permanently remove the group from the list. The group can only be removed if all the users in the group are removed first.

8. To create a new group, click the **Add** button and provide the following information.

Name	Define a unique group name that differentiates this new group from others with similar attributes.
Guest Group	Select the **Guest Group** checkbox to assign this particular group (and the users within) only temporary access to the local Radius server, thus restricting their authentication period to a user defined access interval.
VLAN ID	Define the VLAN ID for the new group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the switch managed network (once authenticated by the local Radius server).
Time of Access Start	Set the time the group is authenticated to interoperate. Each user within the group is authenticated with the local Radius server. Those group members successfully authenticated are allowed access to the switch using the restrictions defined for the group.
Time of Access End	Set the time each group's user base will loose access privileges within the switch managed network. After this time, users within this group will not be authenticated by the local Radius server. However, if a user is part of a different group that has not exceeded their access end interval, the user may still interoperate with the switch (remain authenticated) as part of that group.
Rate Limit Uplink (0,100-100000)	Set the rate limit from the wireless client to the network when using Radius authentication. A rate limit of 0 disables rate limiting for this direction. Any rate limit obtained through radius server authentication overwrites the initial user rate limit for the given MU.
Rate Limit Downlink (0,100-100000)	Set the rate limit from the network to the wireless client when using Radius authentication. Any rate limit obtained through radius server authentication overwrites the initial user rate limit for the given MU.
Available WLANs	Use the Available WLANs **Add ->** and **Remove <-** functions to move WLANs for this new group from the available list to the configured list. Once on the configured list (and the changes applied), the members of this group can interoperate with the switch on these WLANs (once authenticated by the local Radius server).
Configured WLANs	The Configured WLANs columns displays the WLANs this new group can operate within (once users are configured). Use the **Add ->** and **Remove <-** functions to move WLANs from the available list to the configured list.
Time of access in days	Select the checkboxes corresponding to the days of the week you would like this new group to have access to the switch managed network. Of course, the user base within the group still needs to be authenticated by the local Radius server first.

NOTE: Rate limiting parameters need to be part of Radius Access Accept packets. If any radius server doesn't send rate limit parameters in Radius Access Accept packet, these parameters will not be configured.

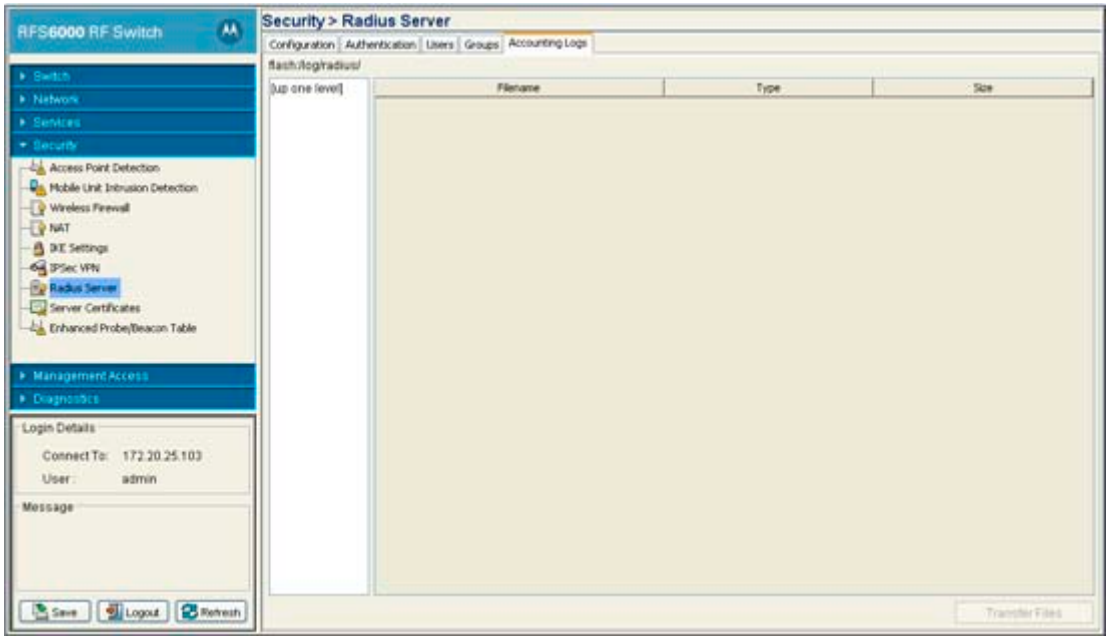
9. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
10. Click **OK** to use the changes to the running configuration and close the dialog.
11. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.8.7 Viewing Radius Accounting Logs

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 location outside of the switch for periodic network and user permission administration.

To display the Radius accounting logs:

1. Select **Security** > **Radius Server** from the main menu.
2. Select the **Accounting Logs** tab.



3. Refer to the following information as displayed within the **Accounting Logs** tab.

Filename	Displays the name of each accounting log file. Use this information to differentiate files with similar attributes.
Type	Displays the type of file each file is.
Size	Display the size of the file.

NOTE: An explicit purge operation is not supported, the accounting logs are purged automatically once they reach their limit.

6.9 Creating Server Certificates

Use the **Server Certificates** screen to view existing self-signed certificate values. The values displayed are read-only. The Server Certificates screen also allows an administrator to:

- *create a certificate request*
- *send it to a Certificate Authority (CA)*
- *create a self signed certificate*

- *upload an external certificate*
- *delete a server certificate and/or root certificate of a trustpoint*
- *create a new key*
- *upload/download keys to and from the switch to and from a server or local disk*
- *delete all the keys in the switch.*

Server certificates are issued to Web Servers and used to authenticate Web Servers to browsers while establishing a Secure Socket Layer (SSL) connection.

The **Server Certificates** screen displays two tabs supporting the following:

- *Using Trustpoints to Configure Certificates*
- *Configuring Trustpoint Associated Keys*

6.9.1 Using Trustpoints to Configure Certificates

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.

To view current certificates values:

1. Select **Security** > **Server Certificates** from the main menu tree.
2. Select the **Trustpoints** tab.

A panel (on the far left of the screen) displays currently enrolled trustpoints.

The **Server Certificate** and **CA Root Certificate** tabs display read-only credentials for the certificates in use by the switch. A table displays the following **Issued To** and **Issued By** details for each:

Issued To	
Country (C)	Displays the country of usage for which the certificate was assigned.
State (ST)	Displays the state (if within the US) or province within the country listed above wherein the certificate was issued.
City (L)	Lists the city wherein the server certificate request was made. The city should obviously be within the State/Prov stated.
Organization (O)	Displays the name of the organization making the certificate request.
Organizational Unit (OU)	Displays the name of the organizational unit making the certificate request.
Common Name (CN)	If there is a common name (IP address) for the organizational unit making the certificate request, it displays here.
Issued By	
Country (C)	Displays the country of the certificate issuer.
State (ST)	Displays the state or province for the country the certificate was issued.
City (L)	Displays the city representing the state/province and country from which the certificate was issued.
Organization (O)	Displays the organization representing the certificate authority
Organizational Unit	If a unit exists within the organization that is representative of the certificate issuer, that name should be displayed here.
Common Name	If there is a common name (IP address) for the organizational unit issuing the certificate, it displays here.
Validity	
Issued On	Displays the date the certificate was originally issued.
Expires On	Displays the expiration date for the certificate.

3. Click the **Certificate Wizard** button to create a self signed certificate, upload an external server certificate (and/or a root certificate) or delete a server certificate (and/or a root certificate) of a trustpoint. For more information, see *Using the Wizard to Create a New Certificate on page 6-100*.

6.9.1.1 Creating a Server / CA Root Certificate

To create a Server Certificate or import a CA Root Certificate:

1. Select **Security** > **Server Certificates** from the main menu tree.

2. Click the **Certificate Wizard** button on the bottom of the screen.
3. Use this wizard for:
   - *Creating a new self-signed certificate or certificate request*
   - *Uploading an external certificate*
   - *Delete Operations*
4. Select the **Create new certificate** radio button to generate a new self-signed certificate or prepare a certificate request which can be sent to a Certificate Authority (CA).

   For more information, see *Using the Wizard to Create a New Certificate on page 6-100*.
5. Select the **Upload an external certificate** radio button to upload an existing Server Certificate or CA Root Certificate.

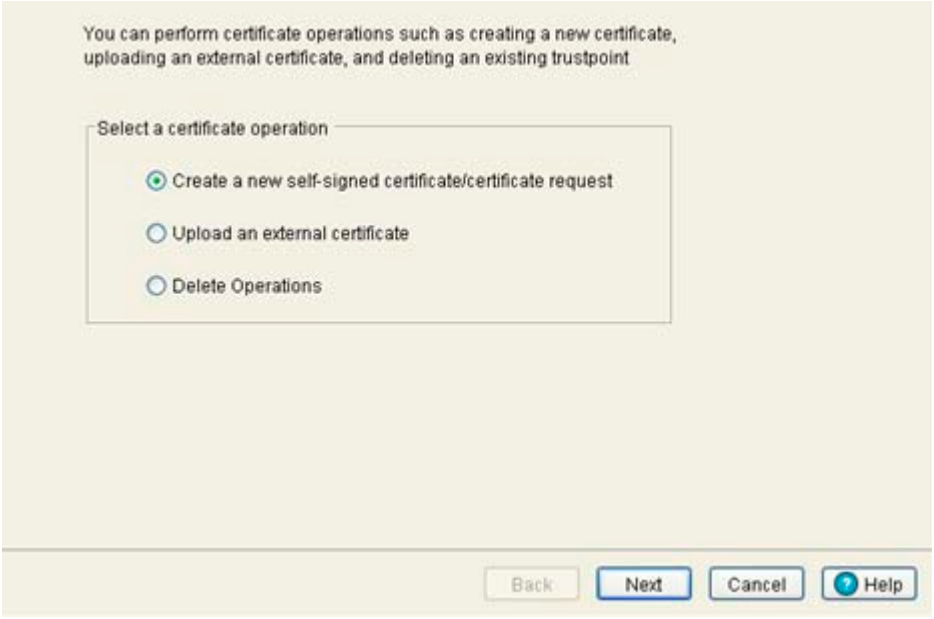
   For more information, see *Using the Wizard Delete Operation on page 6-105*.
6. Select the **Delete Operations** radio button to delete trustpoints and all related keys.

   For more information, see *Using the Wizard Delete Operation on page 6-105*.

Using the Wizard to Create a New Certificate

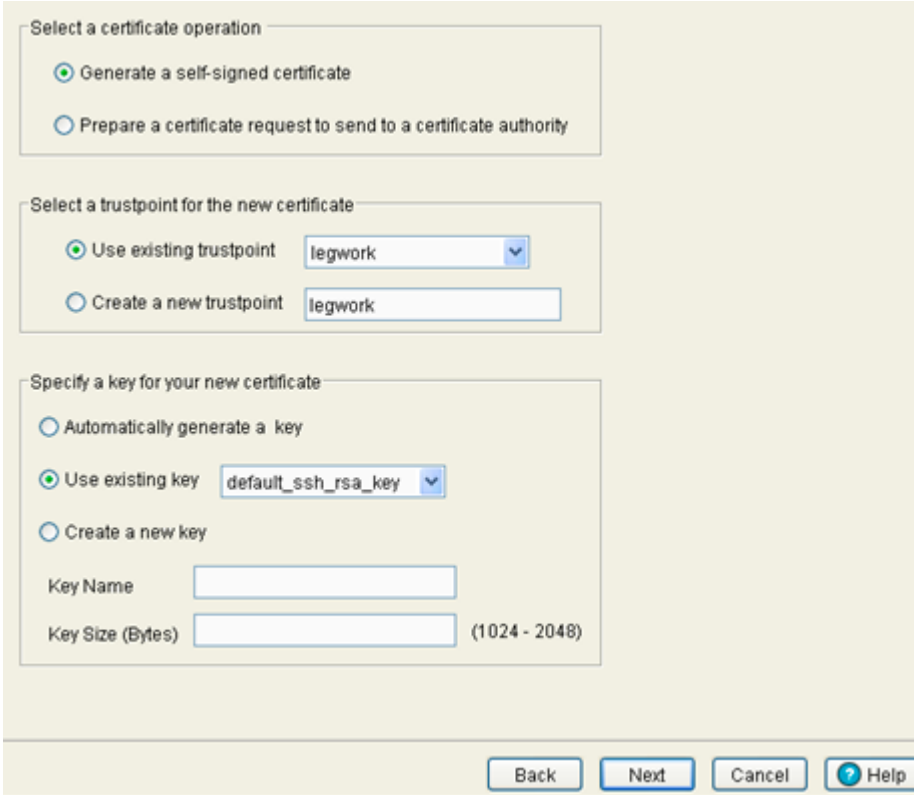
To generate a new self-signed certificate or prepare a certificate request:

1. Select the **Create new self-signed certificate /certificate request** radio button in the wizard and click the **Next** button



The second page of the wizard contains three editable fields, **Select Certificate Operation**, **Select a Trustpoint**, and **Specify a key for you new certificate**.

2. Use the second page to create either a self signed certificate or prepare a certificate request. For certificate creation, select one of the following options:
   - *Generate a self signed certificate* — Configure the properties of a new self-signed certificate. Once the values of the certificate are defined, the user can create and install the certificate.
   - *Prepare a certificate request to send to a Certificate Authority* — Configure and save a valid certificate request. Once the values of the certificate are defined, the user can configure and enroll the trustpoint.



Select a trustpoint for the new certificate.

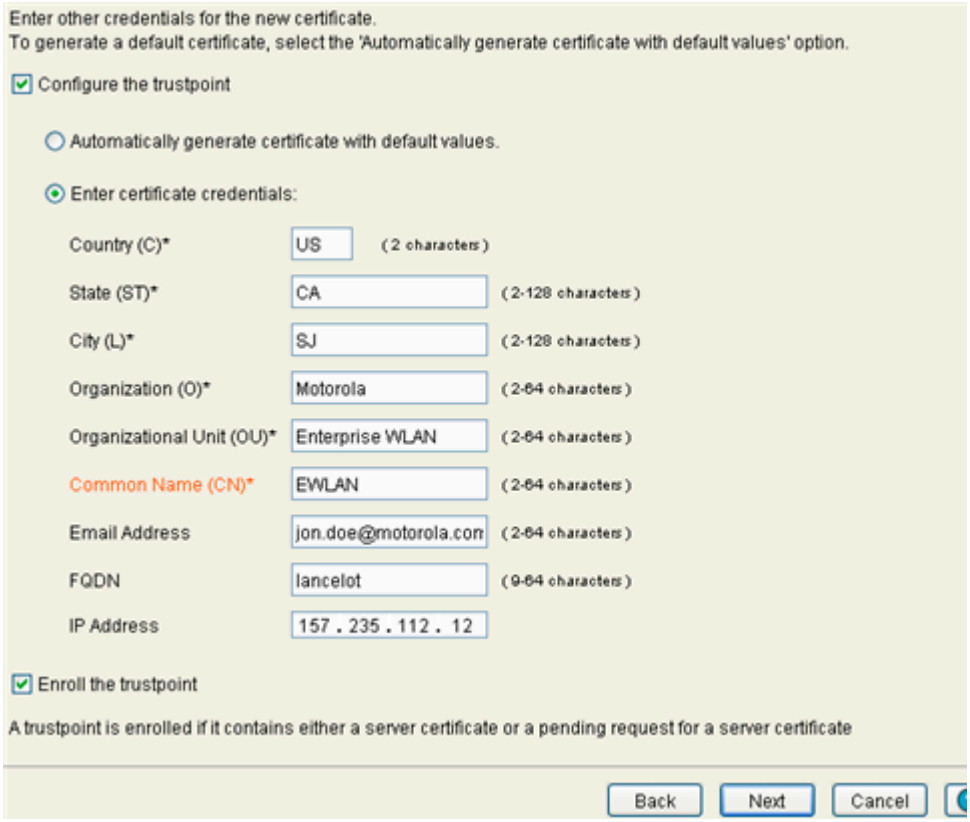
- *Use existing trustpoint* - Select an existing trustpoint from the drop-down menu.
- *Create a new trustpoint* - Provide a name for the new trustpoint in the space provided.

To specify a key for a new certificate, select one of the following:

- *Automatically generate a key* — Automatically generates a key for the trustpoint.
- *Use existing key* — Specify an existing key using the drop-down menu.
- *Use a new key* — Select this option to create a new key for the trustpoint. Define a key name and size as appropriate.

Associate the certificate selected with one of the options provided in the *Specify a key for your new certificate* and click the **Next** button.

If generating a new self-signed certificate (as selected in page 2 of the wizard), the wizard continues the installation. Use the third page of the wizard to enter a unique trustpoint name and other credentials required to create the new certificate.



3. Select the **Configure the trustpoint** checkbox to enable the new self signed certificate configured as a trustpoint.
4. Select the **Automatically generate certificate with default values** checkbox to create a certificate using values the switch assigns by default.

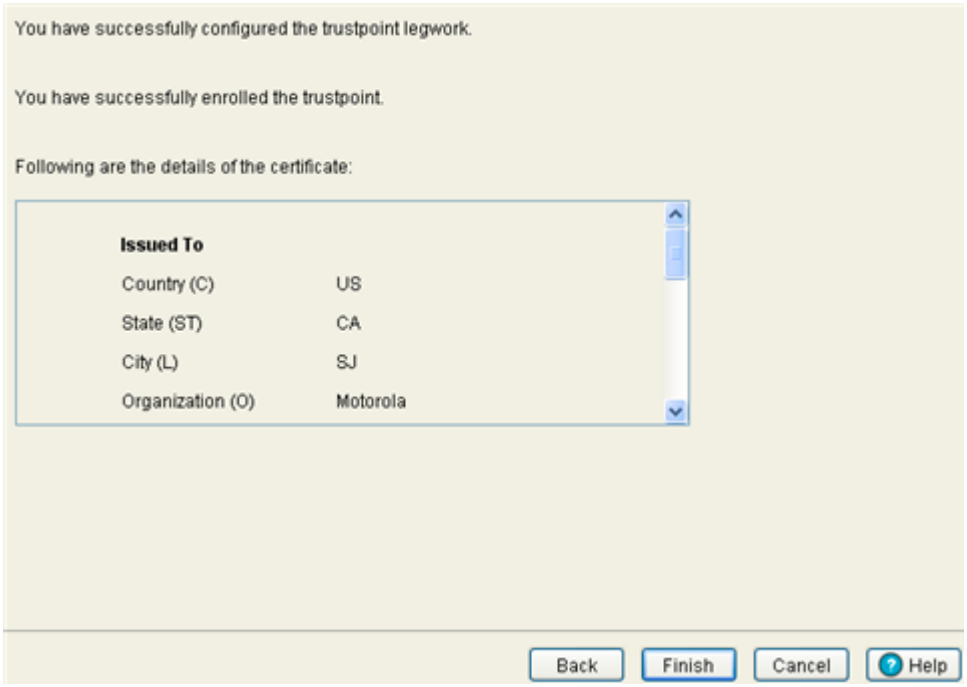
   This option is recommended for generic certificates that do not represent a unique or custom switch configuration.
5. Select the **Enter certificate credentials** radio button to manually enter the values of a unique certificate. If you anticipate using generic (default) values, consider using the Automatically generate certificate with default values option.
6. Provide the following information for the certificate:

Country	Define the Country used in the Self-Signed Certificate. By default, the Country is US. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.
State	Enter a State/Prov. for the state or province name used in the Self-Signed Certificate. By default, the State/Prov. field is CA. This is a required field.
City	Enter a City to represent the city name used in the Self-Signed Certificate. By default, the City name is San Jose. This is a required field.
Organization	Define an Organization for the organization used in the Self-Signed Certificate. By default, it is Motorola, Inc. The user is allowed to modify the Organization name. This is a required field.

Organization Unit	Enter an Org. Unit for the name of the organization unit used in the Self-Signed Certificate. By default, it is Wireless Switch Division. This is a required field.
Email Address	Provide an email address used as the contact address for issues relating to this certificate request.
FQDN	Enter a *fully qualified domain name* (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.
IP Address	Specify the switch IP address used as the switch destination for certificate requests.

7. Select the **Enroll the trustpoint** checkbox to enroll the certificate request with the CA.
8. Click **Next** to proceed with the certificate creation.

   If you created a self-signed certificate on page 2, the wizard completes and displays the details of the newly created self-signed certificate.



   If you selected to prepare a certificate request in the page 2, the wizard continues, prompting the user for the required information to complete the certificate request. Click **Next** to continue.
9. Check the **Copy the certificate request to clipboard** option to add the contents of the certificate request to the clipboard which can then be copied to other locations.

10. Check the **Save the certificate request option** to save the certificate request to an external server.and provide the server information in the fields below:

To	Use the **To** field to define whether the target certificate is to be sent to the system's local disk (**Local Disk)** or to an external server (**Server**).
File	Specify a filename for the certificate to be save as on the target server or local disk.
Using	Use the Using drop down-menu to configure whether the log file transfer is sent using **FTP** or **TFTP**.
IP Address	Specify the server **IP Address** used as the switch destination for certificate requests.
User ID	Enter the **User ID** credentials required to send the file to the target location. Use the User ID for FTP transfers only
Password	Enter the **Password** required to send the file to the target location using FTP.
Path	Specify the appropriate **Path** name to the target directory on the local system disk or server as configured using the "To" parameter.

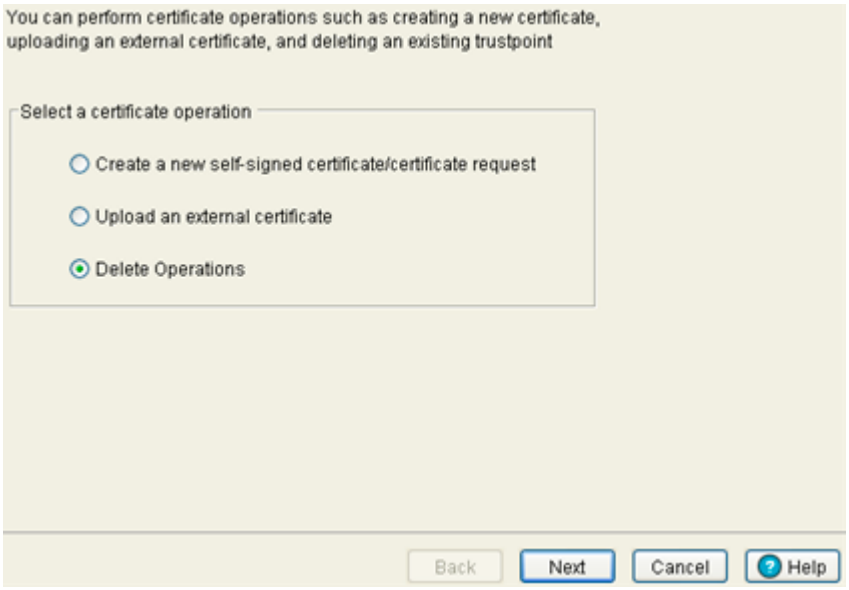
11. Click the **Next** button to complete the certificate request.

Using the Wizard Delete Operation

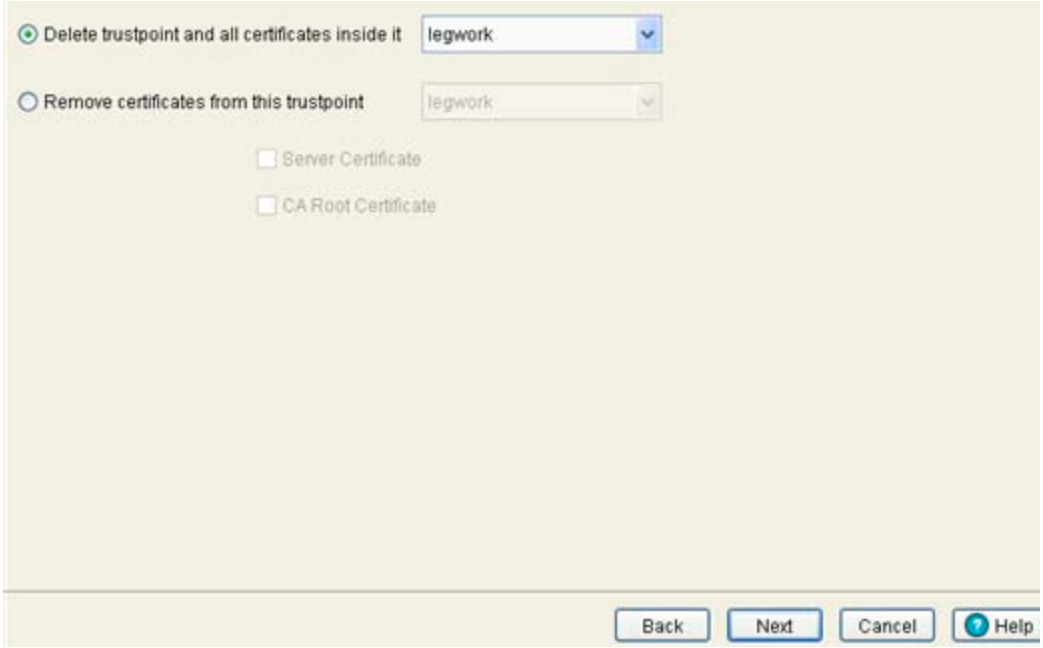
The wizard can also be used to delete entire trustpoints, the certificate used with a trustpoint or the CA root certificate use with a trustpoint. Delete trustpoint properties as they become obsolete or the properties of a certificate are no longer relevant to the operation of the switch.

To use the wizard to delete trustpoint properties:

1. Select the **Delete Operations** radio button and click the **Next** button.



The next page of the wizard is used to delete a trustpoint.



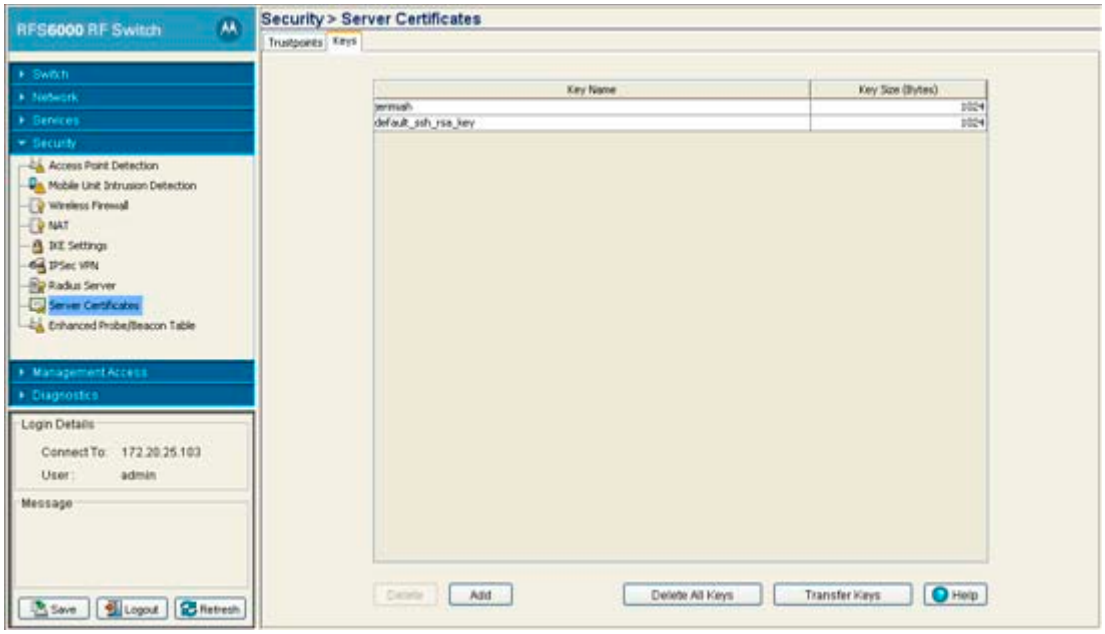
2. Select and use the **Delete trustpoint and all certificates inside it** drop-down menu to define the target trustpoint for removal.
3. Select and use the **Remove certificates from this trustpoint** drop-down menu define the trustpoint that will have either its **Server Certificate** or **CA Root Certificate** removed
4. Click the **Next** button to proceed and complete the trustpoint removal.

6.9.2 Configuring Trustpoint Associated Keys

Trustpoint keys allow a user to use different *Rivest, Shamir*, an *Adelman* (RSA) key pairs. Therefore, the switch can maintain a different key pair for each certificate to significantly enhance security.

To configure the keys associated with trustpoints:

1. Select **Security** > **Server Certificates** from the main menu tree.
2. Select the **Keys** tab.



The Keys tab displays the following:

Key Name	Displays the name of the key pair generated separately, or automatically when selecting a certificate. Specify the option within the wizard.
Key Size (Bytes)	Displays the size of the desired key. If not specified, a default key size of 1024 bytes is used.

3. Highlight a Key from the table and click the **Delete** button to delete it from the switch.
4. Click on **Add** button to add a new key label to the list of keys available to the switch. For more information, see *Adding a New Key on page 6-107*.
5. Select the **Delete All Keys** options to delete all of the keys displayed.
6. Click on **Transfer Keys** to archive the keys to a user-specified location. For more information, see *Transferring Keys on page 6-108*.

6.9.2.1 Adding a New Key

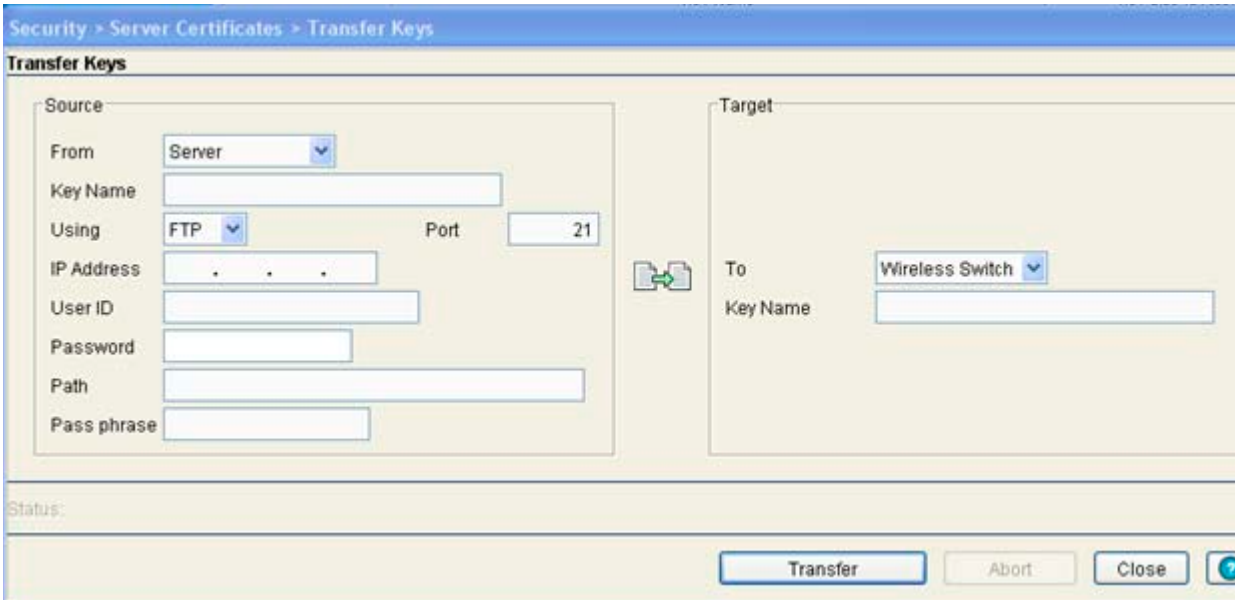
If none of the keys listed within the Keys tab are suitable for use with a certificate, consider creating a new key pair.

1. Select **Security** > **Server Certificates** from the main menu tree.
2. Select the **Keys** tab.
3. Click the **Add** button at the bottom of the screen.

4. Enter a **Key Label** in the space provided to specify a name for the new key pair.
5. Define the **Key Size** between 1024 and 2048 bytes.
6. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
7. Click **OK** to save the changes to the running configuration and close the dialog.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.9.2.2 Transferring Keys

The **Transfer** screen allows for the transfer of keys to and from the switch to (and from) a server or local disk. Transferring keys is recommended to ensure server certificate key information is available if problems are encountered with the switch and the data needs to be retrieved.



1. Select **Security** > **Server Certificate** from the main menu tree.
2. Click the **Keys** Tab.
3. Highlight a target file, and select the **Transfer Keys** button.
4. Use the **From** drop-down menu to specify the location from which the log file is sent. If only the applet is available as a transfer location, use the default switch option.
5. Select a target file for the file transfer from the **File** drop-down menu.

The drop-down menu contains the log files listed within the Server Certificate screen.

6. Use the **To** drop-down menu to define whether the target log file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
7. Provide the name of the file to be transferred to the location specified within the **Target** field.
8. Use the **Using** drop down-menu to configure whether the log file transfer is sent using FTP or TFTP.
9. Enter the **IP Address** of destination server or system receiving the target log file.
10. Enter the **User ID** credentials required to send the file to the target location.

    Use the user ID for FTP transfers only.
11. Enter the **Password** required to send the file to the target location using FTP.
12. Specify the appropriate **Path** name to the target directory on the local system disk or server as configured using the "To" parameter.

    If the local server option is selected, use the browse button to specify the location on the local server.
13. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
14. Click the **Transfer** button when ready to move the target file to the specified location.

    Repeat the process as necessary to move each desired log file to the specified location.
15. Click the **Abort** button to terminate the transfer before completion. The abort option is helpful if certificate credentials prove problematic in the transfer process.
16. Click the **Close** button to exit the screen after a transfer. There are no changes to save or apply.

6.10 Configuring Enhanced Beacons and Probes

The switch can be configured to detect and locate rogue APs and MUs. Refer to *Editing AP Settings on page 4-95* to enable an AP to forward beacons and association information for AP radios to detect a rogue. An AP can also be configured to forward MU probe requests to the switch to help locate a rogue MU.

NOTE: Currently, only an AP300 model Access Port supports enhanced beacons and probes request forward configuration.

Use the Enhanced Beacons/Probe screen to configure enhanced beacons/probes and their output reports. The Enhanced Probes and Beacons screens displays four tabs supporting the following configuration activities:

- *Configuring the Beacon Table*
- *Configuring the Probe Table*
- *Reviewing Found Beacons*
- *Reviewing Found Probes*

6.10.1 Configuring the Beacon Table

The Beacon Table is used to detect rogue APs. An AP300 transmits beacons and MUs send a probe request to the AP for association. The AP300 (on receipt of the probe request) sends a probe response and forms an AP-MU association.

When enabling an Enhanced Beacon, the switch allows adopted Access Ports to periodically scan for rogue APs on different channels without disassociating MUs. The beacons collected in the scan are passed on to the switch so required information is gathered to locate a particular rogue AP. Refer to *Editing AP Settings on page 4-95* to enable an AP to forward beacons and association information for AP radios to detect a rouge.

The switch is provided with a set of 802.11a and 802.11bg radio specific channels. The switch radio scans scan each channel to detect the potential existence or rogues operating on the configured channel. On completion of a scan, the switch moves the AP back to its original channel.

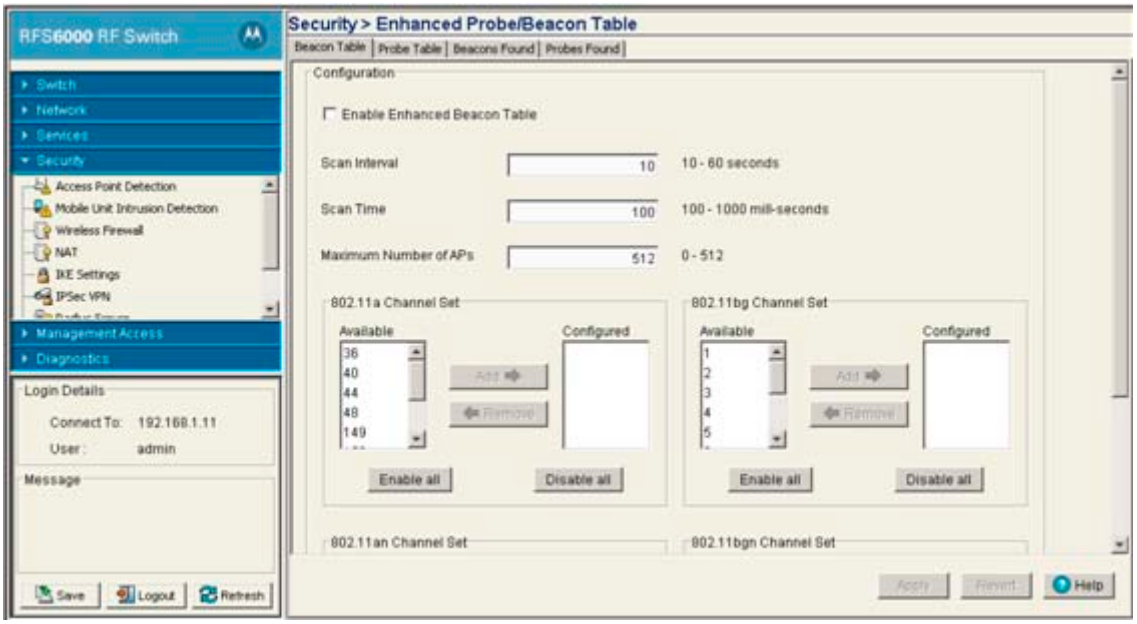
If, during the scan, an AP is detected on a different channel (due to a leaked signal), this channel is also added to the channel set. The AP sends this information to the switch, which maintains a table with the following information:

- *MAC address of the detected rogue AP*
- *AP MAC address*
- *Signal strength of the detected rogue AP*
- *Channel on which the AP was detected*
- *Time when the AP was detected.*

This information is used by the Motorola RF Management application (or Motorola RFMS) to locate the rogue AP. Motorola RFMS uses this information to physically locate the position of rogues and authorized devices within a site map representative of the physical dimensions of the actual device deployment area.

To configure enhanced beacons:

1. Select **Security** > **Enhanced Probe/Beacon Table** from the main menu tree.
2. Select the **Beacon Table** tab.



3. Select the **Enable Enhanced Beacon Table** checkbox to allow the AP to receive beacons and association information.
4. Use **Scan Interval** value to enter the interval used by the radio between scans. The radio scans each channel for the defined interval. The default value is 10 seconds.

5. Use the **Scan Time** value to enter the duration of the scan. The radio scans each channel for the defined interval. The default value is 100 milliseconds.
6. Define a **Max Number of APs** value to set the number of detected APs displayed in the Beacon Found table. The available range is from 0 to 512.
7. Refer to the **802.11a Channel Set** and **802.11an Channel Set** fields to select channels for the 802.11a and 802.11 an transmission bands. The channel information is provided to the switch, which then makes a radio scan for the configured channels.

Allowed	Displays the channels available to the AP. The channel list is country specific and differs from country to country.
Add ->	Select a channel frequency and click the **Add ->** button to include the channel to the **Configured** list box. You can select multiple channels and add them to the **Configured** list box. Press the Ctrl button and use the mouse to select multiple channels. The switch uses an 802.11a radio to scan the selected channels to detect any rogue AP's.
<- Remove	Select the channel's frequency from the Configured list box and click **<- Remove** to remove a channel from the list of channels provided to the switch.
Configured	Displays the channels provided to the switch. The switch makes all the 802.11a radios move to the selected channel and scan (one at a time), for a configurable interval.
Enable all	Select the **Enable all** button (within the 802.11a Radios field) to enable all 802.11a radios from receive beacons.
Disable all	Select the **Disable all** button (within the 802.11a Radios field) to disable all 802.11a radios from receiving beacons.

8. Refer to the **802.11bg Channel Set** and **802.11bgn Channel Set** fields to select channels for the 802.11bg and 802.11bgn transmission bands. The channel information is provided to the switch, which conducts a scan for each channel.

Allowed	Displays all the channels available to the AP. The channel list is country specific and differs from country to country.
Add ->	Select a channel frequency and click the **Add ->** button to include the channel to the **Configured** list box. Select multiple channels and add them to the **Configured** list box. Press the Ctrl button and use the mouse to select multiple channels. The switch uses an 802.11a radio to scan the selected channels to detect any non-adopted or rogue AP's.
<- Remove	Select the channel's frequency from the Configured list box and click **<- Remove** to remove a channel from the list of channels provided to the switch.
Configured	Displays the channels provided to the switch. The switch makes all the 802.11bg radios move to a channel from this channel-set and scan these channels, one at a time, for a configurable duration.
Enable all	Select the **Enable** button (within the 802.11bg Radios field) to enable all the 802.11bg radios receive enhanced beacons.
Disable all	Select the **Disable** button (within the 802.11bg Radios field) to disable all the 802.11bg radios from receiving enhanced beacons.

9. Click **Apply** to save changes to the screen. Navigating away from the screen without clicking the Apply button results in changes being discarded.
10. Click the **Revert** button to undo the changes to the screen and revert to the last saved configuration.

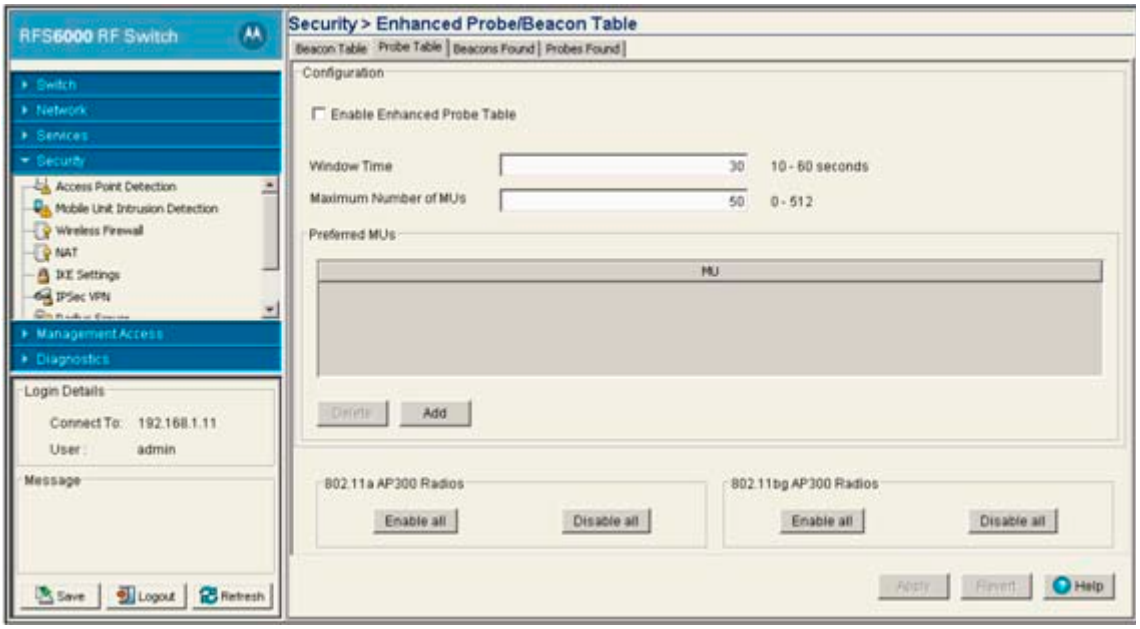
6.10.2 Configuring the Probe Table

Define enhanced probes to detect rogue MUs within the network. An AP300 transmits beacons and the MUs sends a probe request to the AP for association. An AP300 (on receipt of the probe request) sends a probe response and associates to the MU.

When using an enhanced probe, an AP300 sends a probe response to the MU to associate. At the same time, the AP forwards the MU's probe request information to the switch. The switch maintains a table of the probe requests the AP300 receives from MUs. In conjunction with the Motorola RF Management application, the AP locates the rogue MU and displays its location within a Motorola RFMS maintained site map.

To configure enhanced beacons:

1. Select **Security** > **Enhanced Probe/Beacon Table** from the main menu tree.
2. Select the **Probe Table** tab.



3. Select the **Enable Enhanced Probe Table** checkbox to allow an AP to forward MU probe requests to the switch.
4. Define a **Window Time** (from 10 to 60 seconds) to set an interval used by the AP to record MU probe requests. The MU radio probe entry with the highest signal strength during the window period is recorded in the table.
5. Set a **Maximum Numbers of MU's** (from 0 to 512) to define the number of MUs configured in the switch table. The default is 50 MUs.
6. The **Preferred MUs** table lists the MAC Addresses for all preferred MUs.
7. Select a MU from the Preferred MUs table and click the **Delete** button to remove the MU from the table.
8. Click the **Add** button to open a dialogue and add the MAC Address of a preferred MU to the table.

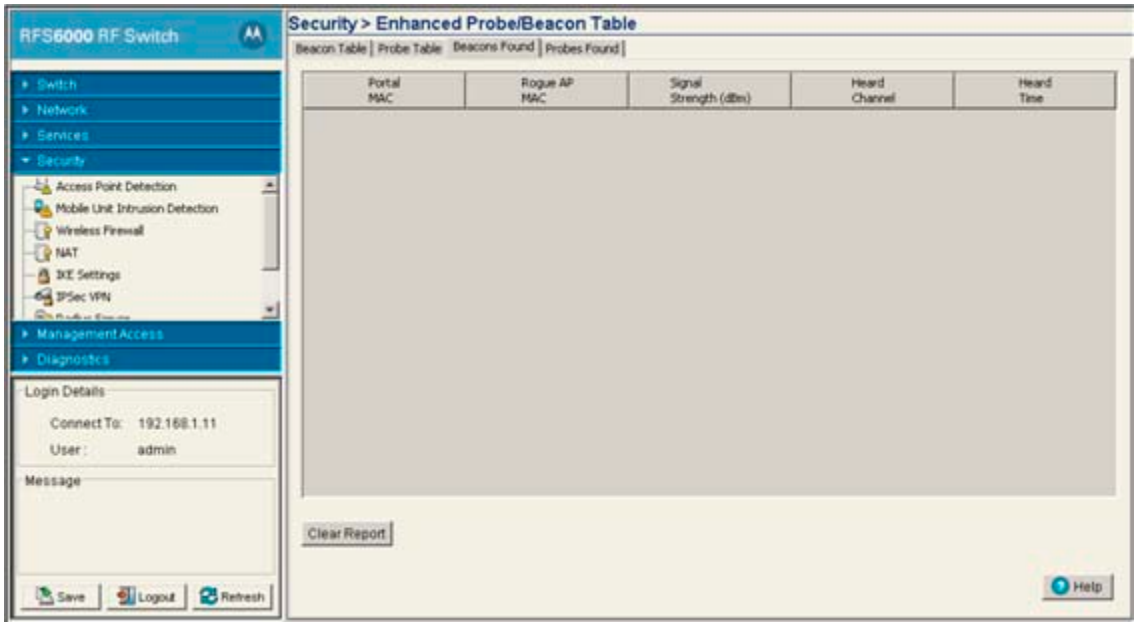
9. **802.11a AP300 Radios:** Click the **Enable all** button to allow an AP's 802.11a radio to receive MU probe requests and forward them to the switch. Click the **Disable all** button to stop AP's 802.11a radios from forwarding MU probe requests to the switch.
10. **802.11bg AP300 Radios:** Click the **Enable all** button to allow the AP's 802.11bg radios to receive MU probe requests and forward them to the switch. Click the **Disable all** button to stop AP's 802.11bg radios from forwarding MU probe requests to the switch.
11. Click **Apply** to save any changes. Navigating away from the screen without clicking the Apply button results in all the changes on the screen being discarded.
12. Click the **Revert** button to undo the changes to the screen and revert to the last saved configuration.

6.10.3 Reviewing Found Beacons

Select the **Beacons Found** tab to view the enhanced beacons report created by the switch. The table displays beacon information collected during the AP's channel scan. The table contains at least 5 entries for each AP radio (channel) scan. The information displayed within the Beacons Found tab is read-only with no user configurable parameters.

To view the enhanced beacons report:

1. Select **Security** > **Enhanced Probe/Beacon Table** from the main menu tree.
2. Select the **Beacons Found** tab.



3. Refer to the following information as displayed within the **Beacons Found** tab.

Portal MAC	Displays the MAC address of the unadopted AP detected by the enhanced beacon supported AP.
Rogue AP MAC	Displays the MAC address of the enhanced beacon supported AP.
Signal Strength (dBm)	Displays the signal strength when the unadopted AP was detected.

Heard Channel	Displays the channel frequency when the unadopted AP was detected.
Heard Time	Displays the time when the unadopted AP was detected.

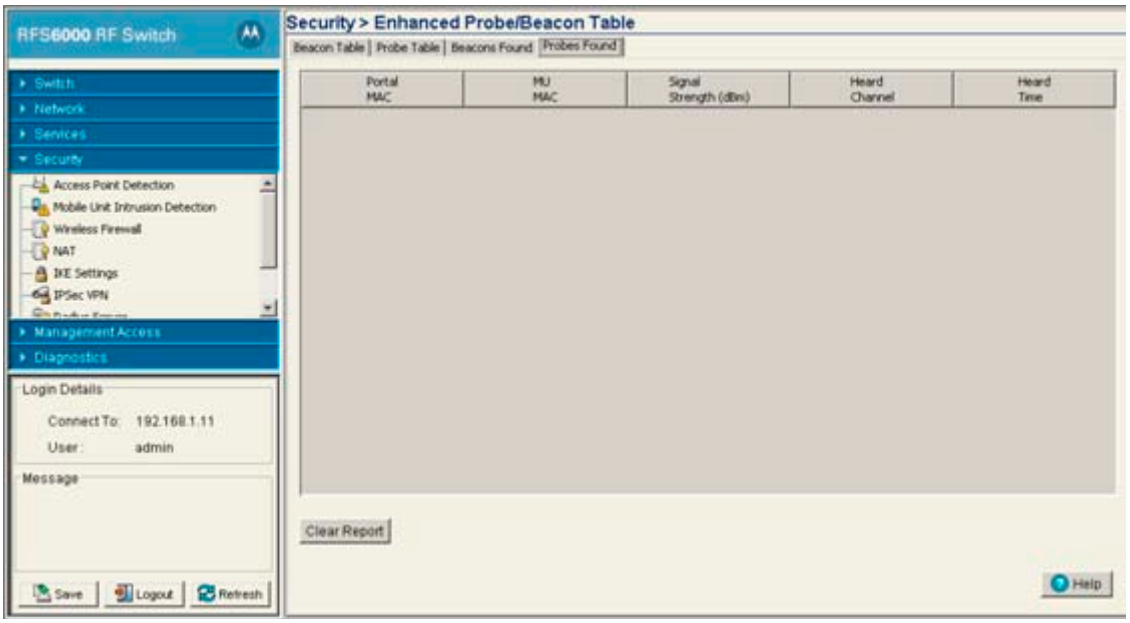
4. Select the **Clear Report** button to clear the statistic counters and begin a new data calculation.

6.10.4 Reviewing Found Probes

Refer to the **Probes Found** tab to view the enhanced Probe report created by the switch. The table displays probe information collected during the AP's channel scan. The information displayed within the Probes Found tab is read-only with no user configurable parameters.

To view the enhanced beacons table report:

1. Select **Security** > **Enhanced Probe/Beacon Table** from the main menu tree.
2. Select the **Probes Found** tab.



3. Refer to the following information as displayed within the **Probes Found** tab.

Portal MAC	Displays the MAC address of the unadopted MU picked detected by the Enhanced Probes enabled AP.
MU MAC	Displays the MAC address of the Enhanced Probe detected MU.
Signal Strength (dBm)	Displays the signal strength when the unadopted MU was detected.
CHeard channel	Displays the channel frequency used when the unadopted MU was detected.
Heard Time	Displays the time the unadopted MU was detected.

4. Select the **Clear Report** button to clear the statistic counters and begin a new data calculation.

7

Switch Management

This chapter describes the Management Access main menu items used to configure the switch. This chapter consists of the following switch management activities:

- *Displaying the Management Access Interface*
- *Configuring Access Control*
- *Configuring SNMP Access*
- *Configuring SNMP Traps*
- *Configuring SNMP Trap Receivers*
- *Configuring Management Users*

NOTE: HTTPS must be enabled to access the switch applet. Ensure HTTPS access has been enabled before using the login screen to access the switch applet.

7.1 Displaying the Management Access Interface

Refer to the main Management Access interface for a high-level overview of the current switch firmware version and the current switch log output configuration. Use this information to discern whether a switch firmware upgrade is required (by checking the Website for a newer version) and if the switch is outputting log data appropriately.

NOTE: When the switch's configuration is successfully updated (using the Web UI), the effected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the effected screen's Status field and the screen remains displayed. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To display the main Management screen:

1. Select **Management Access** from the main menu tree.

2. Refer to the **Current Status** field to review the following read-only information:

Firmware In Use	The **Firmware In Use** value displays the software version currently running on the switch. Use this information to assess whether a firmware update would improve the switch feature set and functionality.
Log Output	The Log Output value displays the target location for log files output by the switch.

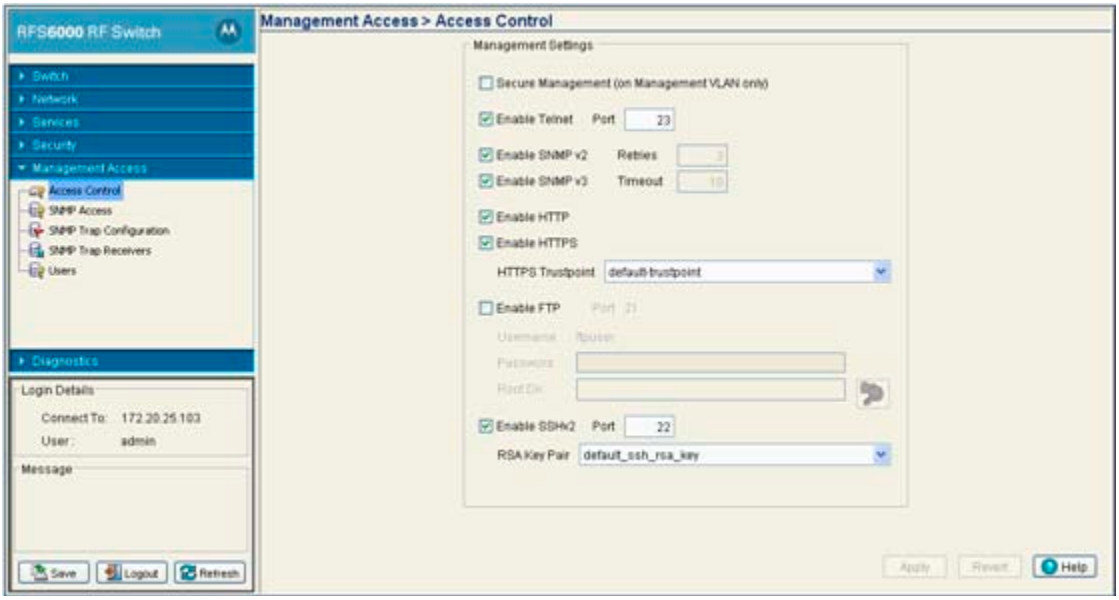
NOTE: The **Apply** and **Revert** functions are greyed out within the Management Access screen, as this screen is has no configurable parameters for the user to update and save.

7.2 Configuring Access Control

Refer to the **Access Control** screen to allow/deny management access to the switch using the different protocols (HTTP, HTTPS, Telnet, SSH or SNMP) available to users. Access options are either enabled or disabled as required. The Access Control screen 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.

To configure access control settings:

1. Select **Management Access** > **Access Control** from the main menu tree.



2. Refer to the **Management Settings** field to enable or disable the following switch interfaces:

Secure Management (on Management VLAN only)	Select this checkbox to allow management VLAN access to switch resources. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN. Only one management VLAN can be active at a time. This option is disabled (not selected) by default.
Enable Telnet	Select this checkbox to allow the switch to use a Telnet session for communicating over the network. This setting is enabled by default.
Port	Define the port number used for the Telnet session with the switch. This field is enabled as long as the Enable Telnet option remains enabled. The default port is port 23.
Enable SNMP v2	Select this checkbox to enable SNMPv2 access to the switch over the SNMPv2 interface. This setting is enabled by default.
Enable SNMP v3	Select this checkbox to enable SNMPv3 access to the switch over the SNMPv3 interface. This setting is enabled by default.
Retries	Define the number of retries the switch uses to connect to the SNMP interface if the first attempt fails. The default value is 3 retry attempts.
Timeout	When the provided interval is exceeded, the user is logged out of the SNMP session and forced re-initiate their connection. The default value is 10 minutes.
Enable HTTP	Select this checkbox to enable HTTP access to the switch. The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This setting is enabled by default.
Enable HTTPS	Select this checkbox to enable HTTPS access to the switch. This setting is enabled by default.
HTTPS Trustpoint	Use the Trustpoint drop-down menu to select the local or default trustpoint used with a HTTPS session with the switch. For information on creating a new certificate, see *Creating Server Certificates on page 6-97*.

Enable FTP	Select this checkbox to enable FTP access to the switch. *File Transfer Protocol* (FTP) is the language used for file transfers across the Web. This setting is disabled by default.
Port	Displays the port number used for the FTP session with the switch (if using FTP).
Username	Displays the read-only name of the user whose credentials are used for the FTP session.
Password	If FTP is enabled, a password is required (for the user specified in the **Username** field) to use the switch with the FTP interface.
Root Dir.	Define the root directory where the FTP server is located (if using FTP). Click the Magnifying Glass icon to display a **Select Directory File** screen useful in selecting the root directory. If necessary a new directory folder can be created.
Enable SSHv2	Select this checkbox to enable SSH version 2 access to the switch. *Secure Shell* (SSH) is a program designed to perform a number of functions, such as file transfer between computers, command execution or logging on to a computer over a network. It is intended to do these tasks with greater security than programs such as Telnet or FTP. This setting is enabled by default.
Port	Define the port number used for the SSH session with the switch.
RSA Key Pair	Use the **RSA Key Pair** drop-down menu to select a public/private key pair used for RSA authentication. The default setting is "default_ssh_rsa_key"

NOTE: You cannot establish a SSH session with the switch when a RSA Key with a length of 360 is associated with the SSH-Server.

3. Click the **Apply** button to save changes made to the screen since the last saved configuration.
4. Click the **Revert** button to revert the screen back to its last saved configuration. Changes made since the contents of the screen were last applied are discarded.

7.3 Configuring SNMP Access

Use the SNMP Access menu to view and configure existing SNMP v1/v2 and SNMP v3 values and their current access control settings. You can also view the SNMP V2/V3 events and their current values. The SNMP Access window consists of the following tabs:

- *Configuring SNMP v1/v2 Access*
- *Configuring SNMP v3 Access*
- *Setting SNMP Access Message Parameters*
- *Accessing SNMP v2/v3 Statistics*

CAUTION: Your system must be running Sun JRE version 1.5.x (or higher) or Mozilla for the switch Web UI to be used with the SNMP interface.

NOTE: The SNMP facility cannot retrieve a configuration file directly from its SNMP interface. First deposit the configuration file to a computer, then FTP the file to the switch.

NOTE: When accessing the switch via a SNMP client ensure that UDP traffic is allowed on port 161 for the network being used for the switch and the SNMP client.

7.3.1 Configuring SNMP v1/v2 Access

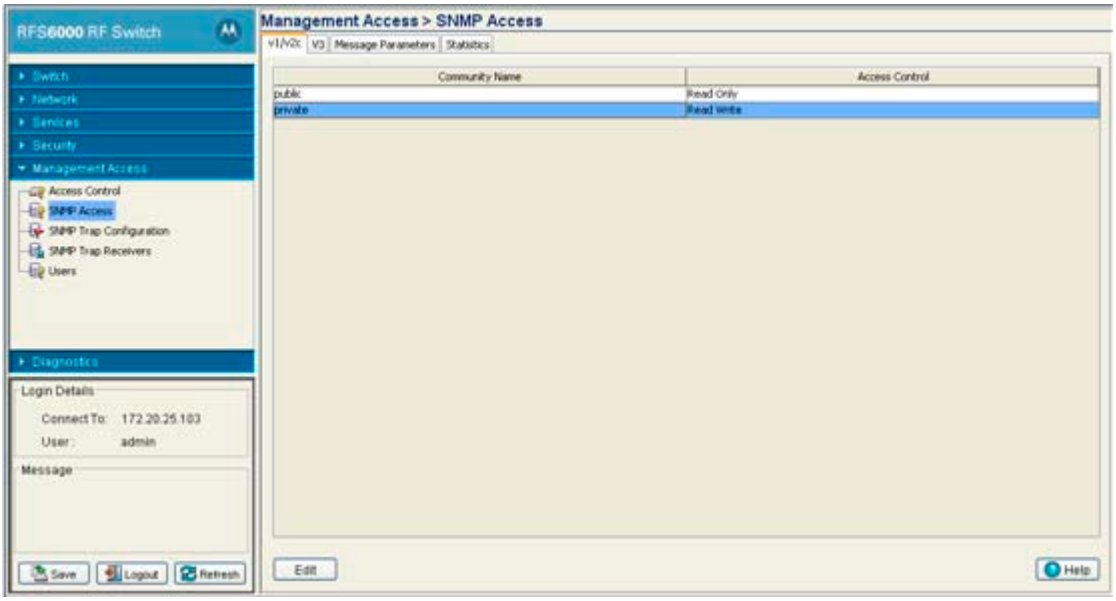
SNMP version 2 (SNMPv2) is an evolution of SNMPv1. The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv2. However, SNMPv2 adds and enhances some protocol operations. The SNMPv2 Trap operation, for example, serves the same function used in SNMPv1, but uses a different message format and is designed to replace a SNMPv1 Trap.

Refer to the v1/v2c screen for information on existing SNMP v1/v2 community names and their current access control settings. Community names can be modified by selecting a community name and clicking the **Edit** button.

NOTE: The SNMP undo feature is not supported.

To review existing SNMP v1/v2 definitions:

1. Select **Management Access** > **SNMP Access** > **v1/v2** from the main menu tree.



2. Refer to the **Community Name** and **Access Control** parameters for the following information:

Community Name	Displays the read-only or read-write name used to associate a site-appropriate name for the community. The name is required to match the name used within the remote network management software. Click the **Edit** button to modify an existing Community Name.
Access Control	The Access Control field specifies a read-only (R) access or read/write (RW) access for the community. Read-only access allows a remote device to retrieve information, while read/write access allows a remote device to modify settings. Click the **Edit** button to modify an existing Access Control permission.

3. Highlight an existing entry and click the **Edit** button to modify the properties of an existing SNMP V1/v2 community and access control definition. For more information, see *Editing an Existing SNMP v1/v2 Community Name on page 7-6*.

7.3.1.1 Editing an Existing SNMP v1/v2 Community Name

The **Edit** screen allows the user to modify a community name and change its read-only or read/write designation. Since the community name is required to match the name used within the remote network management software, it is recommended the name be changed appropriately to match a new naming (and user) requirement used by the management software.

To modify an existing SNMP v1/v2 Community Name and Access Control setting:

1. Select **Management Access** > **SNMP Access** > **v1/v2** from the main menu tree.
2. Select an existing Community Name from those listed and click the **Edit** button.

3. Modify the **Community Name** used to associate a site-appropriate name for the community. The name revised from the original entry is required to match the name used within the remote network management software.
4. Modify the existing read-only (R) access or read/write (RW) access for the community. Read-only access allows a remote device to retrieve information, while read/write access allows a remote device to modify settings.
5. Click **OK** to save and add the changes to the running configuration and close the dialog.
6. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch
7. Click **Cancel** to return back to the SNMP v1/v2 screen without implementing changes.

7.3.2 Configuring SNMP v3 Access

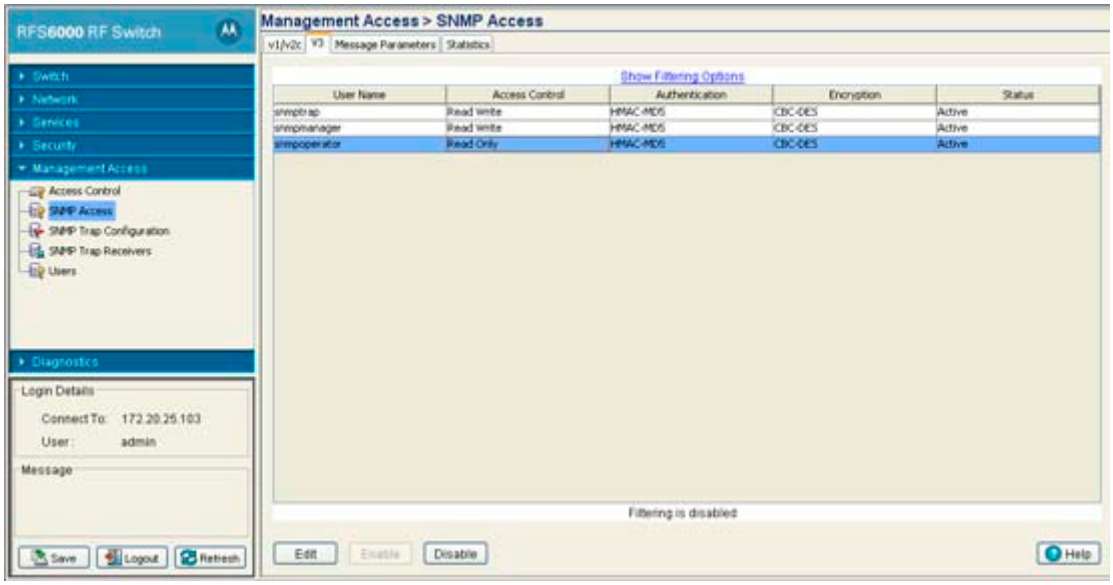
SNMP Version 3 (SNMPv3) adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. The architecture supports the concurrent use of different security, access control, and message processing techniques.

Refer to the **v3** screen to review the current SNMP v3 configuration. An Existing User Name can be selected and edited, enabled or disabled. .

NOTE: The SNMP undo feature is not supported in this product.

To review existing SNMP v3 definitions:

1. Select **Management Access** > **SNMP Access** from the main menu tree.
2. Select the **V3** tab from within the SNMP Access screen.



3. Refer to the fields within the V3 screen for the following information:

User Name	Displays a read-only SNMP v3 username of operator or Admin. An operator typically has an Access Control of read-only and an Admin typically has an Access Control of read/write.
Access Control	Displays a *read-only* (R) access or *read/write* (RW) access for the v3 user. Read-only access allows the user (when active) to retrieve information, while read/write access grants the user modification privileges.
Authentication	Displays the current authorization scheme used by this user for v3 access to the switch. Click the **Edit** button to modify the password required to change authentication keys.
Encryption	Displays the current Encryption Standard (DES) protocol the user must satisfy for SNMP v3 access to the switch. Click the **Edit** button to modify the password required to change encryption keys.
Status	Displays whether this specific SNMP v3 User Name is active on the switch. For more information, see *Accessing SNMP v2/v3 Statistics on page 7-9*.

4. Highlight an existing v3 entry and click the **Edit** button to modify the password for the Auth Protocol and Priv Protocol.

   For additional information, see *Editing an Existing SNMP v1/v2 Community Name on page 7-6*
5. Highlight an existing SNMP v3 User Name and click the **Enable** button to enable the log-in for the specified user. When selected the status of the user is defined as active.
6. Highlight an existing SNMP v3 User Name and click the **Disable** button to disable the log-in for the specified user. When selected the status of the user is defined as inactive.

7.3.2.1 Editing a SNMP v3 Authentication and Privacy Password

The **Edit** screen enables the user to modify the password required to change the authentication keys. Updating the password requires logging off of the system. Updating the existing password creates new authentication and encryption keys. To edit an SNMP v3 user profile:

1. Select **Management Access > SNMP Access** from the main menu tree.
2. Select the **v3** tab from within the SNMP Access screen.
3. Highlight an existing SNMP v3 User Name and click the **Edit** button.

The **Authentication Protocol** is the existing protocol for the User Profile. The Authentication Protocol is not an editable option. The **Privacy Protocol** is the existing protocol for the User Profile. The Privacy Protocol is also not an editable option.

4. Enter the **Old Password** used to grant Authentication Protocol and Privacy Protocol permissions for the User Profile.
5. Enter the **New Password**, then verify the new password within the **Confirm New Password** area.
6. Click **OK** to save and add the changes to the running configuration and close the dialog.
7. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

7.3.3 Setting SNMP Access Message Parameters

The switch Web UI enables an administrator to set SNMP data access retry attempts and timeout values. This affords an administrator the ability define how switch resources are utilized in respect to SNMP connection attempts.

To define the data collection retry and timeout intervals for SNMP Access:

1. Select **Management Access** > **SNMP Access** from the main menu tree.
2. Select the **Message Parameters** tab from within the SNMP Access screen.

3. Define the following vales as required to define how SNMP Access messages are received:

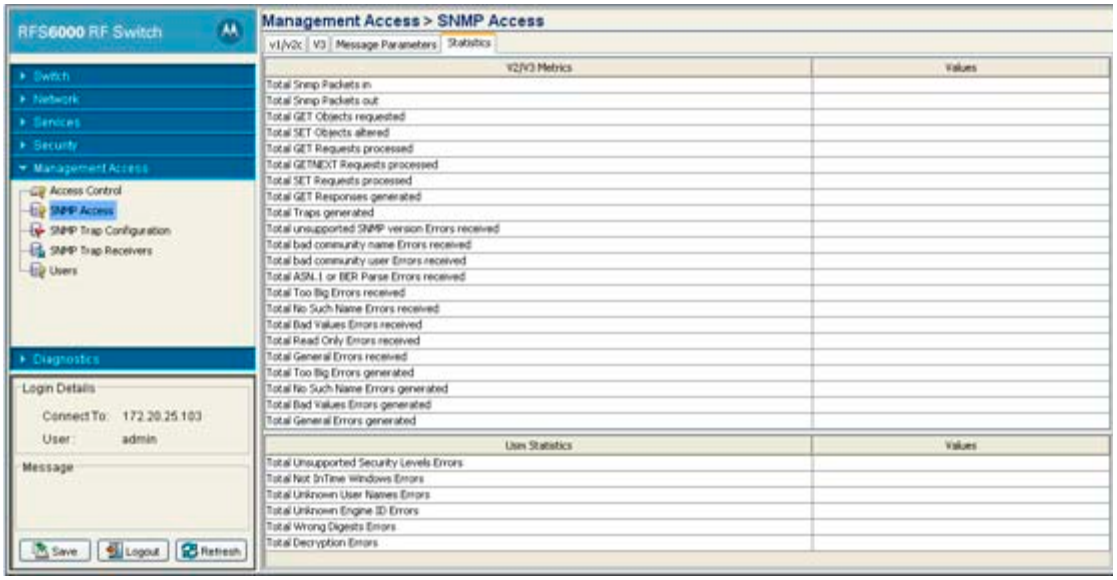
Retries	Define the number of times the switch polls for SNMP values before giving up.The default retry value is 3.
Timeout	Define a timeout interval (in seconds) the switch uses to timeout SNMP connection attempts. the default value is 10 seconds.
Rows per Request	Set the number of data rows returned per SNMP connection. The default value is 10 rows.

7.3.4 Accessing SNMP v2/v3 Statistics

Refer to the **Statistics** screen for a read-only overview of SNMP V2/V3 events and their current values. The screen also displays Usm Statistics (SNMP V3 specific events specific to the User-based Security Model) and their values.

To edit an SNMP v3 user profile:

1. Select **Management Access** > **SNMP Access** from the main menu tree.
2. Select the **Statistics** tab from within the SNMP Access screen.



3. Refer to the following read-only statistics displayed within the SNMP Access Statistics screen:

V2/V3 Metrics — Displays the individual SNMP Access events capable of having a value tracked for them. The metrics range from general SNMP events (such as the number of SNMP packets in and out) to specific error types that can be used for troubleshooting SNMP events (such as Bad Value and Read-Only errors).

Values — Displays the current numerical value for the SNMP V2/V3 Metric described on the left-hand side of the screen. The value equals the number of times the target event has occurred. This data is helpful in troubleshooting SNMP related problems within the network.

Usm Statistics — Displays SNMP v3 events specific to Usm. The *User-based Security Model* (USM) decrypts incoming messages. The module then verifies authentication data. For outgoing messages, the USM module encrypts PDUs and generates authentication data. The module then passes the PDUs to the message processor, which then invokes the dispatcher.

The USM module's implementation of the SNMP-USER-BASED-SM-MIB enables SNMP to issue commands to manage users and security keys. The MIB also enables the agent to ensure a requesting user exists and has the proper authentication information. When authentication is done, the request is carried out by the agent.

Values — Displays the current numerical value for the Usm Metric described on the left-hand side of the screen. The value equals the number of times the target event occurred. This data is helpful in troubleshooting Usm (Authentication and Encryption) related problems within the network.

7.4 Configuring SNMP Traps

Use the SNMP Trap Configuration screen to enable or disable individual traps or by functional trap groups. It is also used for modifying the existing threshold conditions values for individual trap descriptions. Refer to the tabs within the SNMP Trap Configuration screen to conduct the following configuration activities:

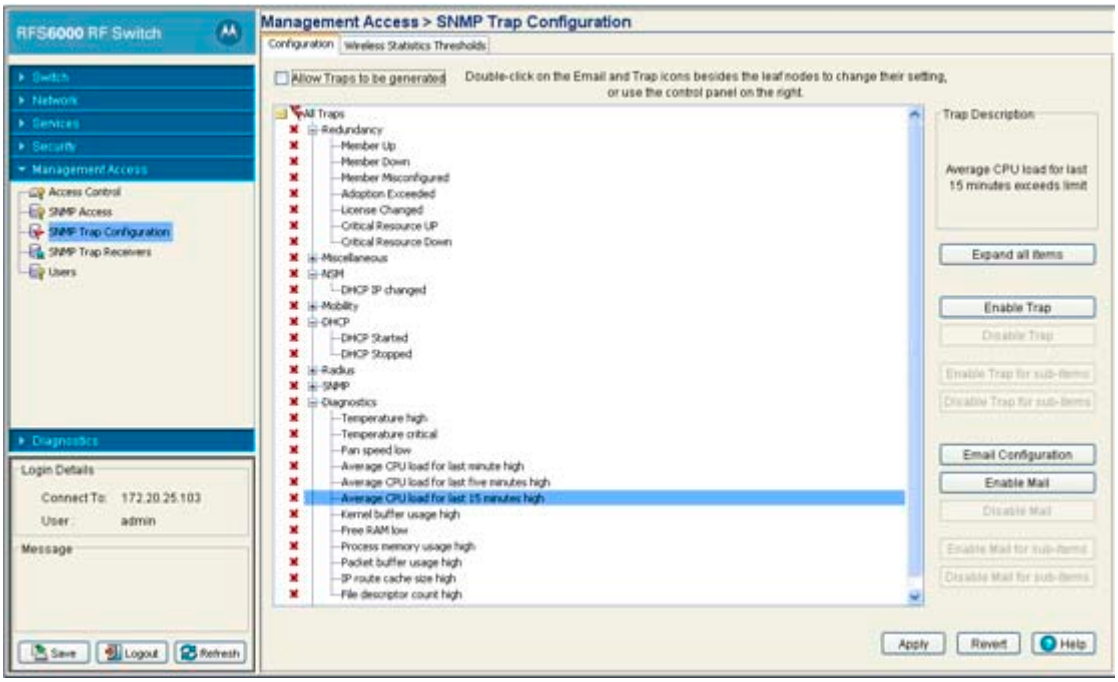
- *Enabling Trap Configuration*
- *Configuring Trap Thresholds*

7.4.1 Enabling Trap Configuration

If unsure whether to enable a specific trap, select it and view a brief description that may help your decision. Use **Expand all items** to explode each trap category and view all the traps that can be enabled. Traps can either be enabled by group or as individual traps within each parent category.

To configure SNMP trap definitions:

1. Select **Management Access** > **SNMP Trap Configuration** from the main menu tree.



2. Select the **Allow Traps to be generated** checkbox to enable the selection (and employment) of all the traps within the screen. Leaving the checkbox unselected means traps must be enabled by category or individually.
3. Refer to trap categories within the Configuration screen to determine whether traps should be enabled by group or individually enabled within parent groups.

4. Select an individual trap, by expanding the node in the tree view, to view a high-level description of this specific trap within the **Trap Description** field. You can also select a trap family category heading (such as "Redundancy" or "NSM") to view a high-level description of the traps within that trap category.

Redundancy	Displays a list of sub-items (trap options) specific to the Redundancy (clustering) configuration option. Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the trap family parent item and click **Enable all sub-items** to enable all traps within the Cluster category.
Miscellaneous	Displays a list of sub-items (trap options) specific to the Miscellaneous configuration option (traps that do not fit in any other existing category). Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the Miscellaneous trap family parent item and click **Enable all sub-items** to enable all traps within the Miscellaneous category.
NSM	Displays a list of sub-items (trap options) specific to the NSM configuration option. Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the NSM trap family parent item and click **Enable all sub-items** to enable all traps within the NSM category.
Mobility	Displays a list of sub-items (trap options) specific to the Mobility configuration option. Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the Mobility trap family parent item and click **Enable all sub-items** to enable all traps within the Mobility category.
DHCP	Displays a list of sub-items (trap options) specific to the DHCP configuration option. Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the DHCP trap family parent item and click **Enable all sub-items** to enable all traps within the DHCP category.
Radius	Displays a list of sub-items (trap options) specific to the Radius configuration option. Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the Radius trap family parent item and click **Enable all sub-items** to enable all traps within the Radius category.
SNMP	Displays a list of sub-items (trap options) specific to the SNMP configuration option. Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the SNMP trap family parent item and click **Enable all sub-items** to enable all traps within the SNMP category.
Diagnostics	Displays a list of sub-items (trap options) specific to the Diagnostics configuration option. Select an individual trap within this subsection and click the **Enable** button to enable this specific trap or highlight the Diagnostics trap family parent item and click **Enable all sub-items** to enable all traps within the Diagnostics category.
Wireless	Displays the list of sub-items (trap options) specific to Wireless configuration. These include traps specific to wireless interoperability between the switch and its associated devices. Select an individual trap and click the **Enable** button to enable a specific trap or highlight the Wireless trap family parent item and click **Enable all sub-items** to enable all traps within the Wireless category.

5. Click the **Expand All Items** button to display the sub-items within each trap category. Use this item to display every trap that can be enabled.

   Once expanded, traps can then be enabled by trap category or individually within each trap category.

6. Highlight a specific trap and click the **Enable** button to enable this specific trap as an active SNMP trap.

   The items previously disabled (with an "X" to the left) now display with a check to the left of it.

7. Highlight a specific trap and click the **Disable** button to disable the item as an active SNMP trap.

   The items previously enabled (with a check to the left) now display with an "X" to the left of it.

8. Highlight a sub-menu header (such as Redundancy or Update Server) and click the **Enable all sub-items** button to enable the item as an active SNMP trap.

   Those sub-items previously disabled (with an "X" to the left) now display with a check to the left of them. Once the **Apply** button is clicked, the selected items are now active SNMP traps on the system.

9. Highlight a sub-menu header (such as Redundancy or SNMP) and click the **Disable all** sub-items button to disable the item as an active SNMP trap.

   Those sub-items previously enabled (with a check to the left) now display with an "X" to the left of them.

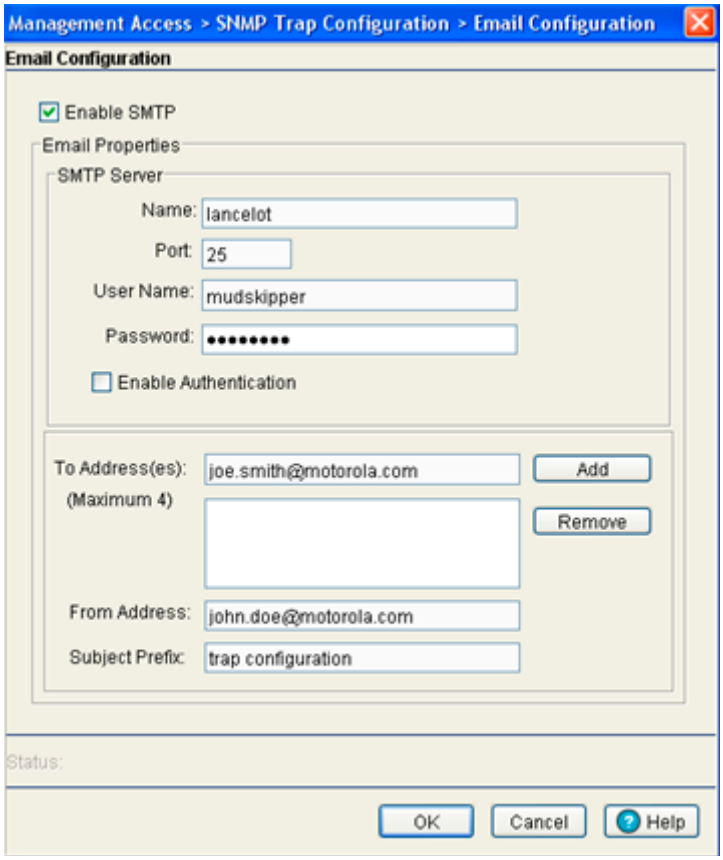
10. Click **Apply** to save the trap configurations enabled using the Enable or Enable all sub-items options.

11. Click **Revert** to discard any updates and revert back to its last saved configuration.

7.4.1.1 Configuring E-mail Notifications

To enable e-mail notification:

1. Select **Management Access** > **SNMP Trap Configuration** from the main menu tree.
2. Click the **Email Configuration** button to launch a dialogue where you can configure outgoing E-mail servers and addresses for alerts.



3. Check the **Enable SMTP** box to enable the outgoing mail server on the switch. In order to use E-mail notification on the switch, this box must be checked.

   Configure the SMTP mail server properties as follows:

Name	Enter the hostname of your outgoing SMTP mail server. This is the server that is used to deliver outgoing mail.
Port	Specify the port number used by your outgoing SMTP server. In many cases this is port 25.
User Name	Enter the username for the user which will be sending outgoing mail through the SMTP server.
Password	Enter the password associated with the above username.
Enable Authentication	Check the Enable Authentication box to enable support for SMTP Authentication which is required for certain outgoing SMTP servers.

4. Configure the mail-to section of the page as follows:

To Address(es)	Specify an e-mail address or addresses that notifications will be sent to. To add an e-mail address to the list, enter the email address in the To Address(es) field and click the Add button. There is a maximum of 4 e-mail addresses allowed on the list.
Add	Click the Add button to add an e-mail address that is in the To Address(es) field to the list below.
Remove	Select an e-mail address from the list and click the Remove button to delete that address from the list.
From Address	Enter an e-mail address serving as the From address for the notifications sent by the switch.
Subject Prefix	Enter a short subject line that prepends the subject line in each outgoing notification e-mail.

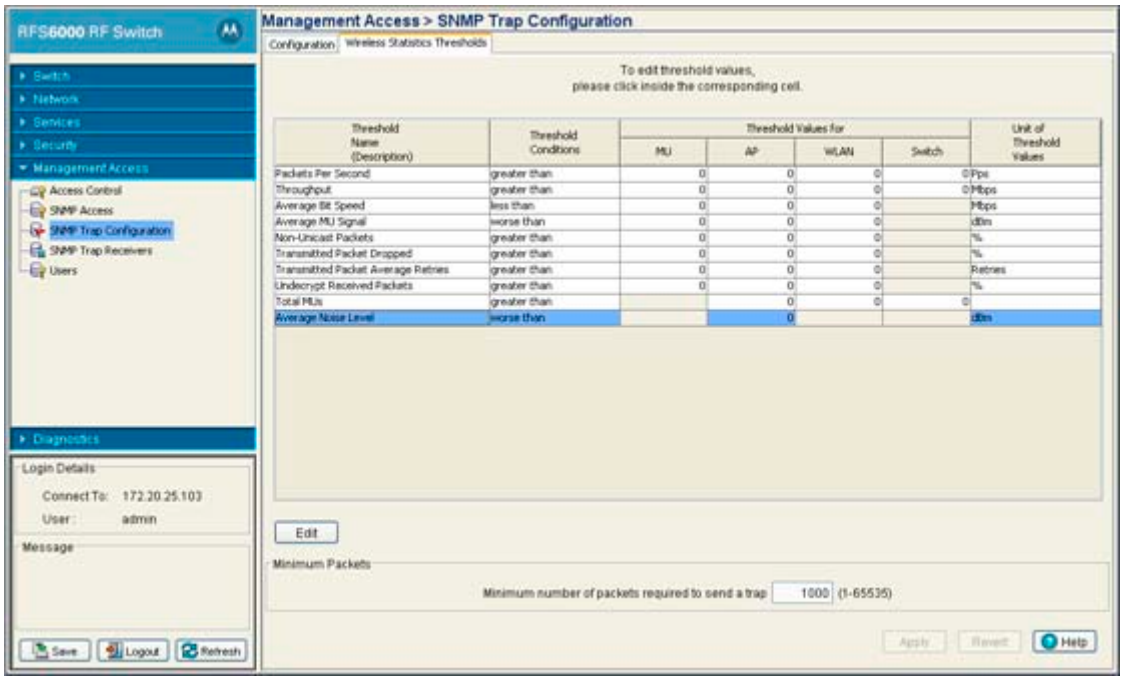
5. Click **OK** to save and add the changes to the running configuration and close the dialog.
6. Click **Cancel** to close the dialog without committing updates to the running configuration.

7.4.2 Configuring Trap Thresholds

Use the **Wireless Statistics Thresholds** screen to modify existing threshold conditions values for individual trap descriptions. Refer to the greater than, less than and worse than conditions to interpret how the values should be defined. Additionally, the Unit of threshold Values increment should be referenced to interpret the unit of measurement used.

To configure SNMP trap threshold values:

1. Select **Management Access** > **SNMP Trap Configuration** from the main menu tree.
2. Click the **Wireless Statistics Thresholds** tab.



3. Refer to the following information for thresholds descriptions, conditions, editable threshold values and units of measurement.

Threshold Name (Description)	Displays the target metric for the data displayed to the right of the item. It defines a performance criteria used as a target for trap configuration.
Threshold Conditions	Displays the criteria used for generating a trap for the specific event. The Threshold conditions appear as greater than, less then or worse then and define a baseline for trap generation.
Threshold values for: MU	Displays a threshold value for associated MUs. Use the **Threshold Name** and **Threshold Conditions** as input criteria to define an appropriate Threshold Value unique to the MUs within the network. For information on specific values, see *Wireless Trap Threshold Values on page 7-17*.
Threshold values for: AP	Set a threshold value for adopted APs. Use the **Threshold Name** and **Threshold Conditions** as input criteria to define an appropriate Threshold Value unique to the APs within the network. For information on specific values, see *Wireless Trap Threshold Values on page 7-17*.
Threshold values for: WLAN	Use the **Threshold Name** and **Threshold Conditions** as input criteria to define an appropriate Threshold Value unique to the switch. For information on specific values, see *Wireless Trap Threshold Values on page 7-17*.
Threshold values for: Switch	Use the **Threshold Name** and **Threshold Conditions** as input criteria to define an appropriate Threshold Value unique to the switch. For information on specific values, see *Wireless Trap Threshold Values on page 7-17*.
Unit of Threshold Values	Displays the measurement value used to define whether a threshold value has been exceeded. Typical values include Mbps, retries and %. For information on specific values, see *Wireless Trap Threshold Values on page 7-17*.

4. Select a threshold and click the **Edit** button to display a screen wherein threshold settings for the MU, AP and WLAN can be modified.

   Adjust the values as needed (between 0 -100) to initiate a trap when the value is exceeded for the MU, AP or WLAN. Ensure the value set is realistic, in respect to the number of MUs and APs supporting WLANs within the switch managed network.

5. Use the **Maximum Number of Packets to Send a Trap** field (at the bottom of the screen) to enter a value used as the minimum number of data packets required for a trap to be generated for a target event. Ensure the value is realistic, as setting it to low could generate traps unnecessarily. Refer to *Wireless Trap Threshold Values on page 7-17* for additional information.

6. Click the **Apply** button to save changes made to the screen since the last saved configuration.

7. Click the **Revert** button to revert the screen back to its last saved configuration. Changes made since the contents of the screen were last applied are discarded.

7.4.2.1 Wireless Trap Threshold Values

The table below lists the Wireless Trap threshold values for the switch:

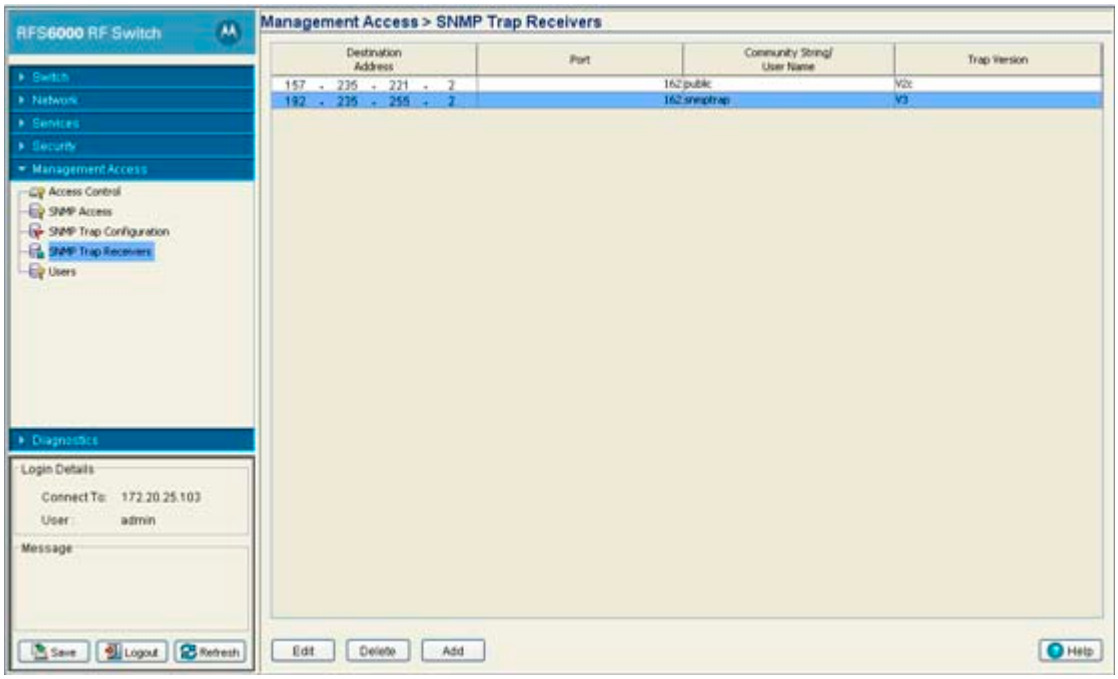
#	***Threshold Name***	***Condition***	***Station Range***	***Radio Range***	***WLAN Range***	***Wireless Service Range***	***Units***
1	Packets per Second	Greater than	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	Pps
2	Throughput	Greater than	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	Mbps
3	Average Bit Speed	Less than	A decimal number greater than 0.00 and less than or equal to 54.00	A decimal number greater than 0.00 and less than or equal to 54.00	A decimal number greater than 0.00 and less than or equal to 54.00	N/A	Mbps
4	Average MU Signal	Worse than	A decimal number less than -0.00 and greater than or equal to -120.00	A decimal number less than -0.00 and greater than or equal to -120.00	A decimal number less than -0.00 and greater than or equal to -120.00	N/A	dBm
5	Non Unicast Packets	Greater than	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	N/A	%
6	Transmitted Packet dropped	Greater than	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	N/A	%
7	Transmitted Packet Average retries	Greater than	A decimal number greater than 0.00 and less than or equal to 16.00	A decimal number greater than 0.00 and less than or equal to 16.00	A decimal number greater than 0.00 and less than or equal to 16.00	N/A	Retries
8	Undecrypted received packets	Greater than	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	N/A	%
9	Total MUs	Greater than	N/A	N/A A decimal N/A in the range <1-1000>	N/A A decimal N/A in the range <1-1000>	A decimal number in the range <1-1000>	Count

7.5 Configuring SNMP Trap Receivers

Refer to the **Trap Receivers** screen to review the attributes of existing SNMP trap receivers (including destination address, port, community and trap version). A new v2c or v3 trap receiver can be added to the existing list by clicking the **Add** button.

To configure the attributes of SNMP trap receivers:

1. Select **Management Access > SNMP Trap Receivers** from the main menu tree.



2. Refer to the following SNMP trap receiver data to assess whether modifications are required.

Destination Address	The **Destination Address** defines the numerical (non DNS name) destination IP address for receiving traps sent by the SNMP agent.
Port	The **Port** specifies a destination User Datagram Protocol (UDP) receiving traps.
Community String/ User Name	Displays the Community String and User Name specific to the SNMP-capable client that receives the traps. The community name is public.
Trap Version	The **Trap Version** defines the trap version (v1/2 or v3) defined by the SNMP-capable client receiving the trap. A trap designation cannot be modified.

3. Highlight an existing Trap Receiver and click the **Edit** button to display a sub-screen used to modify the v2c or v3 Trap Receiver.

   Edit Trap Receivers as needed if existing trap receiver information is insufficient. You can only modify the IP address, port and v2c or v3 trap designation within the Edit screen. For more information, see *Editing SNMP Trap Receivers on page 7-19*.

4. Highlight an existing Trap Receiver and click the **Delete** button to remove the Trap Receiver from the list of available destinations available to receive SNMP trap information.

   Remove Trap Receivers as needed if the destination address information is no longer available on the system.

5. Click the **Add** button to display a sub-screen used to assign a new Trap Receiver IP Address, Port Number and v2c or v3 designation to the new trap.

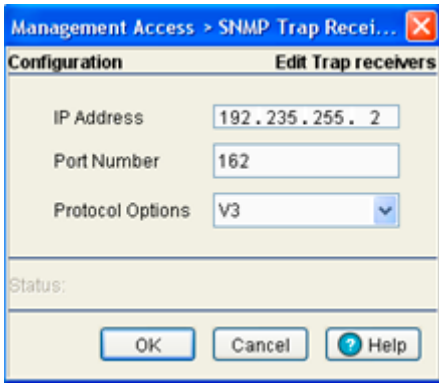
   Add trap receivers as needed if the existing trap receiver information is insufficient. For more information, see *Adding SNMP Trap Receivers on page 7-19*.

7.5.1 Editing SNMP Trap Receivers

Use the **Edit** screen to modify the trap receiver's IP Address, Port Number and v2c or v3 designation. Consider adding a new receiver before editing an existing one or risk overwriting a valid receiver. Edit existing destination trap receivers as required to suit the various traps enabled and their function in supporting the switch managed network.

To edit an existing SNMP trap receiver:

1. Select **Management Access > SNMP Trap Receivers** from the main menu tree.
2. Select (highlight) an existing SNMP trap receiver and click the **Edit** button.



3. Modify the existing **IP Address** if it is no longer a valid address.

   If it is still a valid IP address, consider clicking the **Add** button from within the SNMP Trap Receivers screen to add a new address without overwriting this existing one.

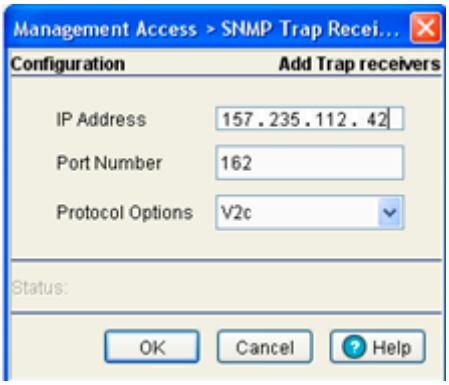
4. Define a **Port Number** for the trap receiver.
5. Use the **Protocol Options** drop-down menu to specify the trap receiver as either a SNMP v2c or v3 receiver.
6. Click **OK** to save and add the changes to the running configuration and close the dialog.
7. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

7.5.2 Adding SNMP Trap Receivers

The SNMP **Add** screen is designed to create a new SNMP trap receiver. Use the Add screen to create a new trap receiver IP Address, Port Number and v2c or v3 designation. Add new destination trap receivers as required to suit the various traps enabled and their function in supporting the switch managed network.

To add a new SNMP trap receiver:

1. Select **Management Access > SNMP Trap Receivers** from the main menu tree.
2. Click the **Add** button at the bottom of the screen.



3. Create a new (non DNS name) destination **IP Address** for the new trap receiver to be used for receiving the traps sent by the SNMP agent.
4. Define a **Port Number** for the trap receiver.
5. Use the **Protocol Options** drop-down menu to specify the trap receiver as either a SNMP v2c or v3 receiver.
6. Click **OK** to save and add the changes to the running configuration and close the dialog.
7. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **Cancel** to close the dialog without committing updates to the running configuration.

7.6 Configuring Management Users

Refer to the **Users** screen to view the administrative privileges assigned to different switch users. You can modify the roles and access modes assigned to each user. The Users screen also allows you to configure the authentication methods used by the switch. Use this screen for the following permission configuration activities:

- *Configuring Local Users*
- *Configuring Switch Authentication*

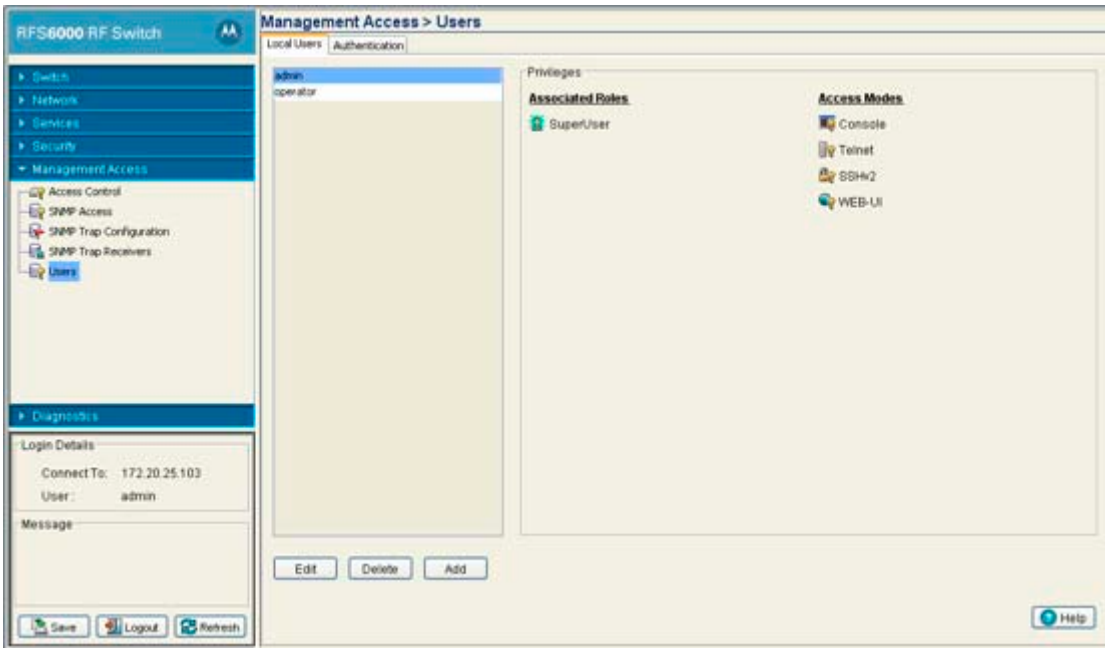
Additionally, the switch Web UI has the facility for creating guest administrators for creating guest users with defined login periods to specific guest groups. For more information, see *Creating a Guest Admin and Guest User on page 7-25*.

7.6.1 Configuring Local Users

Refer to the **Local Users** tab to view the administrative privileges assigned to users, create a new user and configure the associated roles and access modes assigned to each user.

To configure the attributes of Local User Details:

1. Select **Management Access** > **Users** from the main menu tree.
2. Click the **Local Users** tab.



The Local User window consists of 2 fields:

- *Users* – Displays the users currently authorized to use the switch. By default, the switch has two default user types, Admin and Operator.
- *Privileges* – This frame displays the privileges assigned to different type of user.

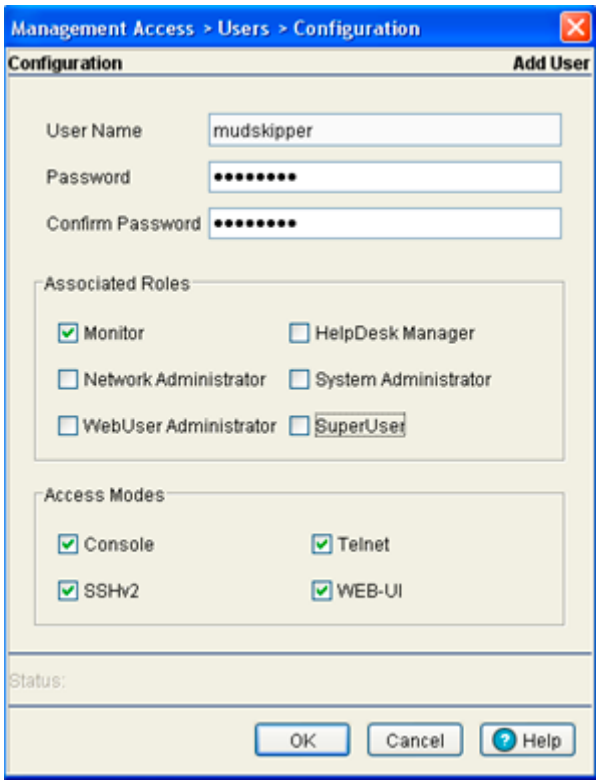
3. Select the user (Admin, Operator or user defined) from the **Users** frame. The **Privilege** frame displays the rights authorized to the user.
4. Click on the **Edit** button to modify the associated roles and access modes of the selected user. By default, the switch has two default users – Admin and Operator. Admin's role is that of a superuser and Operator the role will be monitored (read only).
5. Click on **Add** button to add and assign rights to a new user.
6. Click on **Delete** button to delete the selected user from the Users frame.

7.6.1.1 Creating a New Local User

Local users are those users connected directly into the switch and do not require any sort of configurable remote connection.

To create a new local user:

1. Select **Management Access** > **Users** from the main menu tree.
2. Click the **Add** button within the Local Users tab.



3. Enter the login name for the user in the **Username** field. Ensure this name is practical and identifiable to the user.
4. Enter the authentication password for the new user in the **Password** field and reconfirm the same again in the **Confirm Password** field.
5. Select the role you want to assign to the new user from the options provided in the **Associated Roles** panel. Select one or more of the following options:

Monitor	Select **Monitor** to assign regular user permissions without any administrative rights. The Monitor option provides *read-only* permissions.
Help Desk Manager	Assign this role to someone who typically troubleshoots and debugs problems reported by the customer. The Help Desk Manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the switch.
Network Administrator	The **Network Administrator** has privileges to configure all wired and wireless parameters like IP config, VLANs, Layer 2/Layer 3 security, WLANs, radios, IDS and hotspot.
System Administrator	Select **System Administrator** to allow the user to configure general settings like NTP, boot parameters, licenses, perform image upgrade, auto install, manager redundancy/clustering and control access.
Web User Administrator	Assign **Web User Administrator** privileges to add users for Web authentication (hotspot).
Super User	Select **Super User** to assign complete administrative rights.

NOTE: There are some basic operations/CLI commands (exit, logout and help) available to all user roles. All the roles except Monitor can perform Help Desk role operations.

NOTE: By default, the switch is HTTPS enabled with a self signed certificate. This is required since the Web UI uses HTTPS for user authentication.

6. Select the access modes to assign to the new user from the options provided in the **Access Modes** panel. Select one or more of the following options:

Console	This option provides the new user access to the switch using the console.
SSH	This option provides the new user access to the switch using SSH.
Telnet	This option provides the new user access to the switch using a Telnet session.
Applet	This option provides the new user access to the switch through the Web UI (applet).

NOTE: When establishing a connection to the switch using SSH, ensure that traffic can pass on TCP port 22 between the client and the switch.

NOTE: When establishing a connection to the switch using Telnet, ensure that traffic can pass on TCP port 23 between the client and the switch.

NOTE: When establishing a connection to the switch's applet, ensure that traffic can pass on TCP port 80 for HTTP access and TCP port 443 for HTTPS between the client and the switch.

7. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click the **OK** button to create the new user.
9. Click **Cancel** to revert back to the last saved configuration without saving any of your changes.

7.6.1.2 Modifying an Existing Local User

To create a new local user:

1. Select **Management Access** > **Users** from the main menu tree.
2. Select a user from the Users list and click the **Edit** button.
3. The **Username** field is read-only field and displays the login name of the user.
4. Enter the new authentication password for the user in the **Password** field and reconfirm within the **Confirm Password** field.
5. Select the user role from the options provided in the **Associated Roles** field. Select one or more of the following options:

Monitor	If necessary, modify user permissions without any administrative rights. The Monitor option provides *read-only* permissions.
Help Desk Manager	Optionally assign this role to someone who typically troubleshoots and debugs problems reported by the customer. the Help Desk Manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/ retrieves logs and reboots the switch.

Network Administrator	The **Network Administrator** provides configures all wired and wireless parameters like IP config, VLANs, Layer 2/Layer 3 security, WLANs, radios, IDS and hotspot.
System Administrator	Select **System Administrator** (if necessary) to allow the user to configure general settings like NTP, boot parameters, licenses, perform image upgrade, auto install, manager redundancy/clustering and control access.
Web User Administrator	Assign **Web User Administrator** privileges (if necessary) to add users for Web authentication (hotspot).
Super User	Select **Super User** (if necessary) to assign complete administrative rights.

NOTE: By default, the switch is HTTPS enabled with a self signed certificate. This is required since the applet uses HTTPS for user authentication.

NOTE: There are some basic operations/CLI commands like exit, logout and help available to all user roles. All roles except Monitor can perform Help Desk role operations.

6. Select the access modes you want to assign to the user from the options provided in the **Access Modes** panel. Select one or more of the following options:

Console	Provides the new user access to the switch using the console (applet)
SSH	Provides the new user access to the switch using SSH.
Telnet	Provides the new user access to the switch using Telnet
Applet	Provides the new user access to the switch using the Web UI (applet)

NOTE: When establishing a connection to the switch using SSH, ensure that traffic can pass on TCP port 22 between the client and the switch.

NOTE: When establishing a connection to the switch using Telnet, ensure that traffic can pass on TCP port 23 between the client and the switch.

NOTE: When establishing a connection to the switch's applet, ensure that traffic can pass on TCP port 80 for HTTP access and TCP port 443 for HTTPS between the client and the switch.

7. Refer to the **Status** field for an indication of any problems that may have arisen.

   The Status is the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.

8. Click on **OK** to complete the modification of the users privileges.
9. Click **Cancel** to revert back to the last saved configuration without saving any of your changes.

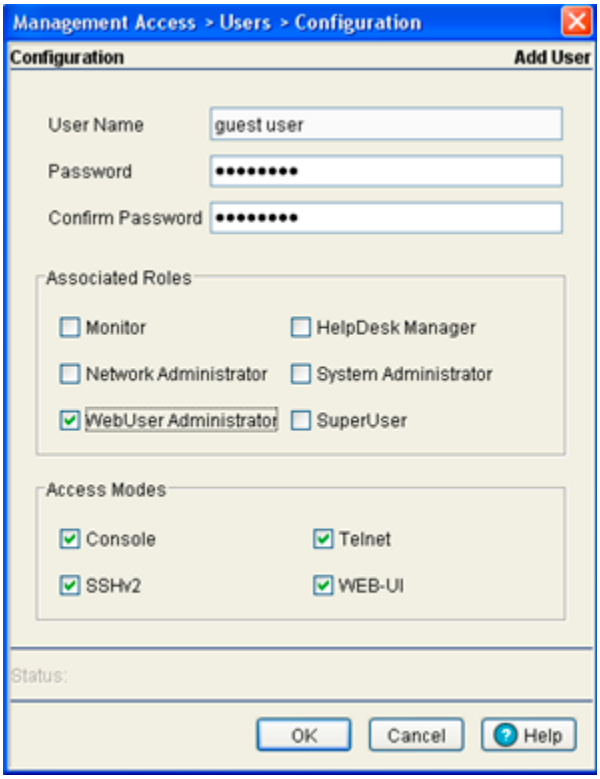
7.6.1.3 Creating a Guest Admin and Guest User

Optionally, create a guest administrator for creating guest users with specific usernames, start and expiry times and passwords. Each guest user can be assigned access to specific user groups to ensure they are limited to just the group information they need, and nothing additional.

NOTE: A guest user added from switch Web UI will be 5 minutes ahead of the switch's current time.

To create a guest administrator:

1. Select **Management Access** > **Users** from the main menu tree.
2. Click the **Add** button within the **Local Users** tab.



3. Enter the new guest-admin login name for the user in the **Username** field.
4. Enter the authentication password for the guest-admin in the **Password** field and reconfirm the same again in the **Confirm Password** field.
5. Assign the guest-admin **WebUser Administrator** access.

NOTE: To create guest users, a guest administrator must be assigned a **WebUser Administrator** access mode. None of the other modes launch the required Guest User Configuration screen upon login.

When the guest-admin user logs in, they are redirected to a **Guest User Configuration** screen, wherein start and end user permissions can be defined in respect to specific users.

6. Add guest users by name, start date and time, expiry date and time and user group.

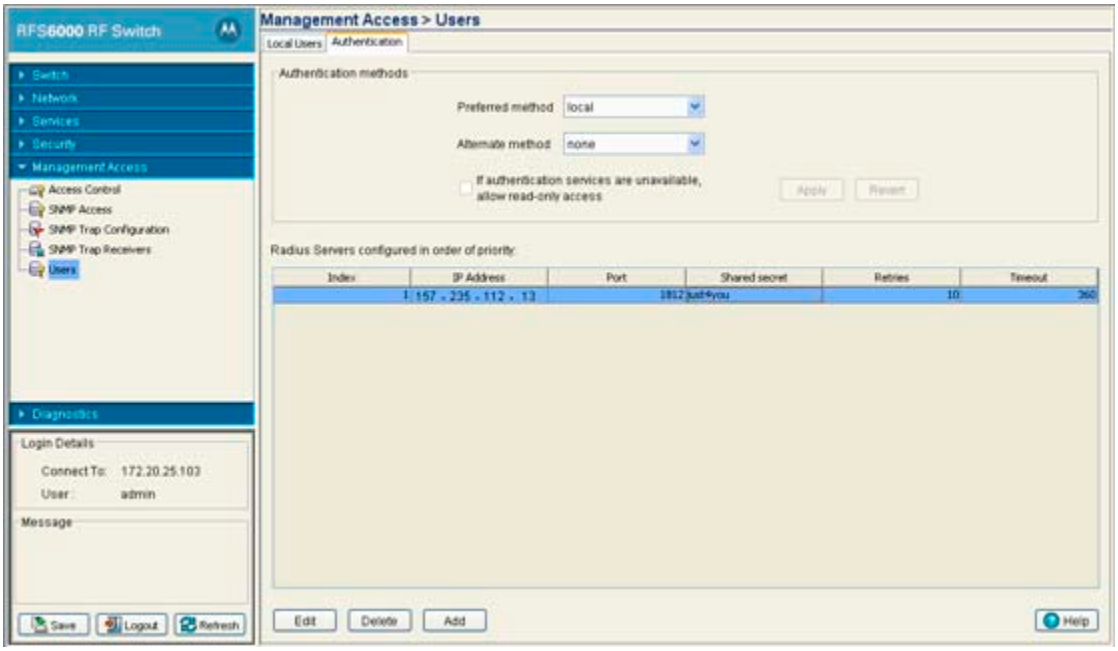
7. Optionally, click the **Generate** button to automatically create a username and password for each guest user.
8. Repeat this process as necessary until all required guest users have been created with relevant passwords and start/end guest group permissions.

7.6.2 Configuring Switch Authentication

The switch provides the capability to proxy authenticate requests to a remote Radius Server. Refer to the **Authentication** tab to view and configure the Radius Server used by the local user to log into the switch.

NOTE: The Radius configuration described in this section is independent of other Radius Server configuration activities performed using other parts of the switch.

1. Select **Management Access** > **Users** from the main menu tree.
2. Select the **Authentication** tab.



3. Refer to the **Authentication methods** field for the following:

Preferred Method — Select the preferred method for authentication. Options include:

- *None* - No authentication
- *Local* - The user employs a local user authentication resource. This is the default setting.
- *Radius* - Uses an external Radius Server

Alternate Method — Select an alternate method for authentication. This drop-down menu will not list the option already selected as the preferred method. Select any of the remaining authentication methods as an alternate method.

If **authentication services are not available**, due to technical reasons, then select the option provided in the panel to avail read-only access.

4. Click the **Apply** button to commit the authentication method for the switch.

5. Click the **Revert** button to rollback to the previous authentication configuration.
6. Refer to the bottom half of the Authentication screen to view the Radius Servers configured for switch authentication. The servers are listed in order of their priority.

Index	Displays a numerical **Index** for the Radius Server to help distinguish this Radius Server from other servers with a similar configuration. The maximum number that can be assigned is 32.
IP Address	Displays the IP address of the external Radius Server. Ensure this address is a valid IP address and not a DNS name.
Port	Displays the TCP/IP port number for the Radius Server. The port range available for assignment is from 1 - 65535.
Shared secret	Displays the shared secret used to verify Radius messages (with the exception of the Access-Request message) are sent by a Radius-enabled device configured with the same shared secret. The shared secret is a case-sensitive string (password) that can include letters, numbers, or symbols. Ensure the shared secret is at least 22 characters long to protect the Radius Server from brute-force attacks.
Retries	Displays the maximum number of times the switch can retransmit a Radius Server frame before it times out of the authentication session.
Timeout	Displays the maximum time (in seconds) the switch waits for the Radius Server's acknowledgment of authentication request packets before the switch times out of the session.

7. Select a Radius Server from the table and click the **Edit** button to modify how the authentication method is used. For more information, see *Modifying the Properties of an Existing Radius Server on page 7-27*.
8. Highlight a Radius Server from those listed and click the **Delete** button to remove the server from the list of available servers.
9. Click the **Add** button at the bottom of the screen to display a sub-screen used to add a Radius Server to the list of servers available to the switch. For more information, see *Adding an External Radius Server on page 7-28*.

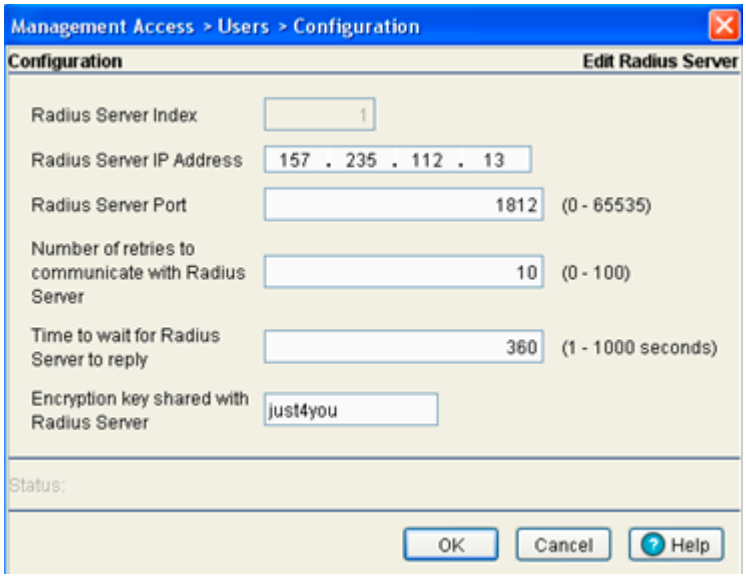
7.6.2.1 Modifying the Properties of an Existing Radius Server

Some of the attributes of an existing Radius Server can be modified by the switch to better reflect the Radius Server's existing connection with the switch.

To modify the attributes of an existing Radius Server:

1. Select **Management Access** > **Users** from the main menu tree.

   The Users screen displays.
2. Click on the **Authentication** tab.
3. Select an existing Radius Server from those listed and click the **Edit** button at the bottom of the screen.



4. Modify the following Radius Server attributes as necessary:

Radius Server Index	Displays the read-only numerical **Index** value for the Radius Server to help distinguish this server from other servers with a similar configuration (if necessary). This is not an editable value.
Radius Server IP Address	Modify the IP address of the external Radius Server (if necessary). Ensure this address is a valid IP address and not a DNS name.
Radius Server Port	Change the TCP/IP port number for the Radius Server (if necessary). The port range available for assignment is from 1 - 65535.
Number of retries to communicate with Radius Server	Revise (if necessary) the maximum number of times the switch retransmits a Radius Server frame before it times out of the authentication session. The available range is between 0 - 100.
Time to wait for Radius Server to reply	Revise (if necessary) the maximum time (in seconds) the switch waits for the Radius Server's acknowledgment of authentication request packets before the switch times out of the session. The configurable range is between 1 - 1000 seconds.
Encryption key shared with Radius Server	Enter the encryption key the switch and Radius Server share and must validate before the user authentication scheme provided by the Radius Server can be initiated.

5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click on **OK** to complete the modification of the Radius Server.
7. Click **Cancel** to revert back to the last saved configuration without saving any of your changes.

7.6.2.2 Adding an External Radius Server

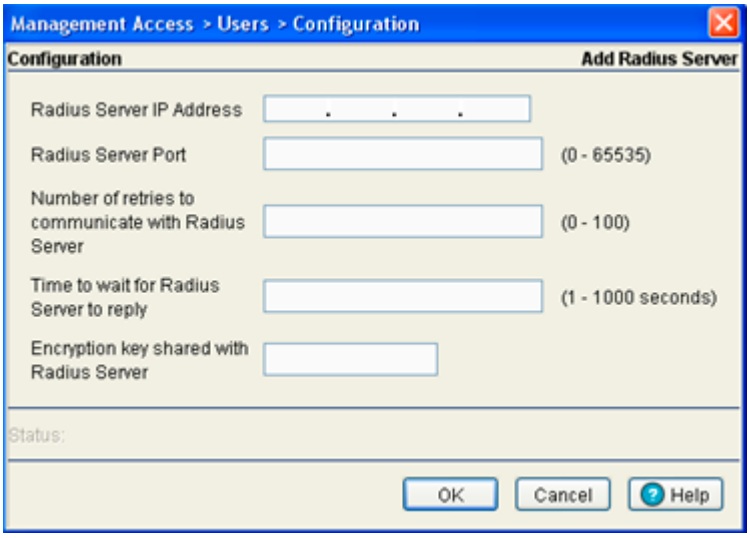
The attributes of a new Radius Server can be defined by the switch to provide a new user authentication server. Once the server is configured and added, it displays within the **Authentication** tab as an option available to the switch.

To define the attributes of a new Radius Server:

1. Select **Management Access** > **Users** from the main menu tree.

   The Users screen displays.

2. Select the **Authentication** tab.
3. Click the **Add** button at the bottom of the screen.



4. Configure the following Radius Server attributes:

Radius Server IP Address	Provide the IP address of the external Radius Server. Ensure this address is a valid IP address and not a DNS name.
Radius Server Port	Enter the TCP/IP port number for the Radius Server. The port range available for assignment is from 1 - 65535.
Number of retries to communicate with Radius Server	Enter the maximum number of times for the switch to retransmit a Radius Server frame before it times out the authentication session. The available range is between 0 - 100.
Time to wait for Radius Server to reply	Enter the maximum number of times the switch can retransmit a Radius Server frame before it times out of the authentication session. The available range is between 0 - 100.
Encryption key shared with Radius Server	Enter the encryption key the switch and Radius Server share and must validate before the user based authentication provided by the Radius Server can be initiated.

5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click on **OK** to complete the addition of the Radius Server.
7. Click **Cancel** to revert back to the last saved configuration without saving any of your changes.

7.6.2.3 External Radius Server Settings

When using an external Radius Server with the switch, ensure that the following values are configured on your server to ensure maximum compatibility with the switch.

Vendor ID

Vendor ID	The Motorola vendor ID is 388

Radius VSAs

There are two radius VSAs used for management user authentication.

VSA Name	*Attribute Number*	*Type*	*Values*
Symbol-Service-Type	1	Integer (Decimal)	• *Monitor Role* - Value is 1. (read-only access to the switch) • *Helpdesk Role* - Value is 2 (helpdesk/support access to the switch) • *Nwadmin Role* - Value is 4 (all wired and wireless access to the switch) • *Sysadmin Role* - Value is 8. (System administrator access) • *WebAdmin Role* - Value is 16 (Guest user application access) • *Superuser Role* - Value is 32768 (grants full read/write access to the switch) **Note:** To configure multiple roles, this value can be configured multiple times with different values for each role.
Symbol-Login-Service	100	Integer (Decimal)	• *Console Access* - Value is 128 (user is allowed to login only from console) • *Telnet Access* - Value is 64 (use is allowed to login only from telnet session) • *SSH Access* - Value is 32 (user is allowed to login only from ssh session) • *Web Access* - Value is 16 (user is allowed to login only from web/ applet) **Note:** To configure multiple access methods, this value can be set multiple times with different access values, or the desired values can be added together and and entered as a single entry.

8

Diagnostics

This chapter describes the various diagnostic features available for monitoring switch performance. This chapter consists of the following switch diagnostic activities:

- *Displaying the Main Diagnostic Interface*
- *Configuring System Logging*
- *Reviewing Core Snapshots*
- *Reviewing Panic Snapshots*
- *Debugging the Applet*
- *Configuring a Ping*

NOTE: HTTPS must be enabled to access the switch applet. Ensure HTTPS access has been enabled before using the login screen to access the switch applet.

NOTE: The *Motorola RF Management Software* is a recommended utility to plan the deployment of the switch and view its configuration once operational. Motorola RFMS can help optimize the positioning and configuration of a switch and assist in the troubleshooting of performance issues as they are encountered in the field.

8.1 Displaying the Main Diagnostic Interface

The main diagnostic screen contains tabs assessing the performance of the following diagnostics:

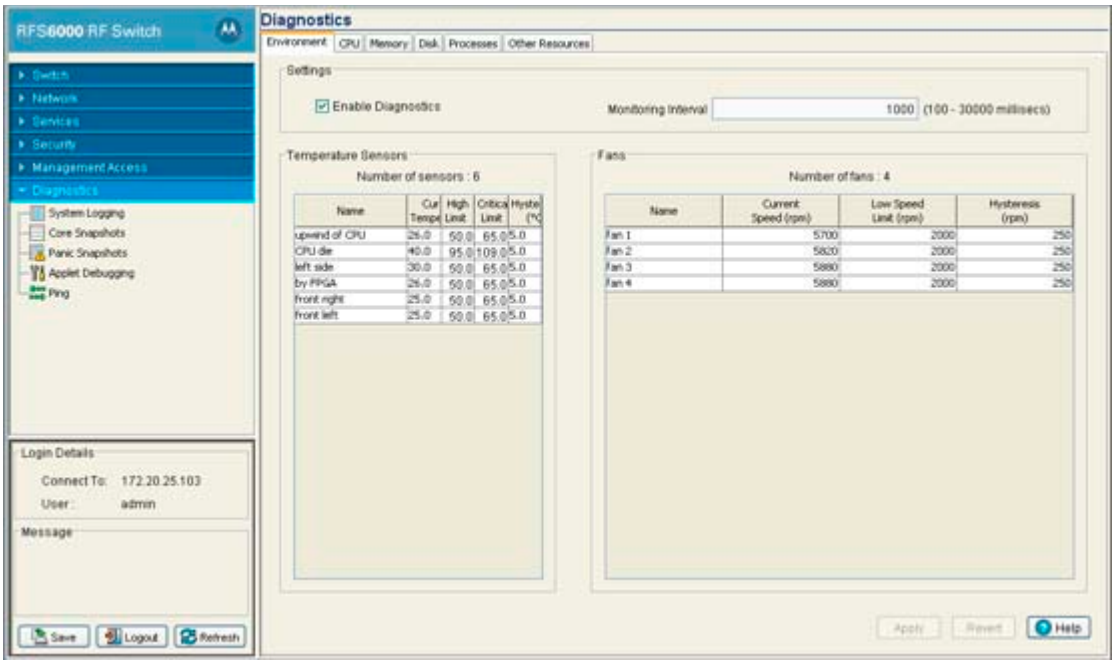
- *Switch Environment*
- *CPU Performance*
- *Switch Memory Allocation*
- *Switch Disk Allocation*
- *Switch Memory Processes*
- *Other Switch Resources*

NOTE: When the switch's configuration is successfully updated (using the Web UI), the effected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the effected screen's Status field and the screen remains displayed. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

8.1.1 Switch Environment

Use the **Environment** tab to view and modify the switch diagnostic interval, temperature sensors and fan speeds.

1. Select **Diagnostics** from the main tree menu.
2. Select the **Environment** tab (opened by default).



3. The Environment displays the following fields:
   - *Settings*
   - *Temperature Sensors*
   - *Fans*
4. In the Settings field, select the **Enable Diagnostics** checkbox to enable/disable diagnostics and set the monitoring interval. The monitoring interval is the interval the switch uses to update the information displayed within the CPU, Memory, Disk, Processes and Other Resources tabs.
   Keep the monitoring interval at a shorter time increment when periods of heavy wireless traffic are anticipated.

NOTE: Enabling switch diagnostics is recommended, as the diagnostics facilities provide detailed information on the physical performance of the switch and may provide indicators in advance of actual problems. Enabling diagnostics also assists in troubleshooting problems associated with data transfers and the monitoring of network traffic.

5. Use the Temperature Sensors field to monitor the CPU and system temperatures. This information is extremely useful in assessing if the switch exceeds its critical limits.

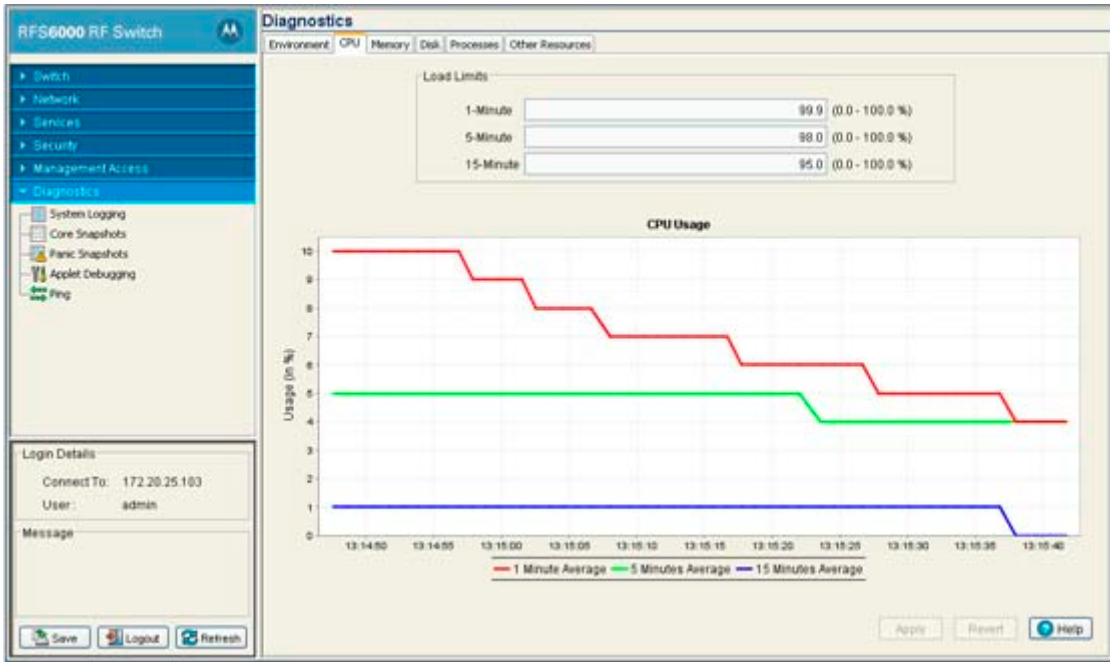
SWITCH NOTE: A RF7000 Series Switch has six sensors.

6. Refer to the **Fans** field to monitor the CPU and system fan speeds.
7. Click the **Apply** button to commit and apply the changes.
8. Click the **Revert** button to revert back to the last saved configuration.

8.1.2 CPU Performance

Use the **CPU** tab to view and define the CPU's load statistics. Load limits can be assessed for the last one minute, five minutes and 15 minutes to better gauge switch loads over differing periods of network activity.

1. Select **Diagnostics** from the main tree menu.
2. Select the **CPU** tab.



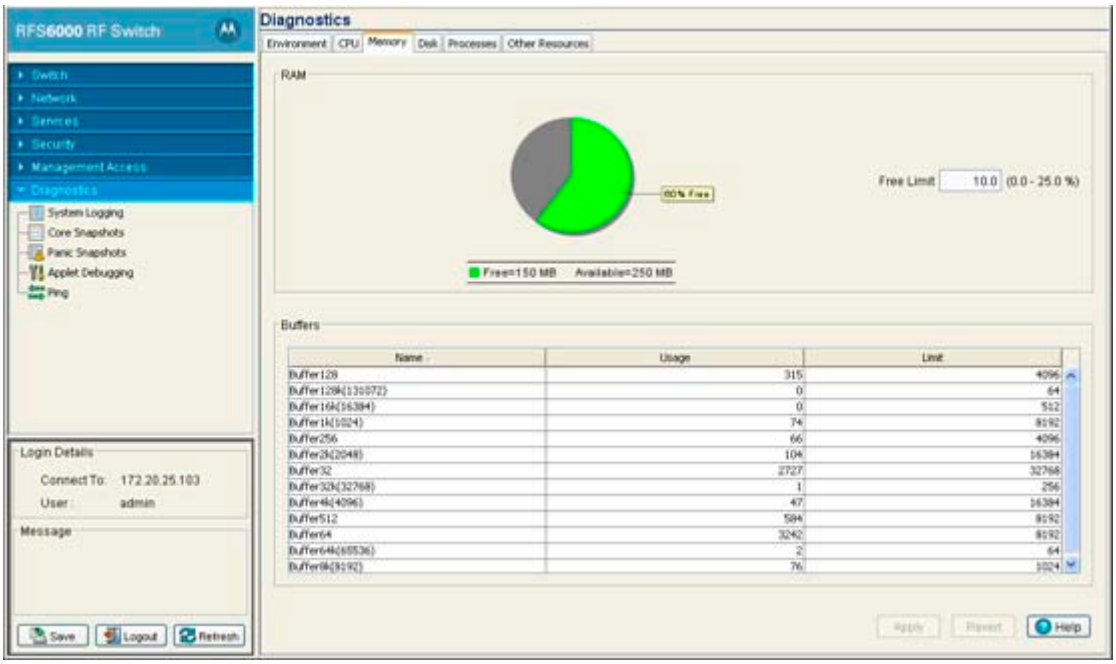
3. The **CPU** screen consists of 2 fields:
   - *Load Limits*
   - *CPU Usage*
4. The **Load Limits** field displays the maximum CPU load limits for the last 1, 5, and 15 minutes. The limits displayed coincide with periods of increased or decreased switch activity. The maximum CPU load threshold can be manually configured.
5. The **CPU Usage** field displays real time CPU consumption values. Use this information to periodically determine if performance is negatively impacted by the over usage of switch CPU resources. If CPU usage is substantial during periods of low network activity, then perhaps, the situation requires troubleshooting.

6. Click the **Apply** button to commit and apply the changes.
7. Click the **Revert** button to revert back to the last saved configuration.

8.1.3 Switch Memory Allocation

Use the **Memory** tab to periodically assess the switch's memory load.

1. Select **Diagnostics** from the main tree menu.
2. Select the **Memory** tab.



The Memory tab is partitioned into the following two fields:

- *RAM*
- *Buffer*

3. Refer to the **RAM** field to view the percentage of CPU memory in use (in a pie chart format).
4. Refer to the **Free Limit** value to change the CPUs memory allocation limits. Free Limit should be configured in respect to high bandwidth and increased load anticipated over the switch managed network.
5. The **Buffers** field displays buffer usage information. The Buffers field consists the following information:

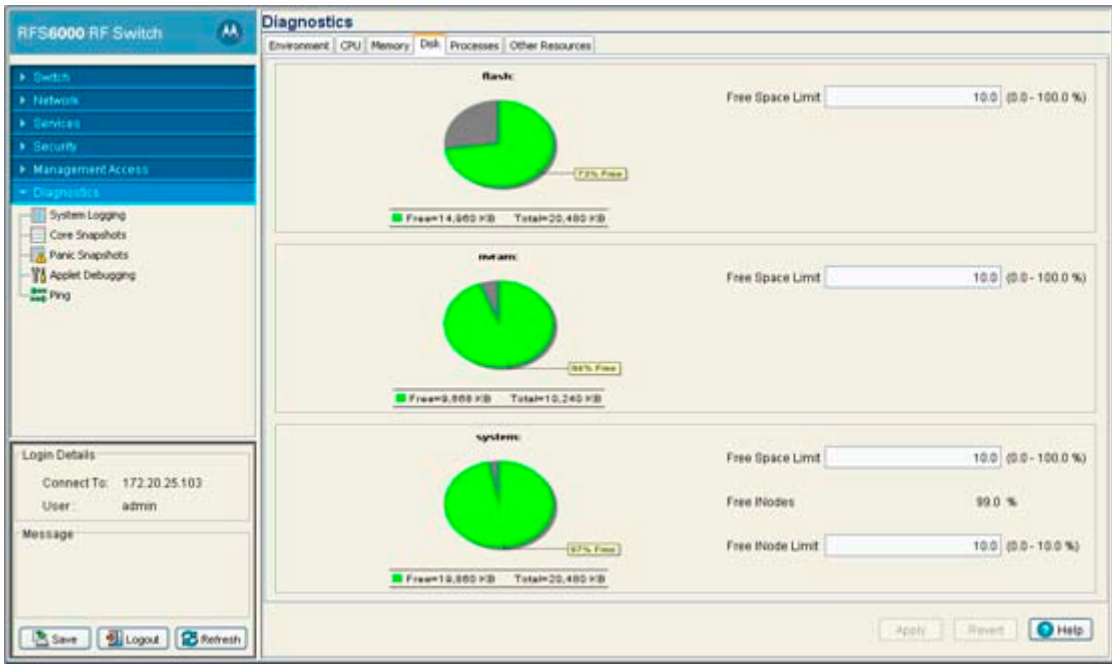
Name	The name of the buffer.
Usage	Buffers current usage
Limit	The buffer limit.

6. Click the **Apply** button to commit and apply the changes.
7. Click the **Revert b**utton to revert back to the last saved configuration.

8.1.4 Switch Disk Allocation

The **Disk** tab contains parameters related to the various disk partitions on the switch. It also displays available space in the external drives (compact flash etc).

1. Select **Diagnostics** from the main tree menu.
2. Select the **Disk** tab.

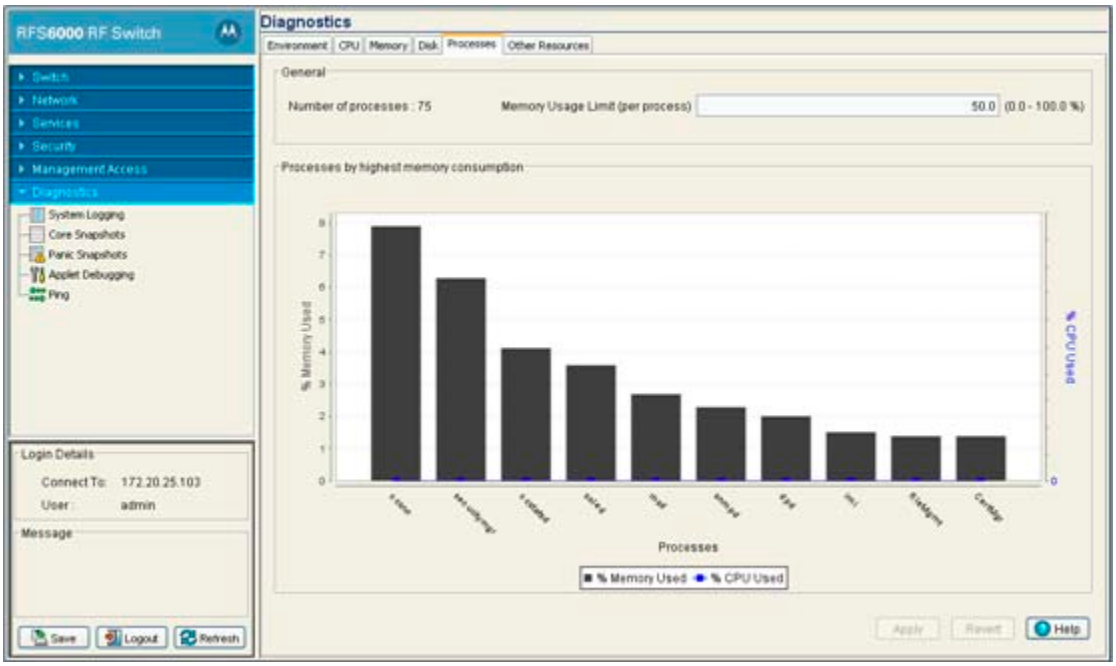


3. This **Disk** tab displays the status of the switch flash, nvram and system disk resources. Each field displays the following:
   - *Free Space Limit*
   - *Free INodes*
   - *Free INode Limit*
4. Define the **Free Space Limit** variable carefully, as disk space may be required during periods of high bandwidth traffic and file transfers.
5. Click the **Apply** button to commit and apply the changes.
6. Click the **Revert** button to revert back to the last saved configuration.

8.1.5 Switch Memory Processes

The **Processes** tab displays the number of processes in use and percentage of memory usage limit per process.

1. Select **Diagnostics** from the main tree menu.
2. Select the **Processes** tab.

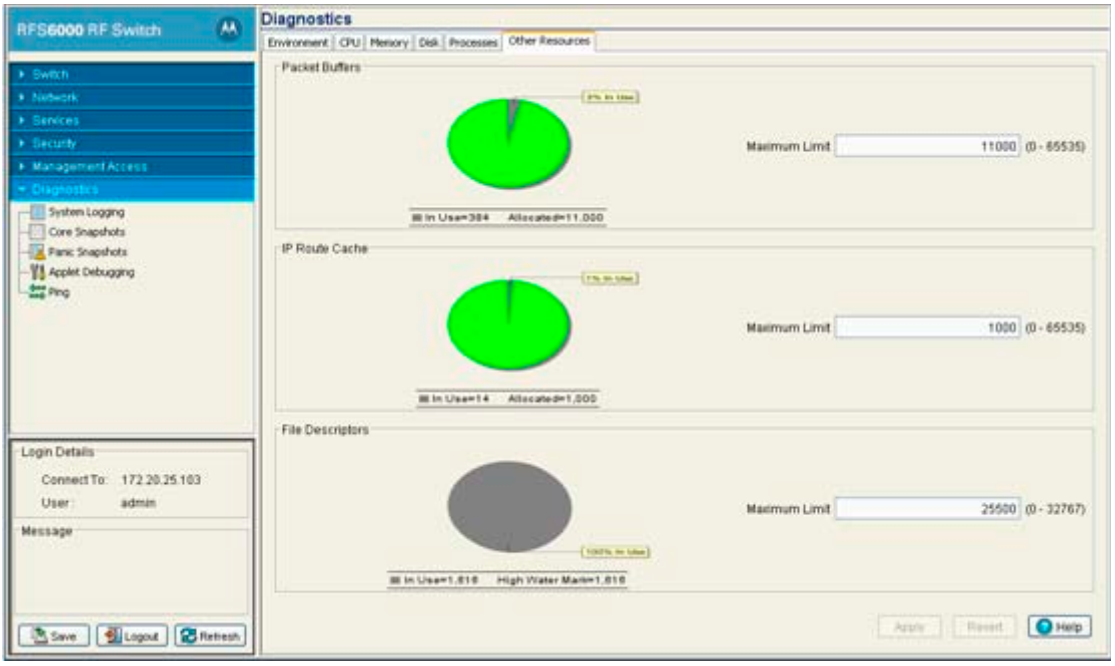


3. The **Processes** tab has two fields:
   - *General*
   - *Processes by highest memory consumption*
4. Refer to the **General** field to review the number of processes in use and percentage of memory usage per process. The value defined is the maximum limit per process during periods of increased and network activity and is negotiated amongst the other process as needed during normal periods of switch activity.
5. **Processes by highest memory consumption** displays a graph of the top ten switch processes based on memory consumption. Use this information to determine if a spike in consumption with the switch priorities in processing data traffic within the switch managed network.
6. Click the **Apply** button to commit and apply any changes to the memory usage limit.
7. Click the **Revert** button to revert back to the last saved configuration.

8.1.6 Other Switch Resources

The **Other Resources** tab displays the memory allocation of Packet Buffer, IP Route Cache and File Descriptors.

1. Select **Diagnostics** from the main tree menu.
2. Select the **Other Resources** tab.



Keep the Cache allocation in line with cache expectations required within the switch managed network.

3. Define the maximum limit for each resource accordingly as you expect these resources to be utilized within the switch managed network.
4. Click the **Apply** button to commit and apply any changes to any of the resources maximum limit.
5. Click the **Revert** button to revert back to the last saved configuration

8.2 Configuring System Logging

Use the **System Logging** screen for logging system events. Its important to log individual switch events to discern an overall pattern that may be negatively impacting switch performance. The System Logging screen consist of the following tabs:

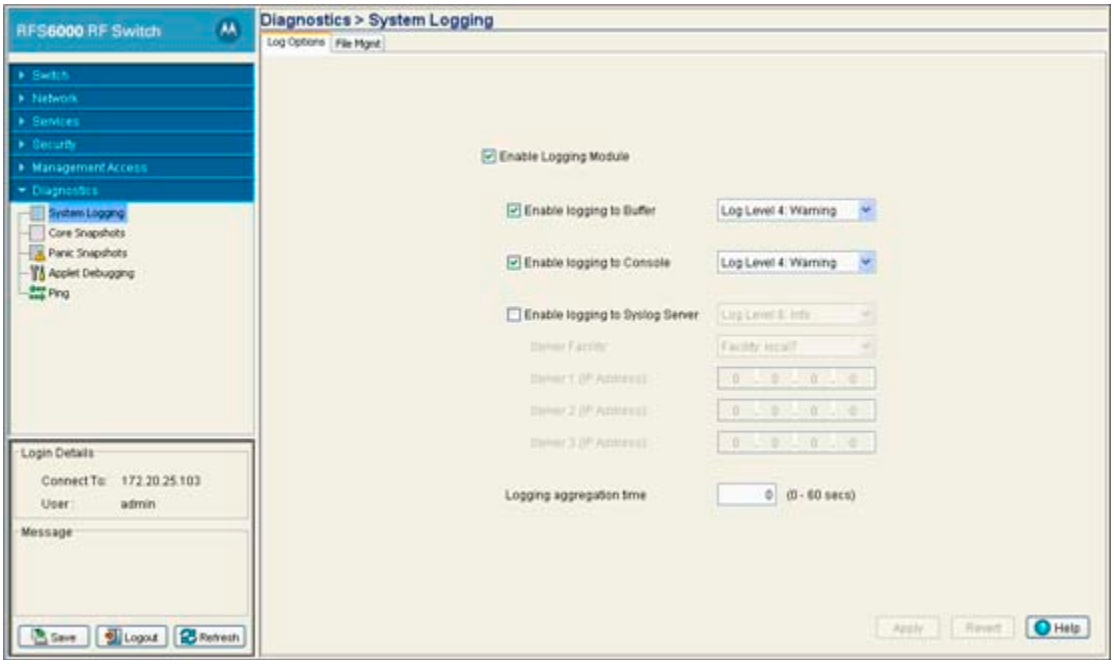
- *Log Options*
- *File Management*

8.2.1 Log Options

Use the Log Options tab to enable logging and define the medium used to capture system events and append them to the log file. Ensure the correct destination server address is supplied.

To view the Log options available to the switch:

1. Select **Diagnostics** > **System Logging** from the main menu tree.
2. Select the **Log Options** tab.



3. Select the **Enable Logging Module** checkbox to enable the switch to log system events to a user defined log file or a syslog server.
4. Select the **Enable Logging to Buffer** checkbox to enable the switch to log system events to a buffer.

   The log levels are categorized by their severity. The default level is 3, (errors detected by the switch). However, more granular log levels can be selected for system level information detected by the switch that may be useful in assessing overall switch performance or troubleshooting.
5. Select the **Enable Logging to Console** checkbox to enable the switch to log system events to the system console.

   Use the drop-down menu to select the desired log level for tracking system events to a local log file. This setting logs warning events (and those more severe) by default.
6. Select the **Enable Logging to Syslog Server** checkbox to enable the switch to log system events send them to an external syslog server. Selecting this option also enables the Server Facility feature. Use the drop-down menu to select the desired log level for tracking system events to a local log file.
   a. Use the **Server Facility** drop-down menu to specify the local server facility (if used) for the transfer.
   b. Specify the numerical (non DNS name) IP address for the first choice syslog server to log system events (within the **Server 1** field.
   c. Optionally, use the **Server 2** parameter to specify the numerical (non DNS name) IP address of an alternative syslog server if the first syslog server is unavailable.
   d. Optionally, use the **Server 3** parameter to specify the numerical (non DNS name) IP address of a third syslog server to log system events if the first two syslog servers are unavailable.

NOTE: 255.255.255.255 is accepted as a valid entry for the IP address of a logging server.

7. Use the **Logging aggregation time** parameter to define the increment (or interval) system events are logged (0-60 seconds). The shorter the interval, the sooner the event is logged.

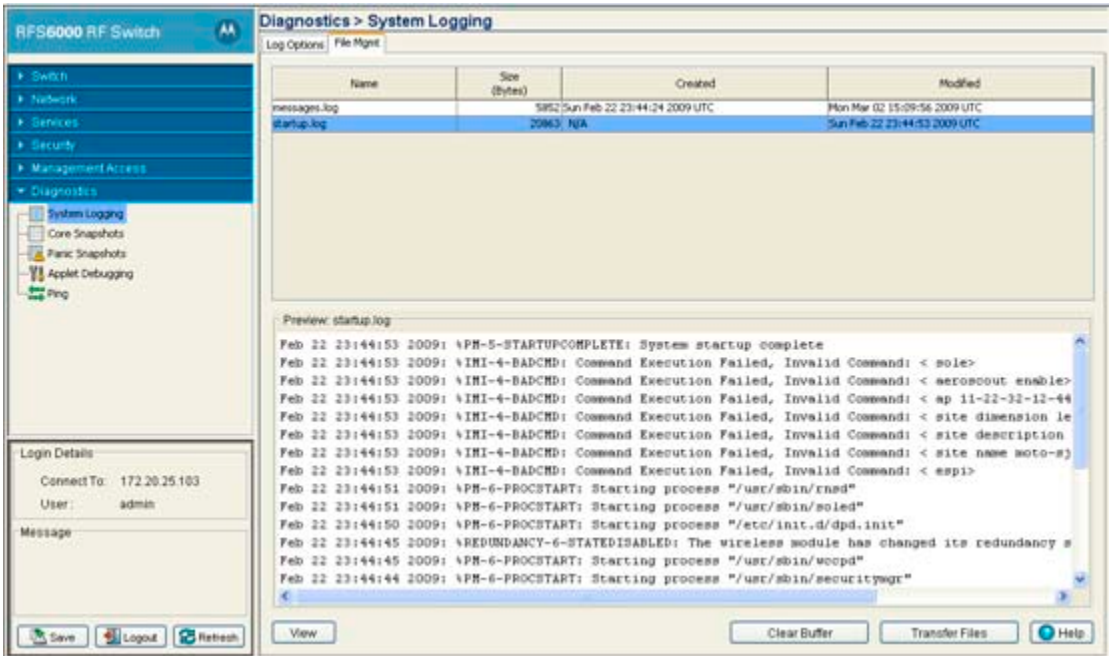
8. Click **Apply** to save the changes made to the screen. This will overwrite the previous configuration.
9. Click the **Revert** button to move the display back to the last saved configuration.

8.2.2 File Management

Use the **File Mgt** tab to view existing system logs. Select a file to display its details in the **Preview** field. Click the **View** button to display the file's entire contents. Once viewed, the user has the option of clearing the file or transferring the file to a user-defined location.

To view the Log options:

1. Select **Diagnostics** > **System Logging** from the main menu tree.
2. Select the **File Mgmt** tab.



3. The **File Mgmt** tab displays existing log files. Refer to the following for log file details:

Name	Displays a read-only list of the log files (by name) created since the last time the display was cleared. To define the type of log files created, click the **Log Options** tab to enable logging and define the log level.
Size	Displays the log file size in bytes. This is the current size of the file, if modifications were made, they have been accounted for.
Created	Displays the date, year and time of day the log file was initially created. This value only states the time the file was initiated, not the time it was modified or appended.
Modified	Displays the date, year and time of day the log file was modified since its initial creation date.

4. Highlight an existing log file to display the file's first page within the **Preview** field. Once a file is selected, its name is appended within the preview field, and its contents are displayed.

   The time, module, severity, mnemonic and description of the file are displayed.

5. Highlight a file from the list of log files available within the File Mgt tab and click the **View** button to display a detailed description of the entire contents of the log file.

   To view the entire content of an individual log file, see *Viewing the Entire Contents of Individual Log Files on page 8-10*.

6. Click the **Clear Buffer** button to remove the contents of the File Mgt tab. This is only recommended if you consider the contents of this file obsolete and wish to begin gathering new log file data.

   When the button is selected, a confirmation prompt displays verifying whether the contents of the log files is cleared.

7. Click the **Transfer Files** button to display a sub-screen wherein log files can be sent to an external location (defined by you) using a user-defined file transfer medium.

SWITCH NOTE: On the RFS7000 users can also transfer log files using USB or Compact Flash. On the RFS6000 users can also transfer log files using USB.

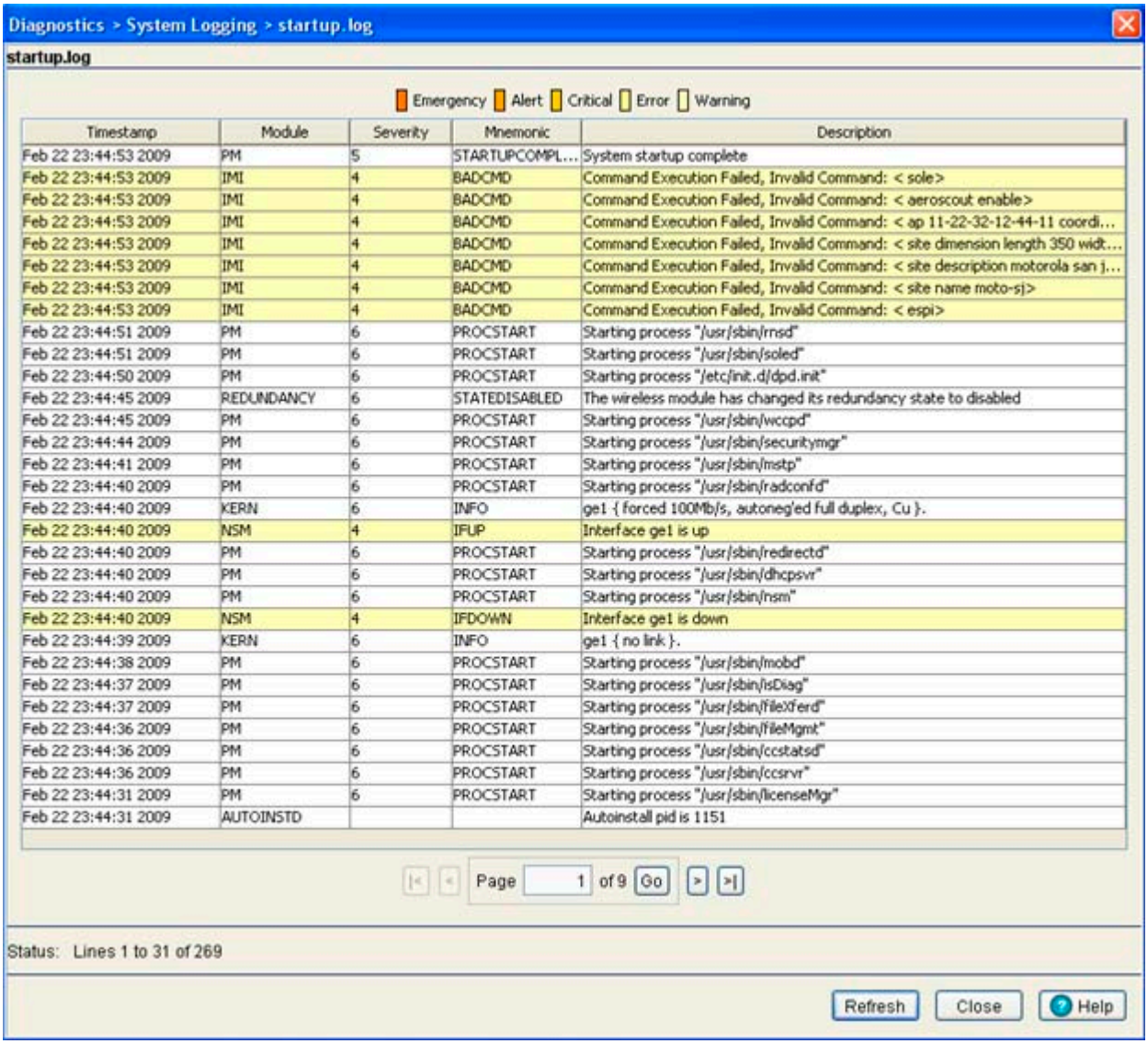
Transferring files is recommended when the log file is frequently cleared, but an archive of the log files is required in a safe location. For more information on transferring individual log files, see *Transferring Log Files on page 8-12*.

8.2.2.1 Viewing the Entire Contents of Individual Log Files

Motorola recommends the entire contents of a log file be viewed to make an informed decision whether to transfer the file or clear the buffer. The **View** screen provides additional details about a target file by allowing the entire contents of a log file to be reviewed.

To display the entire contents of a log file:

1. Select **Diagnostics** > **System Logging** from the main menu tree.
2. Select the **File Mgt** tab.
3. Select an individual log file whose properties you wish to display in detail and click the **View** button.



4. Refer to the following for information on the elements that can be viewed within a log file:

Timestamp — Displays the date, year and time of day the log file was initially created. This value only states the time the file was initiated, not the time it was modified or appended.

Module — Displays the name of the switch logging the target event. This metric is important for troubleshooting issues of a more serious priority, as it helps isolate the switch resource detecting the problem.

Severity	The Severity level coincides with the logging levels defined within the Log Options tab. Use these numeric identifiers to assess the criticality of the displayed event. The severity levels include: • *0 - Emergency* • *1 - Alert* • *2 - Critical* • *3 - Errors* • *4 - Warning* • *5 - Notice* • *6 - Info* • *7 - Debug*
Mnemonic	Use the **Mnemonic** as a text version of the severity code information. A mnemonic is convention for the classification, organization, storage and recollection of switch information.
Description	Displays a high-level overview of the event, and (when applicable) message type, error or completion codes for further clarification of the event. Use this information for troubleshooting or for data collection.

5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click the **Refresh** button to update the contents of the screen to the latest values.
7. Click the **Close** button to exit the screen. Clicking Close does not lose any data, as there are no values configured within this screen (it is view-only).

8.2.2.2 Transferring Log Files

If a system log contains data that may require archiving, consider using the **Transfer Files** screen to export the log file to an external location (that you designate) where there is no risk of deleting the contents of the log.

To transfer a log file to a user specified location:

1. Select **Diagnostics** > **System Logging** from the main menu tree.
2. Select the **File Mgt** tab.
3. Select a target log file to transfer and click the **Transfer File** button.
4. Use the **From** drop-down menu (within the Source field) to specify the location from which the log file is sent. If only the applet is available as a transfer location, use the default switch option.
5. Select a target file for transfer from the **File** drop-down menu. The drop-down menu contains the log files listed within the **File-Mgt** screen.
6. Use the **To** drop-down menu (within the Target field) to define whether the target log file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
7. Provide the name of the file to be transferred within the **File** parameter. Ensure the file name is correct or the transfer will not take place.
8. If Server has been selected as the source, use the **Using** drop down-menu to configure whether the log file transfer is conducted using FTP or TFTP.

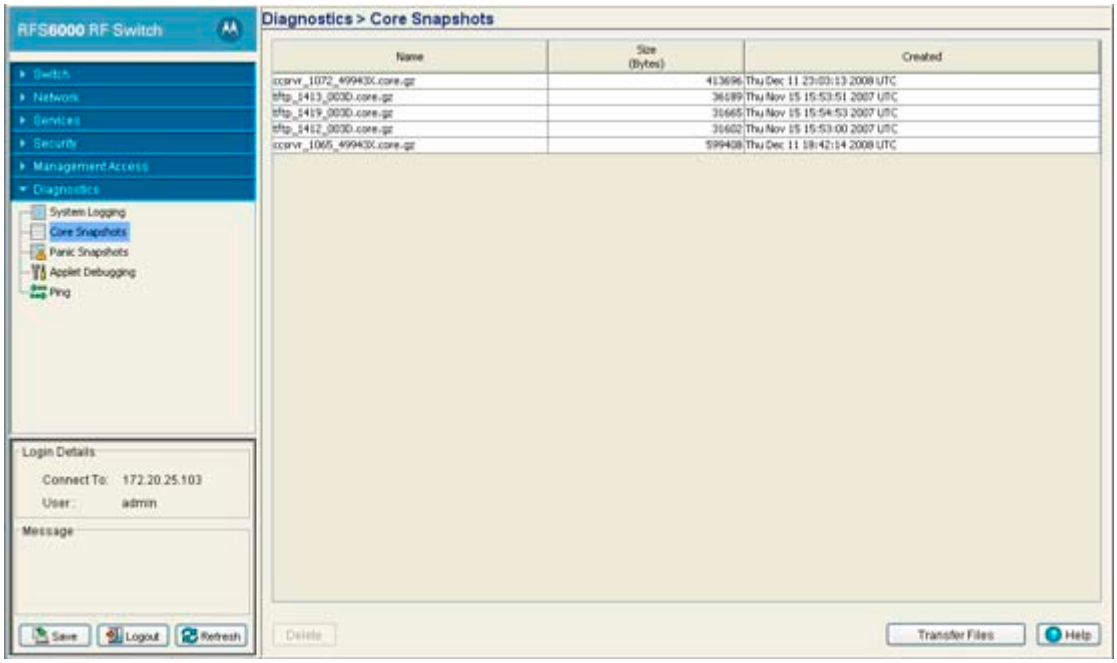
9. If Server has been selected as the source, enter the **IP Address** of the destination server or system receiving the log file. Ensure the IP address is valid or risk jeopardizing the success of the log file transfer.
10. If Server has been selected as the source, enter the **User ID** credentials required to send the log file to the target location.
11. If Server has been selected as the source, use the **Password** parameter to enter the password required to send the log file to the target location.
12. Specify the appropriate **Path** name to the target directory on the local system disk or server as configured using the **To** parameter. If the local disk is selected, a browse button is available.
13. Click the **Transfer** button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired log file to the specified location.
14. If a problem condition is discovered during the file transfer, click the **Abort** button to terminate the transfer.
15. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
16. Click the **Close** button to exit the screen. No values need to be saved once the transfer has been made.

8.3 Reviewing Core Snapshots

Use the **Core Snapshots** screen to view the core snapshots (system events and process failures with a .core extension) logged by the system. Core snapshots are issues impacting switch core (or distribution layer). Once reviewed, core files can be deleted or transferred for archive.

To view core snapshots available on the switch:

1. Select **Diagnostics** > **Core Snapshots** from the main menu tree.



2. Refer to the following table headings within the Core Snapshots screen:

Name	Displays the title of the process, *process ID* (pid) and build number separated by underscores. The file extension is always .core for core files.
Size (Bytes)	Displays the size of the core file in bytes.
Created	Displays the date and time the core file was generated. This information may be useful in troubleshooting issues.

3. Select a target file and click the **Delete** button to remove the selected file. This option is not recommended until the severity of the core snapshot has been assessed.
4. Click the **Transfer Files** button to open the transfer dialogue to enable a file to be copied to another location. For more information on transferring core snapshots, see *Transferring Core Snapshots on page 8-14*.

8.3.1 Transferring Core Snapshots

Use the **Transfer** screen to define a source for transferring core snapshot files to a secure location for potential archive.

To transfer core snapshots to a user defined location:

1. Select **Diagnostics** > **Core Snapshots** from the main menu tree.
2. Select a target file, and select the **Transfer Files** button.
3. Use the **From** drop-down menu to specify the location from which the log file is sent.

   If only the applet is available as a transfer location, use the default switch option.
4. Select a target file for the file transfer from the **File** drop-down menu.

   The drop-down menu contains the core files listed within the File-Mgmt screen.
5. Use the **To** drop-down menu (within the Target field) to define whether the target log file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
6. Provide the name of the file to be transferred to the location specified within the **File** field.
7. If Server has been selected as the source, use the **Using** drop down-menu to configure whether the log file transfer is sent using FTP or TFTP.
8. If Server has been selected as the source, enter the **IP Address** of destination server or system receiving the target log file.
9. If Server has been selected as the source, enter the **User ID** credentials required to send the file to the target location. Use the user ID for FTP transfers only.
10. If Server has been selected as the source, enter the **Password** required to send the file to the target location using FTP.
11. Specify the appropriate **Path** to the target directory on the local system disk or server as configured using the **To** parameter. If the local disk option is selected, use the browse button to specify the location on the local disk.
12. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
13. Click the **Transfer** button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired log file to the specified location.

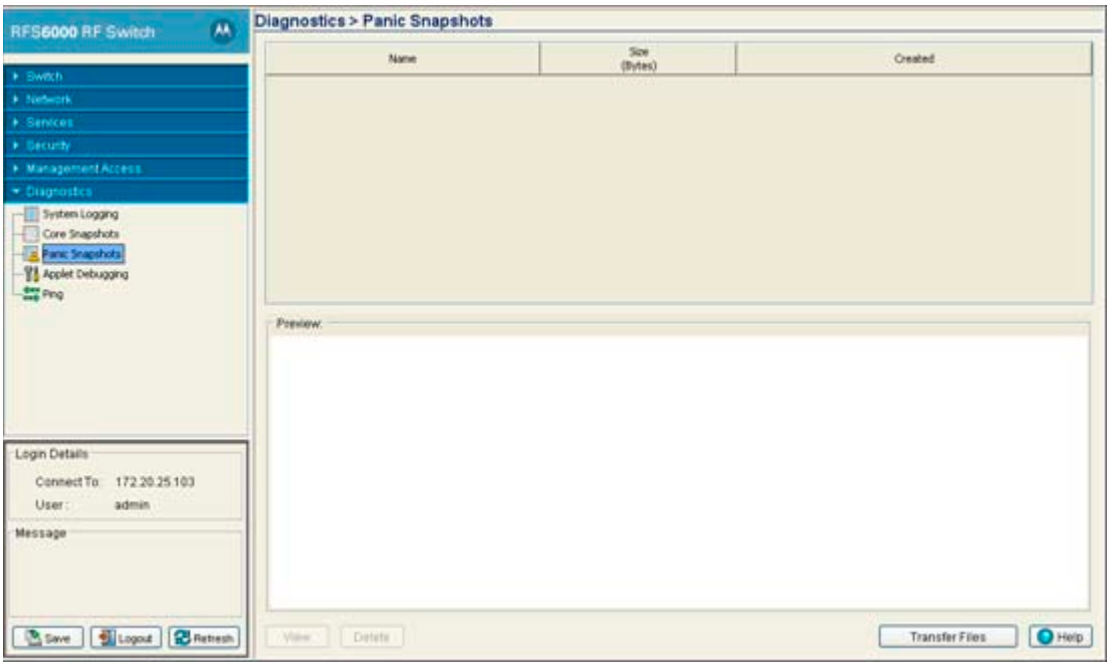
14. If a problem condition is discovered during the file transfer, click the **Abort** button to terminate the transfer.
15. Click the **Close** button to exit the screen after a transfer. There are no changes to save or apply.

8.4 Reviewing Panic Snapshots

Refer to the **Panic Snapshots** screen for an overview of the panic files available. Typically, panic files refer to switch events interpreted as critical conditions (and thus requiring prompt attention). Use the information displayed within the screen to make informed decisions whether a target file should be discarded or transferred to a secure location for permanent archive.

To review the current panic snapshots on the switch:

1. Select **Diagnostics** > **Panic Snapshots** from the main menu.



2. Refer to the following table headings within the Panic Snapshots screen:

Name	Displays the title of the panic file. Panic files are named n.panic where n is in the range 0-9. 0 is always the oldest saved panic file and the highest number is the most recent. If the system experiences a panic, there are ten existing panics, the oldest is deleted and the remaining nine are renamed so the newest can be saved as 9.
Size	Displays the size of the panic file in bytes.
Created	Displays the date and time the panic file was created. The panic file is created after the system reboots, however the panic information within the file contains the date and time the panic actually occurred.

3. Refer to the **Preview** field for panic information in ASCII text. When a panic file is selected, the corresponding text is displayed in the preview screen and the name of the file displays. Use this information as a high-level overview of the panic.

4. Select a target panic file and click the **Delete** button to remove the file.
5. Select a target panic file and click the **View** button to open a separate viewing screen to display the panic information in greater detail. For more information, see *Viewing Panic Details on page 8-16*.
6. Click the **Transfer Files** button to open the transfer dialogue to transfer the file to another location. For more information, see *Transferring Panic Files on page 8-16*.

8.4.1 Viewing Panic Details

Use the **View** facility to review the entire contents of a panic snapshot before transferring or deleting the file. The view screen enables you to display the entire file.

To review Panic Snapshots:

1. Select **Diagnostics** > **Panic Snapshots** from the main menu.
2. Select a panic from those available and click the **View** button.
3. Refer to the following information to review the severity of the panic file:

Main	The **Main** parameter displays detailed panic information for the selected file.
Page	Panic information may be spread across multiple pages. The Page value allows the user to view complete information on the panic. Use the < and > options to navigate through the contents of the file.
Refresh	Click the **Refresh** button to update the data displayed within the screen to the latest values.
Close	Click the **Close** button to exit the screen.

8.4.2 Transferring Panic Files

It is recommended that panic snapshots files be kept in a safe location off the system used to create the initial files. Use the **Transfer Files** screen to specify a location where files can be archived without the risk of them being lost or corrupted.

For information on transferring panic files:

1. Select **Diagnostics** > **Panic Snapshots** from the main menu.
2. Select a record from those available and click the **Transfer** button.
3. Use the **From** drop-down menu to specify the location from which the file is sent. If only the applet is available as a transfer location, use the default switch option.
4. Select a file for the file transfer from the **File** drop-down menu. The drop-down menu contains the panic files listed within the File-Mgmt screen.
5. Use the **To** drop-down menu (within the Target field) to define whether the target panic file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
6. Provide the name of the file to be transferred to the location specified within the **File** field.
7. If Server has been selected as the source, use the **Using** drop down-menu to configure whether the panic file transfer will be sent using FTP or TFTP.
8. If Server has been selected as the source, enter the **IP Address** of the destination server or system receiving the target panic file.

9. If Server has been selected as the source, enter the **User ID** credentials required to send the file to the target location. The User ID is required for FTP transfers only.
10. If Server has been selected as the source, enter the **Password** required (for FTP transfers) to send the file to the target location.
11. Specify the appropriate path name to the target directory on the local system disk or server as configured using the "To" parameter. If local server is selected, use the Browse button to specify a location on your local machine.
12. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
13. Click the **Transfer** button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired log file to the specified location.
14. If a problem condition is discovered during the file transfer, click the **Abort** button to terminate the transfer.
15. Click the **Close** button to exit the dialogue and abandon the transfer.

8.5 Debugging the Applet

Refer to the **Applet Debugging** screen to debug the applet. This screen allows you to view and debug system events by a criticality level you define.

1. Select **Diagnostics** > **Applet Debugging** from the main menu.

2. To use this window, select the **Enable Web-UI Debug Mode** checkbox.

   The Applet Debugging field is partitioned into the following editable fields:

   - *Send log message to a file.*
   - *Use SNMP v2 only.*
   - *Message Severity.*

- *What kinds of message should be seen.*

3. Select the **Send log message to a file** checkbox if you wish to store the log message.

   Enabling this checkbox allows you to select the file location where you wish to store the log message.

4. Select the **Use SNMP V2 only** checkbox to use SNMP v2 to debug the applet.

   Check whether you have access to SNMP v2 by clicking on the **Test SNMP V2 access** button. If SNMP v2 access is available, the test icon will change from grey to green, indicating the SNMPv2 interface is viable on the switch.

5. Select the severity of the message you wish to store in the log file.

   The **Message Severity** section allows you to report a bug and log it as per the following severity levels:

   - *Fatal* - loss of data or switch functionality
   - *Error* - switch data compilation problem, could result in data loss
   - *Warning* - potential data loss of configuration corruption
   - *Informational* - data that may be useful in assessing a potential error
   - *Debug* - information relevant to troubleshooting
   - *None* - no impact.

6. Select the message deployed when a bug is raised.

   The **What Kind of message should be seen** field allows you to select a range of parameters for returned messages while debugging. Move your mouse pointer over a message checkbox for a message description.

   a. Click the **Advanced** button to display the entire list of message categories when bugs are raised. Select the checkboxes corresponding to the message types you would like to receive.

      Each message category is enabled by default. Click the **Simple** button to minimize this area and hide the available message categories.

   b. Click the **All Messages** button to select all the message categories.

   c. Click the **No Messages** button if you do not want to select any of the message categories.

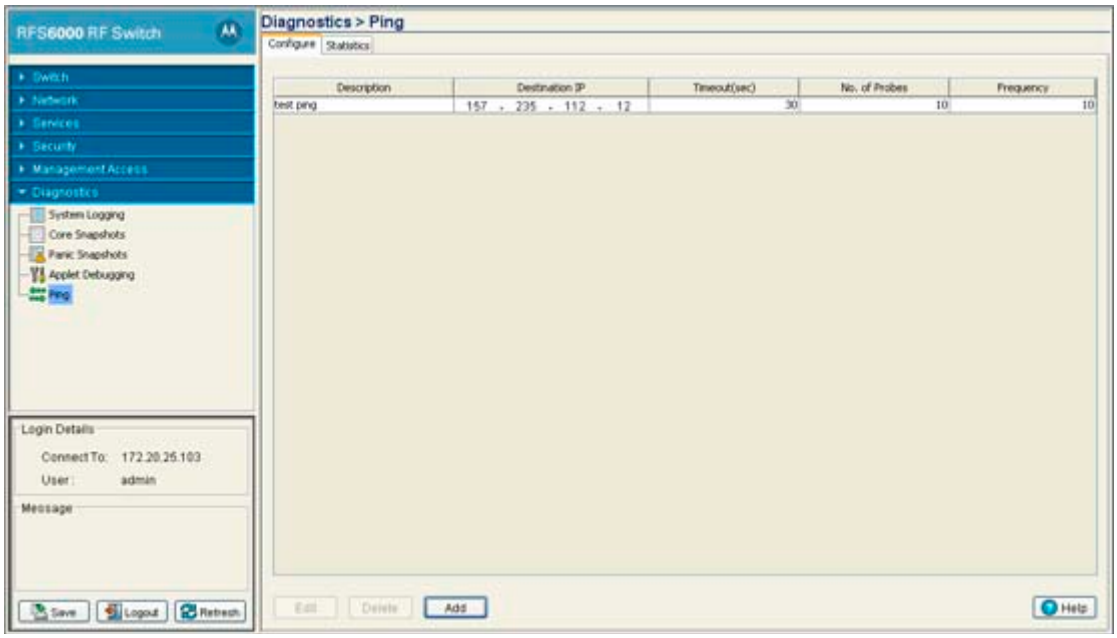
7. Click the **Apply** button to save the changes you have applied within this screen.
8. Click the **Revert** button to revert back to the last saved configuration.

8.6 Configuring a Ping

The switch can verify its link with other switches and associated MUs by sending ping packets to the associated device. Use a ping to test the connection between the switch and IP destinations you specify. For each ping packet transmitted, statistics are gathered for the round-trip time (RTT) between the switch and its destination. The RTT is the time (in milliseconds) for a ping packet to travel from the switch to its target destination and back again. This number can vary significantly due to the random nature of packet routings and random loads on the switch and its destination.

To view the switch's existing ping configuration:

1. Select **Diagnostics** > **Ping** from the main menu.



2. Refer to the following information displayed within the Configuration tab:

Description	Displays the user assigned description of the ping test. The name is read-only. Use this title to determine whether this test can be used as is or if a new ping test is required.
Destination IP	Displays the IP address of the target device. This is the numeric destination for the device sent the ping packets. If this address does not accurately reflect the ping destination target, the ping test will not be successful.
Timeout (sec)	Displays the timeout value (in seconds) used to timeout the ping test if a round trip packet is not received from the target device.
No. of Probes	Displays the number of packets transmitted to the target IP address to discern the round trip time between the switch and its connected device.
Frequency	Define the interval (in seconds) between ping packet transmissions. Define a longer interval if high levels of network congestion are anticipated between the switch and its target device. Use a value of 0 to execute a single ping test or stop a currently executing ping test.

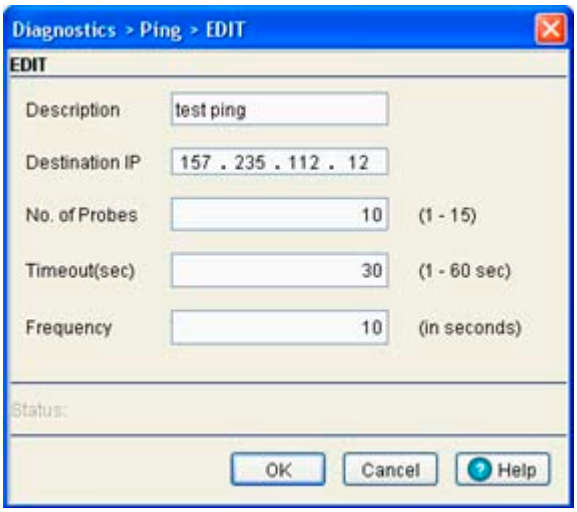
3. To edit the properties of an existing ping test, select a ping based on the description listed and click the **Edit** button. For more information, see *Modifying the Configuration of an Existing Ping Test on page 8-19*.
4. Select an existing ping test from those displayed within the Configure tab and click the **Delete** button to remove the ping test from those displayed.
5. Click the **Add** button to display a screen used to define the attributes of a new ping test. For more information, see *Adding a New Ping Test on page 8-20*.

8.6.1 Modifying the Configuration of an Existing Ping Test

The properties of an existing ping tests can be modified to ping an existing (known) device whose network address attributes may have changed and require modification to connect (ping) to it.

To modify the attributes of an existing ping test:

1. Select **Diagnostics** > **Ping** from the main menu.
2. Highlight an existing ping test within the Configuration tab and select the **Edit** button.



3. Modify the following information (as needed) to edit the existing ping test:

Description	If necessary, modify the description for the ping test. Ensure this description is representative of the test, as this is the description displaying within the Configuration tab.
Destination IP	If necessary, modify the IP address of the target device. This is the numeric (non DNS address) destination for the device transmitted the ping packets.
No. of Probes	If necessary, modify the number of packets transmitted to the target IP address to discern the round trip time between the switch and its connected device.
Timeout(sec)	If necessary, modify the timeout value (in seconds) used to timeout the ping test if a round trip packet is not received by the switch from its target device. Ensure this interval is long enough to account for network congestion between the switch and its target device.
Frequency	If necessary, modify the interval (in seconds) between ping packet transmissions. Define a longer interval if high levels of network congestion are anticipated between the switch and its target device. Use a value of 0 to execute a single ping or stop a currently executing ping test.

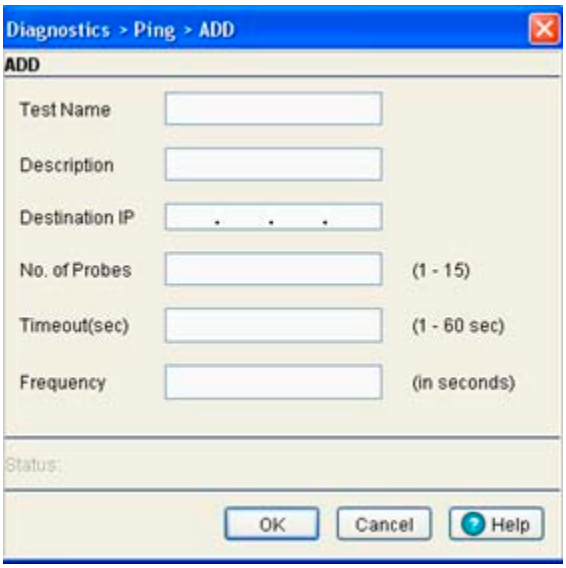
4. Click **OK** to save and add the changes to the running configuration and close the dialog.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **Cancel** to return back to the Configuration tab without implementing changes.

8.6.2 Adding a New Ping Test

If the attributes of an existing ping test do not satisfy the requirements of a new connection test, and you do not want to modify an existing test, a new test can be created and added to the list of existing ping tests displayed within the Configuration tab.

To create a new ping test and add it to the list of existing tests:

1. Select **Diagnostics** > **Ping** from the main menu.
2. Click the **Add** button at the bottom of the Configuration tab.



3. Enter the following information to define the properties of the new ping test:

Test Name	Enter a short name for the ping test to describe either the target destination of the ping packet or the ping test's expected result. Use the name provided in combination with the ping test description to convey the overall function of the test.
Description	Ensure the description is representative of the test, as this is the description displaying within the Configuration tab.
Destination IP	Enter the IP address of the target device. This is the numeric (non DNS address) destination for the device transmitted the ping packets.
No. of Probes	Define the number of ping packets transmitted to the target device. This value represents the number of packets transmitted to the target IP address to discern the round trip time between the switch and its connected device.
Timeout(sec)	Configure the timeout value (in seconds) used to timeout the ping test if a round trip packet is not received from the target device. Ensure this interval is long enough to account for network congestion between the switch and its target device.
Frequency	Define the interval (in seconds) between ping packet transmissions. Define a longer interval if high levels of network congestion are anticipated between the switch and its target device. Use a value of 0 to execute a single ping test or stop a currently running ping test.

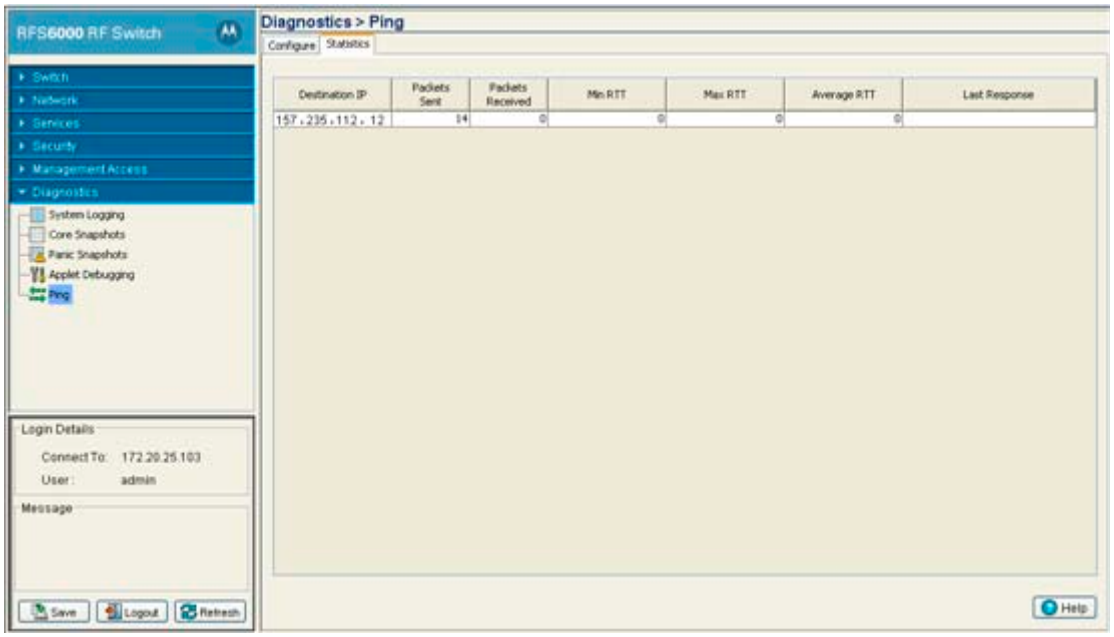
4. Click **OK** to save and add the changes to the running configuration and close the dialog.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch
6. Click **Cancel** to return back to the Configuration tab without implementing changes.

8.6.3 Viewing Ping Statistics

Refer to the Statistics tab for an overview of the overall success of the ping test with the destination IP addresses displayed within the screen. Use this information to determine whether the destination IP represents a device offering the switch a viable connection to either extend the switch's existing radio coverage area or provide support for additional MUs within an existing network segment.

To view ping test statistics:

1. Select **Diagnostics** > **Ping** from the main menu.
2. Select the **Statistics** tab.



3. Refer to the following content within the Statistics tab to assess the connection with the target device:

Destination IP	Displays the numeric (non DNS address) destination for the device transmitted the ping packets.
Packets Sent	Displays the number of packets transmitted to the target device IP address. Compare this value with the number of packets received to assess the connection quality with the target device.
Packets Received	Displays the number of packets received from the target device. If this number is significantly lower than the number sent to the target device, consider removing this device from consideration for permanent connection with the switch.
Min RTT	Displays the quickest round trip time for ping packets transmitted from the switch to its destination IP address. This may reflect the time when data traffic was at its lowest for the two devices.
Max RTT	Displays the longest round trip time for ping packets transmitted from the switch to its destination IP address. This may reflect the time when data traffic was at its most congested for the two devices.

Average RTT	Displays the average round trip time for ping packets transmitted between the switch and its destination IP address. Use this value as a general baseline (along with packets sent vs packets received) for the overall connection and association potential between the switch and target device.
Last Response	Displays the time (in seconds) the switch last "heard" the destination IP address over the switch managed network. Use this time (in contention with the RTT values displayed) to determine whether this device warrants a permanent switch connection.

Appendix A
Customer Support

Motorola's Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility support for your region. Contact information is available by visiting http://www.motorola.com/customersupport and after selecting your region, click on the appropriate link under Support for Business.

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

Customer Support Web Site

Motorola's 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.

Appendix B Adaptive AP

B.1 Adaptive AP Overview

An *adaptive AP* (AAP) is an Access Point that can adopt like an AP300 (Layer 3). The management of an AAP is conducted by the switch, once the Access Point connects to a Motorola RFS6000 or RFS7000 model switch and receives its AAP configuration.

An AAP provides:

- *local 802.11 traffic termination*
- *local encryption/decryption*
- *local traffic bridging*
- *the tunneling of centralized traffic to the wireless switch*

An AAP's switch connection can be secured using IP/UDP or IPSec depending on whether a secure WAN link from a remote site to the central site already exists.

The switch can be discovered using one of the following mechanisms:

- *DHCP*
- *Switch fully qualified domain name (FQDN)*
- *Static IP addresses*

The benefits of an AAP deployment include:

- *Centralized Configuration Management & Compliance* - Wireless configurations across distributed sites can be centrally managed by the wireless switch or cluster.
- *WAN Survivability* - Local WLAN services at a remote sites are unaffected in the case of a WAN outage.
- *Securely extend corporate WLAN's to stores for corporate visitors* - Small home or office deployments can utilize the feature set of a corporate WLAN from their remote location.
- *Maintain local WLAN's for in store applications* - WLANs created and supported locally can be concurrently supported with your existing infrastructure.

B.1.1 Where to Go From Here

Refer to the following for a further understanding of AAP operation:

- *Adaptive AP Management*
- *Types of Adaptive APs*

- *Licensing*
- *Switch Discovery*
- *Securing a Configuration Channel Between Switch and AP*
- *Adaptive AP WLAN Topology*
- *Configuration Updates*
- *Securing Data Tunnels between the Switch and AAP*
- *Adaptive AP Switch Failure*
- *Remote Site Survivability (RSS)*
- *Adaptive Mesh Support*

For an understanding of how AAP support should be configured for the Access Point and its connected switch, see *How the AP Receives its Adaptive Configuration*.

For an overview of how to configure both the Access Point and switch for basic AAP connectivity and operation, see *Establishing Basic Adaptive AP Connectivity*.

B.1.2 Adaptive AP Management

An AAP can be adopted, configured and managed like a thin Access Port from the wireless switch.

NOTE To support AAP functionality, a switch must be running firmware version the appropriate firmware version as follows:

- *RFS6000: Versions 1.0 and higher*
- *RFS7000 Versions 1.1 and higher*

NOTE: An AAP cannot support a firmware download from the wireless switch.

NOTE: Configuration changes made on the AP-5131or AP-7131 will not be updated on the switch. To change the AAP configuration for the AP-5131and AP-7131 make the changes using the switch's interface.

Once an Access Point connects to a switch and receives its AAP configuration, its WLAN and radio configuration is similar to a thin Access Port. An AAP's radio mesh configuration can also be configured from the switch. However, non-wireless features (DHCP, NAT, Firewall etc.) cannot be configured from the switch and must be defined using the Access Point's resident interfaces before its conversion to an AAP.

B.1.3 Types of Adaptive APs

Two low priced AP-5131 SKU configurations are being introduced allowing customers to take advantage of the adaptive AP architecture and to reduce deployment costs.

These dependent mode AP configurations are a software variant of the AP-5131 and will be functional only after the Access Point is adopted by a wireless switch. After adoption, the dependent mode AP receives its configuration from the switch and starts functioning like other adaptive Access Points. For ongoing operation, the dependent mode AP-5131 needs to maintain connectivity with the switch. If switch connectivity is lost, the dependent mode AP-5131 continues operating as a stand-alone Access Point for a period of 3 days before resetting and executing the switch discovery algorithm again.

A dependent mode AP cannot be converted into a standalone AP-5131 through a firmware change. Refer to the *AP-5131 Hardware/ Software Compatibility Matrix* within the release notes bundled with the Access Point firmware.

AP-5131-13040-D-WR	Dependent AP-5131 Dual Radio (Switch Required)
AP-5131-40020-D-WR	Dependent AP-5131 Single Radio (Switch Required)

B.1.4 Licensing

An AAP uses the same licensing scheme as a thin Access Port. This implies an existing license purchased with a switch can be used for an AAP deployment. Regardless of how many AP300 and/or AAPs are deployed, you must ensure the license used by the switch supports the number of radio ports (both AP300s and AAPs) you intend to adopt.

B.1.5 Switch Discovery

For an AP-5131 to function as an AAP (regardless of mode), it needs to connect to a switch to receive its configuration. There are two methods of switch discovery:

- *Auto Discovery using DHCP*
- *Manual Adoption Configuration*

NOTE: To support switch discovery, a switch must be running firmware version 3.1 or higher. An AP-51xx Access Point must running firmware version 2.0 or higher.

B.1.5.1 Auto Discovery using DHCP

Extended Global Options 189, 190, 191, 192 can be used or Embedded Option 43 - Vendor Specific options can be embedded in Option 43 using the vendor class identifier: MotorolaAP.51xx-V2-0-0.

	Code	***Data Type***
List of Switch IP addresses *(separate by comma, semi-colon, or space delimited)*	189	String
Switch FQDN	190	String
AP-51XX Encryption IPSec Passphrase (Hashed)**	191	String
AP-51XX switch discovery mode 1 = auto discovery enable 2 = auto discover enabled (using IPSec)	192	String

** The AP-5131 uses an encryption key to hash passphrases and security keys. To obtain the encryption passphrase, configure an AP-5131 with the passphrase and export the configuration file.

```
enc-admin-passwd d2
/
// System Configuration
/
system
set name AP-51xx
set loc \0
set email \0
set cc us
/
system
aap-setup
// Adaptive AP menu
set auto-discovery disable
set interface lan1
set name \0
set port 24576
delete all
set enc-passphrase bf0819993a702c39
set ac-keepalive 5
set tunnel-to-switch enable
/
// System-Access menu
system
access
set applet lan 1 enable
set applet slan 1 enable
set cli lan 1 enable
set ssh lan 1 enable
set snmp lan 1 enable
```

Encrypted Passphrase to be used in DHCP Option

B.1.5.2 Manual Adoption Configuration

A manual switch adoption of an AAP can be conducted using:

- *Static FQDN* - A switch fully qualified domain name can be specified to perform a DNS lookup and switch discovery.
- *Static IP addresses* - Up to 12 switch IP addresses can be manually specified in an ordered list the AP can choose from. When providing a list, the AAP tries to adopt based on the order in which they are listed (from 1-12).

NOTE: For a review of some important considerations impacting the use of extended and independent WLANs within an AAP deployment, see *Adaptive AP Deployment Considerations*.

The WAN has no PoE support and has a default static AP address of 10.1.1.1/8.

B.1.6 Securing a Configuration Channel Between Switch and AP

Once an Access Point obtains a list of available switches, it begins connecting to each. The switch can be either on the LAN or WAN side of the Access Point to provide flexibility in the deployment of the network. If the switch is on the Access Point's LAN, ensure the LAN subnet is on a secure channel. The AP will connect to the switch and request a configuration.

B.1.7 Adaptive AP WLAN Topology

An AAP can be deployed in the following WLAN topologies:

- *Extended WLANs* - Extended WLANs are centralized WLANs created on the switch

- *Independent WLANs* - Independent WLANs are local to an AAP and can be configured from the switch. You must specify a WLAN as independent to stop traffic from being forwarded to the switch. Independent WLANs behave like WLANs on a standalone Access Point.
- *Both* - Extended and independent WLANs are configured from the switch and operate simultaneously.

NOTE: For a review of some important considerations impacting the use of extended and independent WLANs within an AAP deployment, see *Adaptive AP Deployment Considerations*.

B.1.8 Configuration Updates

An AAP receives its configuration from the switch initially as part of its adoption sequence. Subsequent configuration changes on the switch are reflected on an AAP when applicable.

An AAP applies the configuration changes it receives from the switch after 30 seconds from the last received switch configuration message. When the configuration is applied on the AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds) forcing associated MUs to be deauthenticated. MUs are quickly able to associate.

NOTE: When using a dependant mode AP, be aware that any configuration changes made directly on the AP will be overwritten once the AP is adopted by the switch and the configuration file from the switch is received.

B.1.9 Securing Data Tunnels between the Switch and AAP

If a secure link (site-to-site VPN) from a remote site to the central location already exists, the AAP does not require IPSec be configured for adoption.

For sites with no secure link to the central location, an AAP can be configured to use an IPSec tunnel (with AES 256 encryption) for adoption. The tunnel configuration is automatic on the AAP side and requires no manual VPN policy be configured. On the switch side, configuration updates are required to adopt the AAP using an IPSec tunnel.

To review a sample AAP configuration, see *Sample Switch Configuration File for IPSec and Independent WLAN*.

B.1.10 Adaptive AP Switch Failure

In the event of a switch failure, an AAP's independent WLAN continues to operate without disruption. The AAP attempts to connect to other switches (if available) in background. Extended WLANs are disabled once switch adoption is lost. When a new switch is discovered and a connection is secured, an extended WLAN can be enabled.

If a new switch is located, the AAP synchronizes its configuration with the located switch once adopted. If *Remote Site Survivability* (RSS) is disabled, the independent WLAN is also disabled in the event of a switch failure.

B.1.11 Remote Site Survivability (RSS)

RSS can be used to turn off RF activity on an AAP if it loses adoption (connection) to the switch.

RSS State	Independent WLANs	Extended WLANs

RSS Enabled	WLAN continues beaconing	WLAN continues beaconing but AP does allow clients to associate on that WLAN
RSS Disabled	WLAN stops beaconing	WLAN stops beaconing

NOTE: For a dependant AAP, independent WLANs continue to beacon for three days in the absence of a switch.

B.1.12 Adaptive Mesh Support

An AAP can extend an AP51x1's existing mesh functionality to a switch managed network. All mesh APs are configured and managed through the wireless switch. APs without a wired connection form a mesh backhaul to a repeater or a wired mesh node and then get adopted to the switch. Mesh nodes with existing wired access get adopted to the switch like a wired AAP.

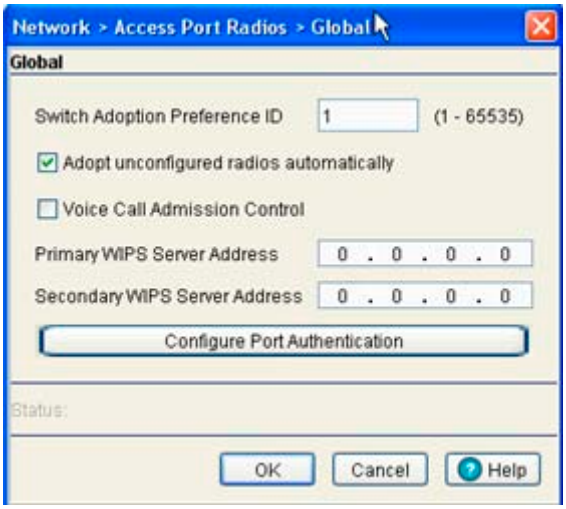
Mesh AAPs apply configuration changes 180 seconds after the last received switch configuration message. When the configuration is applied on the Mesh AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds), forcing associated MUs to be deauthenticated and the Mesh link will go down. MUs are able to quickly associate, but the Mesh link will need to be re-established before MUs can pass traffic. This typically takes about 90 to 180 seconds depending on the size of the mesh topology.

NOTE: When mesh is used with AAPs, the "ap-timeout" value needs to be set to a higher value (for example, 180 seconds) so Mesh AAPs remain adopted to the switch during the period when the configuration is applied and mesh links are re-established.

B.1.12.1 Configuring Adaptive AP Mesh

To configure mesh support for Adaptive AP:

1. Go to **Network** > **Access Port Radios** and click on the *Global Settings* button.



2. Uncheck the **Adopt Unconfigured Radios Automatically** option to prevent the switch from automatically adopting new APs when they are connected to the switch.
3. Configure the client bridge back haul WLAN, base bridge and client bridge radios on the switch using the Command Line Interface (CLI) commands listed below.

```
Client Bridge Back Haul WLAN Configuration:
RFS7000(config-wireless)#wlan 1 enable
RFS7000(config-wireless)#wlan 1 ssid meshWlan
RFS7000(config-wireless)#wlan 1 independent
RFS7000(config-wireless)#wlan 1 client-bridge-backhaul enable

Base Bridge Radio Configuration: (AP5131 that is wired to the switch)
RFS7000(config-wireless)#radio add 1 “base bridge radio mac” 11bg aap51x1
RFS7000(config-wireless)#radio add 2 “base bridge radio mac” 11a aap51x1
RFS7000(config-wireless)#radio 1 base-bridge enable
RFS7000(config-wireless)#radio 1 bss 1 1
(map the mesh WLAN if manual mapping is enabled, not needed otherwise)

Client Bridge Radios Configuration: (AP51x1’s that are wirelessly
connected)
RFS7000(config-wireless)#radio add 3 “client bridge radio mac” 11bg
aap51x1
RFS7000(config-wireless)#radio add 4 “client bridge radio mac” 11a aap51x1
RFS7000(config-wireless)#radio 3 client-bridge enable
RFS7000(config-wireless)#radio 3 client-bridge ssid meshWlan
RFS7000(config-wireless)#radio 3 bss 1 1
(map the mesh WLAN if manual mapping is enabled, not needed otherwise)
```

4. Configure Adaptive AP support on the AP-5131 or AP-7131 by adopting the AP’s base bridge as well as client bridge. The client-bridge radios must be directly wired to the switch during this configuration step.
5. Once all AP5131 APs are adopted, wait for 3 minutes. After 3 minutes disconnect the client-bridge AP5131s from the network. The client bridge AP5131s will continue to be adopted.

B.1.13 AAP Radius Proxy Support

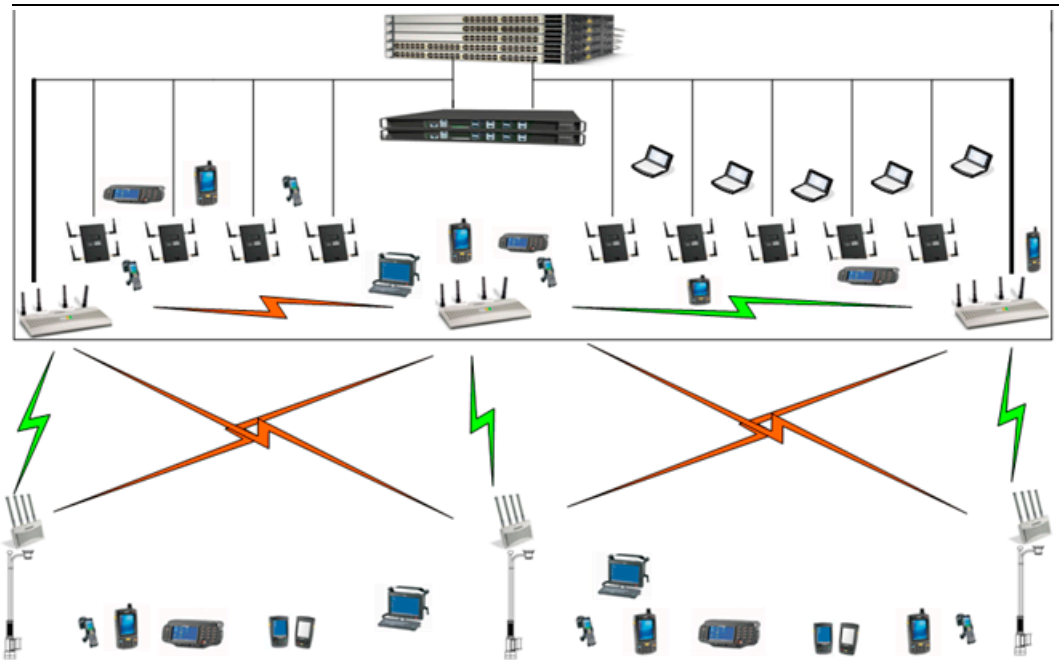
When an Adaptive AP is adopted to a central switch over a WAN Link, the switch configures the Adaptive AP for a WLAN with Radius authentication from a Radius server residing at the central site. When the Adaptive AP gets a Radius MU associated, it sends the Radius packets on the wired side with its own IP Address as the source IPof the request and the Destination IP Address of the Radius Server. In a local network implementation, the Adaptive APs, switch and Radius Servers are all on the same LAN and the routing works fine. However, when the Adaptive AP is adopted over a WAN link, the Radius Server IP Address will be an internal address which is non-routable I over the Internet.

To access the Radius server’s non-routable IP address over the WAN, you have the option to configure Adaptive AP Radius Proxying for the WLAN. When this flag is enabled, the Adaptive AP is reconfigured to send all radius traffic to the switch and the switch does the proxying to the real Radius server to handle authentication. The switch automates the process of handling Radius proxy configuration and client configurations. The switch supports only one real radius server configuration without the presence of realm information. To support multiple radius servers, a realm has to be associated with the real Radius server.

When AAP radius proxying is enabled without specifying a realm, the switch can no longer process requests on the on-board radius server. You cannot authenticate using the on-board Radius server any longer because all authentications done by users without a realm are forwarded to the external radius server, as configured for the WLAN with Adaptive AP Radius Proxy.

NOTE: The Motorola RF Series Wireless Switches support Adaptive AP Radius proxy without specifying realm information. If AAP Proxy Radius is enabled without specifying realm information, the onboard Radius server can no longer be used to authenticate users. If AAP Proxy Radius is enabled for a WLAN with realm configured, then the onboard Radius server can perform as usual.

NOTE: If AAP Proxy Radius is configured, the onboard Radius server has to be enabled. By default the onboard Radius server is disabled. To enable the onboard Radius server use the Web UI or issue the "service radius" command in the CLI.



B.2 Supported Adaptive AP Topologies

The following AAP topologies are supported:

- *Extended WLANs Only*
- *Independent WLANs Only*
- *Extended WLANs with Independent WLANs*
- *Extended VLAN with Mesh Networking*

B.2.1 Topology Deployment Considerations

When reviewing the AAP topologies describes in the section, be cognizant of the following considerations to optimize the effectiveness of the deployment:

- An AAP firmware upgrade will not be performed at the time of adoption from the wireless switch. Instead, the firmware is upgraded using the AP-51x1's firmware update procedure (manually or using the DHCP Auto Update feature).
- An AAP can use its LAN1 interface or WAN interface for adoption. The default gateway interface is set to LAN1. If the WAN Interface is used, explicitly configure WAN as the default gateway interface.
- Motorola recommends using the LAN1 interface for adoption in multi-cell deployments.
- If you have multiple independent WLANs mapped to different VLANs, the AAP's LAN1 interface requires trunking be enabled with the correct management and native VLAN IDs configured. Additionally, the AAP needs to be connected to a 802.1q trunk port on the wired switch.
- Be aware IPSec Mode supports NAT Traversal (NAT-T).

B.2.2 Extended WLANs Only

An extended WLAN configuration forces all MU traffic through the switch. No wireless traffic is locally bridged by the AAP.

Each extended WLAN is mapped to the Access Point's virtual LAN2 subnet. By default, the Access Point's LAN2 is not enabled and the default configuration is set to static with IP addresses defined as all zeros. If the extended VLAN option is configured on the switch, the following configuration updates are made automatically:

- The AAP's LAN2 subnet becomes enabled
- All extended VLANs are mapped to LAN2.

NOTE: MUs on the same WLAN associated to the AAP can communicate locally at the AP Level without going through the switch. If this scenario is undesirable, the Access Point's MU-to-MU disallow option should be enabled.

B.2.3 Independent WLANs Only

An independent WLAN configuration forces all MU traffic be bridged locally by the AAP. No wireless traffic is tunneled back to the switch. Each extended WLAN is mapped to the Access Point's LAN1 interface. The only traffic between the switch and the AAP are control messages (for example, heartbeats, statistics and configuration updates).

B.2.4 Extended WLANs with Independent WLANs

An AAP can have both extended WLANs and independent WLANs operating in conjunction. When used together, MU traffic from extended WLANs go back to the switch and traffic from independent WLANs is bridged locally by the AP.

All local WLANs are mapped to LAN1, and all extended WLANs are mapped to LAN2.

B.2.5 Extended VLAN with Mesh Networking

Mesh networking is an extension of the existing wired network. There is no special configuration required, with the exception of setting the mesh and using it within one of the two extended VLAN configurations.

NOTE: The mesh backhaul WLAN must be an independent WLAN mapped to LAN2. The switch enforces the WLAN be defined as an independent WLAN by automatically setting the WLAN to independent when backhaul is selected. The AP ensures the backhaul WLAN be put on LAN1.

B.3 How the AP Receives its Adaptive Configuration

An AAP does not require a separate "local" or "running" configuration. Once enabled as an AAP, the AP obtains its configuration from the switch. If the AP's WAN link fails, it continues to operate using the last valid configuration until its link is re-established and a new configuration is pushed down from the switch. There is no separate file-based configuration stored on the switch.

Only WLAN, VLAN extension and radio configuration items are defined for the AAP by its connected switch. None of the other Access Point configuration items (RADIUS, DHCP, NAT, Firewall etc.) are configurable from the connected switch.

After the AP downloads a configuration file from the switch, it obtains the version number of the image it should be running. The switch does not have the capacity to hold the Access Point's firmware image and configuration. The Access Point image must be downloaded using a means outside the switch. If there is still an image version mismatch between what the switch expects and what the AAP is running, the switch will deny adoption.

NOTE: When configuring wireless settings for Adaptive APs all configuration must be done through the switch and not from the AP management console. Making changes directly in the AP management console can lead to unstable operation of the Adaptive AP.

B.3.1 Adaptive AP Pre-requisites

Converting an AP-5131 or AP-7131 model Access Point into an AAP requires:

- Version 2.0 or higher firmware running on the Access Point.
- A Motorola RF Swtich running firmware version 3.1 or later.
- The appropriate switch licenses providing AAP functionality on the switch.
- The correct password to authenticate and connect the adaptive to the switch.

B.3.2 Configuring the Adaptive AP for Adoption by the Switch

To configure an AAP for switch adoption:

1. An AAP needs to find and connect to the switch. To ensure this connection:
   - Configure the switch's IP address on the AAP
   - Provide the switch IP address using DHCP option 189 on a DHCP server. The IP address is a comma delimited string of IP addresses. For example "157.235.94.91, 10.10.10.19". There can be a maximum of 12 IP addresses.
   - Configure the switch's FQDN on the AAP. The AAP can use this to resolve the IP address of the switch.
2. Use the switch's secret password on the AAP for the switch to authenticate it.

   To avoid a lengthy broken connection with the switch, Motorola recommends generating an SNMP trap when the AAP loses adoption with the switch.

NOTE: For additional information (in greater detail) on the AP configuration activities described above, see *Adaptive AP Configuration on page B-11*.

B.3.3 Configuring the Switch for Adaptive AP Adoption

The tasks described below are configured on a Motorola RF switch. For information on configuring the switch for AAP support, see *http://www.motorola.com/customersupport.*

To adopt an AAP on a switch:

1. Ensure enough licenses are available on the switch to adopt the required number of AAPs.
2. As soon as the AAP displays in the adopted list:

   Adjust each AAP's radio configuration as required. This includes WLAN-radio mappings and radio parameters. WLAN-VLAN mappings and WLAN parameters are global and cannot be defined on a per

radio basis. WLANs can be assigned to a radio as done today for an AP300 model Access Port. Optionally, configure WLANs as independent and assign to AAPs as needed.

3. Configure each VPN tunnel with the VLANs to be extended to it.

   If you do not attach the target VLAN, no data will be forwarded to the AAP, only control traffic required to adopt and configure the AP.

NOTE: For additional information (in greater detail) on the switch configuration activities described above, see *Switch Configuration*.

B.4 Establishing Basic Adaptive AP Connectivity

This section defines the activities required to configure basic AAP connectivity with the switch. In establishing a basic AAP connection, both the Access Point and switch require modifications to their respective default configurations. For more information, see:

- *Adaptive AP Configuration*
- *Switch Configuration*

NOTE: Refer to *Adaptive AP Deployment Considerations* for usage and deployment caveats that should be considered before defining the AAP configuration. Refer to *Sample Switch Configuration File for IPSec and Independent WLAN* if planning to deploy an AAP configuration using IPSec VPN and an extended WLAN

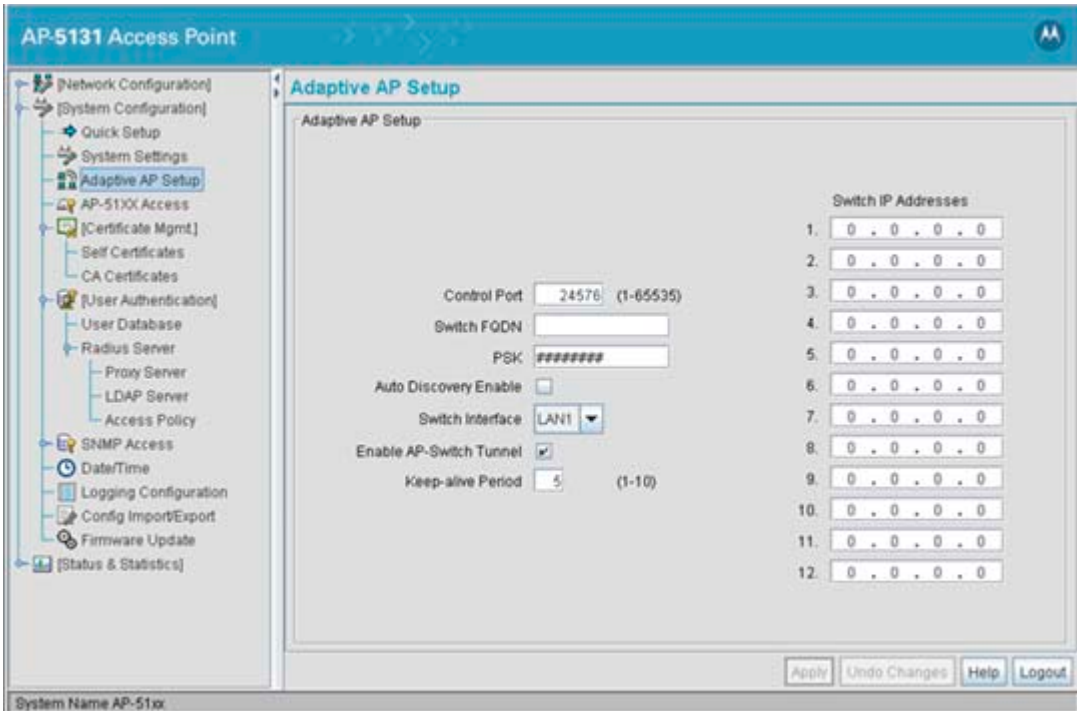
B.4.1 Adaptive AP Configuration

An AAP can be manually adopted by the switch, adopted using a configuration file (consisting of the adaptive parameters) pushed to the Access Point or adopted using DHCP options. Each of these adoption techniques is described in the sections that follow.

B.4.1.1 Adopting an Adaptive AP Manually

To manually enable the Access Point's switch discovery method and connection medium required for adoption:

1. Select **System Configuration** -> **Adaptive AP Setup** from the Access Point's menu tree.



2. Select the **Auto Discovery Enable** checkbox.

   Enabling auto discovery will allow the AAP to be detected by a switch once its connectivity medium has been configured (by completing steps 3-6).

NOTE: Auto discovery must be enabled for a switch to detect an AP.

3. Enter up to 12 **Switch IP Addresses** constituting the target switches available for AAP connection.

   The AAP will begin establishing a connection with the first addresses in the list. If unsuccessful, the AP will continue down the list (in order) until a connection is established.

4. If a numerical IP address is unknown, but you know a switch's *fully qualified domain name* (FQDN), enter the name as the **Switch FQDN** value.
5. Select the **Enable AP-Switch Tunnel** option to allow AAP configuration data to reach a switch using a secure VPN tunnel.
6. If using IPSec as the tunnel resource, enter the IPSec **Passkey** to ensure IPSec connectivity.
7. Click **Apply** to save the changes to the AAP setup.

NOTE: The manual AAP adoption described above can also be conducted using the Access Point's CLI interface using the *admin(system.aapsetup)>* command.

B.4.1.2 Adopting an Adaptive AP Using a Configuration File

To adopt an AAP using a configuration file:

1. Refer to *Adopting an Adaptive AP Manually* and define the AAP switch connection parameters.

2. Export the AAP's configuration to a secure location.

   Either import the configuration manually to other APs or the same AP later (if you elect to default its configuration). Use DHCP option 186 and 187 to force a download of the configuration file during startup (when it receives a DHCP offer).

NOTE: When an Adaptive AP is adopted over an IP Sec Tunnel you cannot export the configuration file to a system on the other side of the IP Sec Tunnel. You may still export the conifguration file to a system local to the AAP.

B.4.1.3 Adopting an Adaptive AP Using DHCP Options

An AAP can be adopted to a wireless switch by providing the following options in the DHCP Offer:

Option	*Data Type*	*Value*
189	String	<Switch IP Address or Range of IP addresses separated by [, ; <space>]>
190	String	<Fully qualified Domain Name for the Wireless Switch>
191	String	<Hashed IPSec Passkey - configure on 1 AP and export to get hashed key>
192	String	<Value of "1" denotes Non-IPSec Mode and "2" denotes IPSec Mode>

NOTE: Options 189 and 192 are mandatory to trigger adoption using DHCP options. Unlike an AP300, option 189 alone won't work. These options can be embedded in Vendor Specific Option 43 and sent in the DHCP Offer.

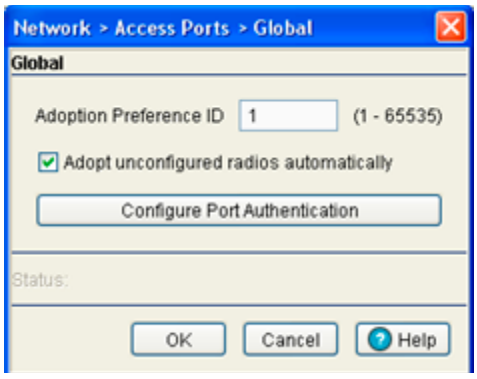
B.4.2 Switch Configuration

A Motorola RF Switch (running firmware version 3.1 or later) requires an explicit adaptive configuration to adopt an Access Point (if IPSec is not being used for adoption). The same licenses currently used for AP300 adoption can be used for an AAP.

Disable the switch's **Adopt unconfigured radios automatically** option and manually add AAPs requiring adoption, or leave as default. In default mode, any AAP adoption request is honored until the current switch license limit is reached.

To disable automatic adoption on the switch:

1. Select **Network** > **Access Port Radios** from the switch main menu tree.
2. Select the **Configuration** tab (should be displayed be default) and click the **Global Settings** button.



3. Ensure the **Adopt unconfigured radios automatically** option is NOT selected.

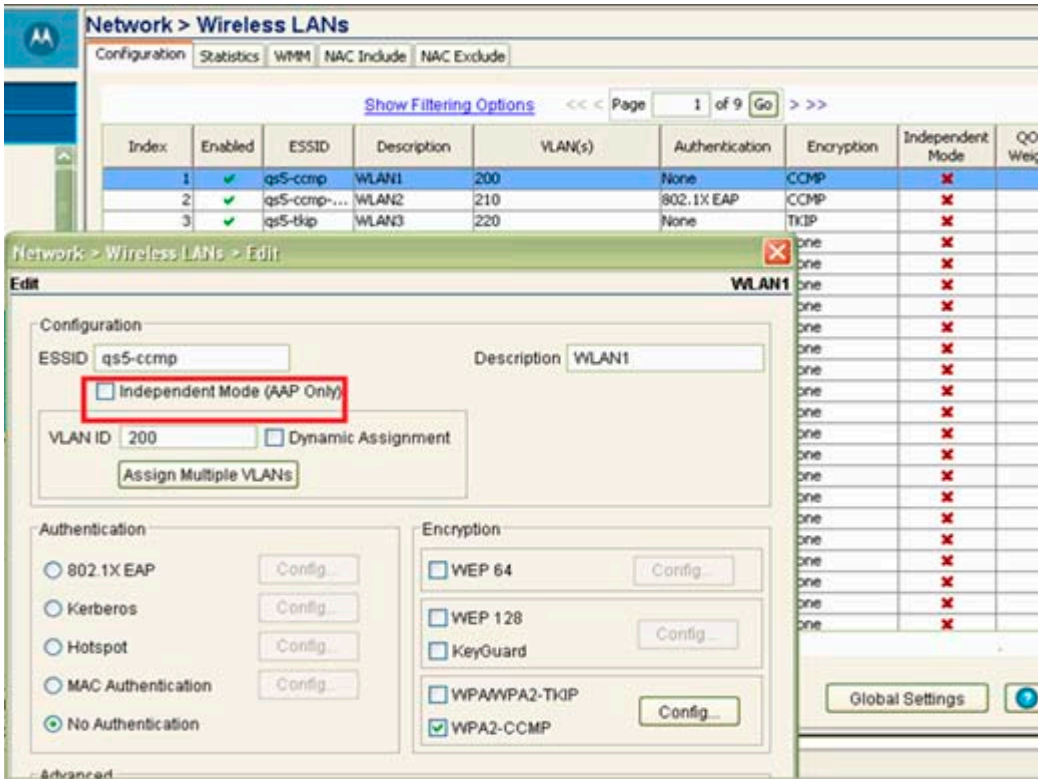
   When disabled, there is no automatic adoption of non-configured radios on the network. Additionally, default radio settings will NOT be applied to Access Ports when automatically adopted.

NOTE: For IPSec deployments, refer to *Sample Switch Configuration File for IPSec and Independent WLAN* and take note of the CLI commands in red and associated comments in green.

Any WLAN configured on the switch becomes an extended WLAN by default for an AAP.

4. Select **Network** > **Wireless LANs** from the switch main menu tree.
5. Select the target WLAN you would like to use for AAP support from those displayed and click the **Edit** button.
6. Select the **Independent Mode (AAP Only)** checkbox.

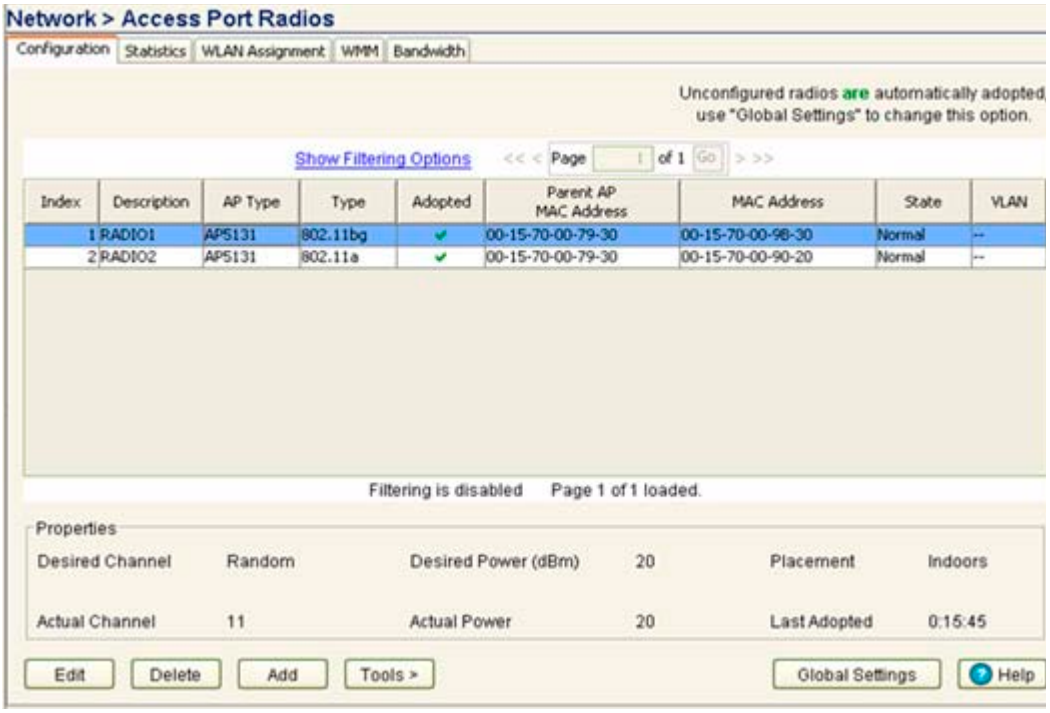
   Selecting the checkbox designates the WLAN as independent and prevents traffic from being forwarded to the switch. Independent WLANs behave like WLANs as used on a a standalone Access Point. Leave this option unselected (as is by default) to keep this WLAN an extended WLAN (a typical centralized WLAN created on the switch).



NOTE: Additionally, a WLAN can be defined as independent using the "*wlan <index> independent*" command from the config-wireless context.

NOTE: For AAP to work properly with RFS7000, you need to have independent and extended WLANs mapped to a different VLAN than the ge port.

Once an AAP is adopted by the switch, it displays within the switch **Access Port Radios** screen (under the Network parent menu item) as an AP-5131, AP-5181 or AP-7131 within the **AP Type** column.



B.4.3 Adaptive AP Deployment Considerations

Before deploying your switch/AAP configuration, refer to the following usage caveats to optimize its effectiveness:

- Extended WLANs are mapped to the AP's LAN2 interface and all independent WLANs are mapped to the AP's LAN1 Interface.
- If deploying multiple independent WLANs mapped to different VLANs, ensure the AP's LAN1 interface is connected to a trunk port on the Layer 2/Layer 3 switch and appropriate management and native VLANs are configured.
- The WLAN used for mesh backhaul must always be an independent WLAN.
- The switch configures an AAP. If manually changing wireless settings on the AP, they are not updated on the switch. It's a one way configuration, from the switch to the AP.
- An AAP always requires a router between the AP and the switch.
- An AAP can be used behind a NAT.
- An AAP uses UDP port 24576 for control frames and UDP port 24577 for data frames.
- Multiple VLANs per WLAN, Layer 3 mobility, dynamic VLAN assignment, NAC, self healing, rogue AP, MU locationing, hotspot on extended WLAN are some of the important wireless features not supported in an AAP supported deployment.

B.4.4 Sample Switch Configuration File for IPSec and Independent WLAN

The following constitutes a sample switch configuration file supporting an AAP IPSec with Independent WLAN configuration. Please note new AAP specific CLI commands in red and relevant comments in blue.

The sample output is as follows:

```
!
! configuration of RFS6000
!
!
aaa authentication login default none
service prompt crash-info
!
hostname RFS6000-1
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
To configure the ACL to be used in the CRYPTO MAP
!
ip access-list extended AAP-ACL permit ip host 10.10.10.250 any rule-precedence
20
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst config
name My Name
!
country-code us
logging buffered 4
logging console 7
logging host 157.235.92.97
logging syslog 7
snmp-server sysname RFS6000-1
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5
0x49c451c7c6893ffcede0491bbd0a12c4
!
To configure the passkey for a Remote VPN Peer - 255.255.255.255 denotes all
AAPs. 12345678 is the default passkey. If you change on the AAP, change here as
well.
!
crypto isakmp key 0 12345678 address 255.255.255.255
!
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
no service pm sys-restart
timezone America/Los_Angeles
license AP
xyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxyxy
```

```
xyxyxyxxyxyxyx
!
wireless
no adopt-unconf-radio enable
manual-wlan-mapping enable
wlan 1 enable
wlan 1 ssid qs5-ccmp
wlan 1 vlan 200
wlan 1 encryption-type ccmp
wlan 1 dot11i phrase 0 Symbol123
wlan 2 enable
wlan 2 ssid qs5-tkip
wlan 2 vlan 210
wlan 2 encryption-type tkip
wlan 2 dot11i phrase 0 Symbol123
wlan 3 enable
wlan 3 ssid qs5-wep128
wlan 3 vlan 220
wlan 3 encryption-type wep128
wlan 4 enable
wlan 4 ssid qs5-open
wlan 4 vlan 230
wlan 5 enable
wlan 5 ssid Mesh
wlan 5 vlan 111
wlan 5 encryption-type ccmp
wlan 5 dot11i phrase 0 Symbol123
!
To configure a WLAN as an independent WLAN
!
wlan 5 independent
wlan 5 client-bridge-backhaul enable
wlan 6 enable
wlan 6 ssid test-mesh
wlan 6 vlan 250
radio add 1 00-15-70-00-79-30 11bg aap5131
radio 1 bss 1 3
radio 1 bss 2 4
radio 1 bss 3 2
radio 1 channel-power indoor 11 8
radio 1 rss enable
radio add 2 00-15-70-00-79-30 11a aap5131
radio 2 bss 1 5
radio 2 bss 2 1
radio 2 bss 3 2
radio 2 channel-power indoor 48 8
radio 2 rss enable
radio 2 base-bridge max-clients 12
radio 2 base-bridge enable
radio add 3 00-15-70-00-79-12 11bg aap5131
radio 3 bss 1 3
radio 3 bss 2 4
radio 3 bss 3 2
radio 3 channel-power indoor 6 8
radio 3 rss enable
radio add 4 00-15-70-00-79-12 11a aap5131
radio 4 bss 1 5
radio 4 bss 2 6
```

```
radio 4 channel-power indoor 48 4
radio 4 rss enable
radio 4 client-bridge bridge-select-mode auto
radio 4 client-bridge ssid Mesh
radio 4 client-bridge mesh-timeout 0
radio 4 client-bridge enable
radio default-11a rss enable
radio default-11bg rss enable
radio default-11b rss enable
no ap-ip default-ap switch-ip
!
radius-server local
!
To create an IPSEC Transform Set
!
crypto ipsec transform-set AAP-TFSET esp-aes-256 esp-sha-hmac mode tunnel
!
To create a Crypto Map, add a remote peer, set the mode, add a ACL rule to match
and transform and set to the Crypto Map
!
crypto map AAP-CRYPTOMAP 10 ipsec-isakmp
set peer 255.255.255.255
set mode aggressive
match address AAP-ACL
set transform-set AAP-TFSET
!
interface ge1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge2
switchport access vlan 1
!
interface ge3
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge4
switchport access vlan 1
!
interface me1
ip address dhcp
!
interface sa1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan none
switchport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
switchport trunk allowed vlan add 180,190,200,210,220,230,240,250,
!
```

```
!
!
!
interface vlan1
ip address dhcp
!
To attach a Crypto Map to a VLAN Interface
!
crypto map AAP-CRYPTOMAP
!
sole
!
ip route 157.235.0.0/16 157.235.92.2
ip route 172.0.0.0/8 157.235.92.2
!
ntp server 10.10.10.100 prefer version 3
line con 0
line vty 0 24
!
end
```

Appendix C
Troubleshooting Information

This appendix provides basic troubleshooting information and workarounds to known conditions the user may encounter. Wherever possible, it includes possible suggestions or solutions to resolve the issues. It is divided into the following section:

- *General Troubleshooting*
- *Troubleshooting SNMP Issues*
- *Security Issues*

C.1 General Troubleshooting

This section describes common system issues and what to look for while diagnosing the cause of a problem.

The following information is included:

- *Wireless Switch Issues*
- *Access Port Issues*
- *Mobile Unit Issues*
- *Miscellaneous Issues*
- *System Logging Mechanism*

C.1.1 Wireless Switch Issues

This section describes various issues that may occur when working with a Motorola RF Series Switch. Possible issues include:

- *Switch Does Not Boot Up*
- *Switch Does Not Obtain an IP Address through DHCP*
- *Unable to Connect to the Switch using Telnet or SSH*
- *Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond*
- *Console Port is Not Responding*

C.1.1.1 Switch Does Not Boot Up

The Motorola RF Series Switch does not boot up to a username prompt via CLI console or Telnet.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Switch has no power	• Verify power cables, fuses, UPS power The front panel LEDs lights up when power is applied to the switch. • Have a qualified electrician check the power source to which the switch is connected.
All else...	Contact Motorola Support.

C.1.1.2 Switch Does Not Obtain an IP Address through DHCP

A Motorola RF Series Switch requires a routable IP address for the administrator to manage it via Telnet, SSH or a Web browser.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
DHCP is not configured, or not available on same network as the Motorola RF Series Switch	• Verify the configuration for the switch has DHCP enabled. By default, the ports have DHCP enabled. Otherwise, refer to the CLI Reference Guide or System Reference Guide for instructions on enabling the switch interfaces. • Connect another host configured for DHCP and verify it is getting a DHCP address
DHCP is not enabled on a Gigabit Ethernet interface	• Enable DHCP for the port by using the CLI command or the Web UI to enable DHCP on the port connected to your external network. • Verify that DHCP packets are being sent to the port using a sniffer tool • If DHCP packets are seen, check to ensure that the switch is not configured for a static IP on the port.
All else...	Contact Motorola Support.

C.1.1.3 Unable to Connect to the Switch using Telnet or SSH

The Motorola RF Series Switch is physically connected to the network, but connecting to the switch using SSH or Telnet does not work.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Telnet is not enabled and/or SSH is disabled	Verify Telnet or SSH are enabled by using the CLI or Web UI (By default, telnet is disabled.)
Max sessions have been reached	Maximum allowed sessions is 8 concurrent users connected to a switch. Verify the threshold has not been reached.
Primary LAN is not receiving Telnet or SSH traffic	Verify Telnet and SSH traffic is allowed on the primary VLAN
All else...	Contact Motorola Support

C.1.1.4 Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond

When configuring the switch, it is easy to overlook the fact that the host computer is running the browser while the Motorola RF Series Switch is providing the data to the browser. Occasionally, while using the Web UI the switch does not respond or appears to be running very slow; this could be a symptom of the host computer or the network, and not the switch itself. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Bad connection between switch and console system	Verify the line between the switch and the host computer is functioning normally
Slow transmission of data packets	Verify the data packets are being sent to and from the switch using a sniffer tool
Access ports may try to adopt while country code is not set	Set the country name for the switch, which is set to “none” by default
Packet storm	Check Syslog for any type of a packet storm
Overburdened with a large number of Access Ports	With large numbers of Access Ports, changing the configuration quickly may cause the switch to not refresh properly, at least immediately following configuration.
Java JRE is out of date	Be sure you are using Sun Java JRE 1.5 or later. To download the appropriate for your system go to: http://www.sun.com/java/
Cannot access Web UI through a Firewall	To successfully access the switch Web UI through a firewall, UDP port 161 must be open in order for the switch’s SNMP backend to function
All else...	Contact Motorola Support

C.1.1.5 Console Port is Not Responding

The Motorola RF Series Switch console port is connected to the host computer’s serial port, but pressing the [Enter] key gets no response from the switch.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Cabling issue	Ensure a console cable is connected from the console port to the host computer’s serial port
Not using a terminal emulation program	Verify a serial terminal emulation program, such as HyperTerminal, is in use on the host computer

Possible Problem	Suggestions to Correct
Settings in terminal emulation program are incorrectly set	Check the serial port settings in the serial terminal emulation program being used. The correct settings are: Terminal Type: VT-100 Port: Any COM port Terminal Settings: 19200 bps transfer rate, 8 data bits, no parity, 1 stop bit, no flow control
All else...	Contact Motorola Support.

C.1.2 Access Port Issues

This section describes various issues related to Access Ports within theMotorola RF Series Switch network. Possible issues include:

- *Access Ports are Not Adopted*
- *Access Ports are Not Responding*

C.1.2.1 Access Ports are Not Adopted

Access ports are not being adopted. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Access port is not configured	Verify the license key that is set in the switch
Country code for switch is not set	Verify the country code is entered into the switch prior to adopting any Access Ports. The switch is not fully functional until a country code is set.
Access ports are off-network	Verify the Access Ports are connected to the network and powered on
Access ports are restricted in configuration	Verify the switch is not configured with an access control list that does not allow Access Port adoption; verify that Access Port adoption is not set to “deny”. Ensure that the Access Port adoption policy is added with a WLAN
Access Port is on Exclude List	Verify the Motorola RF Series Switch ACL adoption list does not include the Access Ports that are not being adopted.
Miscellaneous other issues	• With a packet sniffer, look for 8375 (broadcast) packets • Reset the Motorola RF Series Switch. If the switch is hung, it may begin to adopt Access Ports properly once it has been reset.
All else...	Contact Motorola Support

C.1.2.2 Access Ports are Not Responding

Access Ports are not responding. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Access Port not responding after converting to a Detector AP	When converting an AP300 to an Intrusion Detection Sensor, the conversion requires approximately 60 seconds.
All else...	Contact Motorola Support

C.1.2.3 Sensor Port frequently goes up and down

Possible Problem	Suggestions to Correct
Sensor Port flapping (going up and down)	This may be caused by the sensor being unable to find its server. Ensure that the detection configuration is correct and that all cables are secure.
All else...	Contact Motorola Support

C.1.3 Mobile Unit Issues

This section describes various issues that may occur when working with the mobile units associated with the wireless switch or associated Access Ports. Possible issues include:

- *Access Port Adopted, but MU is Not Being Associated*
- *MUs Cannot Associate and/or Authenticate with Access Ports*
- *Poor Voice Quality Issues*

C.1.3.1 Access Port Adopted, but MU is Not Being Associated

Access Port associated with an MU is not yet being adopted. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Unadopted Access Port	Verify that the switch has adopted the Access Port with which the MU is trying to associate
Incorrect ESSID applied to the MU	Verify on the MU the correct ESSID has been applied to the MU
Ethernet port configuration issues	• Verify that the Ethernet port connected to thenetwork and has a valid configuration. • If DHCP is used, verify that the Ethernet cable is connected to the same NIC upon which DHCP services are enabled
Incorrect security settings	Verify the correct security settings are applied to a WLAN in which the MU is tryng to associate
All else...	Contact Motorola Support

C.1.3.2 MUs Cannot Associate and/or Authenticate with Access Ports

MUs cannot associate and/or authenticate with Access Ports.
The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Preamble differences	Verify the preamble type matches between switch and MUs. Try a different setting.
Device key issues	Verify in Syslog there is not a high rate of decryption error messages. This could indicate a device key is incorrect.
MU is not in Adopt List	Verify the device is not in the "do not adopt ACL".
Keyguard not set on client	Verify Keyguard is set on the client if the Security/WLAN Policy calls for Keygaurd.
Encryption Problems	If Encryption is being used, verify the encryption settings on the MU and the switch match. If WEP Encryption is being used with non-Symbol or Motorola MUs, ensure the key being entered is in HEX format and not a Passphrase.
Authentication Problems	If the switch is configured to use RADIUS authentication, check the RADIUS log file for any failure information.
Encryption or Authentication Problems	If you are using Authentication and/or Encryption on the switch, and the previous troubleshooting steps have not fixed the problem, try temporarily disabling Authentication and Encryption to see if that fixes the problem.

C.1.3.3 Poor Voice Quality Issues

VOIP MUs, BroadCast MultiCast and SpectraLink phones have poor voice quality issues. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Traffic congestion with data traffic	• Maintain voice and data traffic on separate WLANs. • Use a QoS Classifier to provide dedicated bandwidth if data and voice traffic are running on the same WLAN.
Long preamble not used on Spectralink phones	Verify a long preamble is used with Spectralink phones.

C.1.4 Miscellaneous Issues

This section describes various miscellaneous issues related to the Motorola RF Series Switch which don't fall into any of the previous categories. Possible issues include:

- *Excessive Fragmented Data or Excessive Broadcast*
- *Excessive Memory Leak*

C.1.4.1 Excessive Fragmented Data or Excessive Broadcast

Excessive fragmented data or excessive broadcast.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Fragmentation	• Do not allow VoIP traffic when operating on a flat network (no routers or smart switches). • Move to a trunked Ethernet port. • Move to a different configuration.
All else...	Contact Motorola Support

C.1.4.2 Excessive Memory Leak

Excessive memory leak. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Memory leak	Using the CLI or Web UI's Diagnostics section to check the available virtual memory. If any one process displays an excessive amount of memory usage, that process could be one of the possible causes of the problem.
Too many concurrent Telnet or SSH sessions	Keep the maximum number of Telnet or SSH sessions low (6 or less), even though up to 8 sessions are allowed.
All else...	Contact Motorola Support

C.1.5 System Logging Mechanism

The Motorola RF Series Switch provides subsystem logging to a Syslog server. There are two Syslog systems, local and remote. Local Syslog records system information locally, on the switch. The remote Syslog sends messages to a remote host. All Syslog messages conform to the RFC 3164 message format.

C.2 Troubleshooting SNMP Issues

The following SNMP-releated issued could require troubleshooting as SNMP issues are experienced with the Motorola RF Series Switch.

- *MIB Browser not able to contact the agent*
- *Not able to SNMP WALK for a GET*
- *MIB not visible in the MIB browser*
- *SNMP SETs not working*
- *Not receiving SNMP traps*
- *Additional Configuration*

C.2.1 MIB Browser not able to contact the agent

General error messages on the MIB Browser: Timeout, No Response.

The client IP where the MIB browser is present should be made known to the agent. Adding SNMP clients through CLI or Web UI can do this.

C.2.2 Not able to SNMP WALK for a GET

- Check whether the MIB browser has IP connectivity to the SNMP agent on the the switch. Use IP Ping from the client system which has the MIB Browser.
- Check if the community string is the same at the agent side and the manager (MIB Browser) side. The community name is case sensitive.

C.2.3 MIB not visible in the MIB browser

The filename.mib file should be first compiled using a MIB compiler, which creates a smidb file. This file must be loaded in the MIB browser.

C.2.4 SNMP SETs not working

Check to see if environment variables are set. The following are the environment variables to be set.

```
SNMPCONFPATH=/butterfly/snmp
MIBDIRS=/butterfly/snmp/mibs
MIBS=ALL
```

Restart the SNMP agent (the snmpd daemon)

C.2.5 Not receiving SNMP traps

Check whether SNMP traps are enabled through CLI or Applet. Configure the MIB browser to display notifications or traps. (This would generally be a check box in the MIB browser preferences).

C.2.6 Additional Configuration

Double check Managers' IP Address, community string, port number, read/write permissions, and snmp version. Remember community string is CASE SENSITIVE.

C.3 Security Issues

This chapter describes the known troubleshooting techniques for the following data protection activities:

- *Switch Password Recovery*
- *RADIUS Troubleshooting*
- *Troubleshooting RADIUS Accounting Issues*
- *Rogue AP Detection Troubleshooting*
- *Troubleshooting Firewall Configuration Issues*

C.3.1 Switch Password Recovery

If the switch Web UI password is lost, you cannot get past the Web UI login screen for any viable switch configuration activity. Consequently, a password recovery login must be used that will default your switch back to its factory default configuration.

To access the Motorola RF Series Switch using password recovery:

CAUTION: Using this recovery procedure erases the switch's current configuration and data files from the switch /flash dir. Only the switch's license keys are retained. You should be able to log in using the default username and password (admin/superuser) and restore the switch's previous configuration (only if it has been exported to a secure location before the password recovery procedure was invoked).

1. Connect a terminal (or PC running terminal emulation software) to the serial port on the front of the switch.

   The switch login screen displays. Use the following CLI command for normal login process:
   `RFSwitch login: cli`

2. Enter a password recovery username of **restore** and password recovery password of **restoreDefaultPassword**.

   User Access Verification

   Username: restore

   Password: restoreDefaultPassword

   WARNING: This will wipe out the configuration (except license key) and user data under "flash:/" and reboot the device

   Do you want to continue? (y/n):

3. Press **Y** to delete the current configuration and reset factory defaults.

   The switch will login into the Web UI with its reverted default configuration. If you had exported the switch's previous configuration to an external location, it now can be imported back to the switch.

C.3.2 RADIUS Troubleshooting

This section covers troubleshooting and workarounds for common RADIUS problems. It includes the following issues:

- *Radius Server does not start upon enable*
- *Radius Server does not reply to my requests*
- *Radius Server is rejecting the user*
- *Time of Restriction configured does not work*
- *Authentication fails at exchange of certificates*
- *When using another RFS7000 (switch 2) as RADIUS server, access is rejected*
- *Authentication using LDAP fails*
- *VPN Authentication using onboard RADIUS server fails*
- *Accounting does not work with external RADIUS Accounting server*

C.3.2.1 Radius Server does not start upon enable

Ensure the following have been attempted:

- Import valid server and CA certificates

- Add a Radius client in AAA context
- Ensure that key password in AAA/EAP context is set to the key used to generate imported certificates
- DO NOT forget to SAVE!

C.3.2.2 Radius Server does not reply to my requests

Ensure the following have been attempted:

- Add a Radius client in Radius server configuration with the Switch's VLAN interface, IP address and subnet, which have been marked as management
- Save the current configuration
- Ensure that the WLAN settings haves been set to use the on-board/local Radius server by entering the local IP address or the switch management VLAN IP address

C.3.2.3 Radius Server is rejecting the user

Ensure the following have been attempted:

- Verify a SAVE was done after adding this user.
- Is the user present in a group?
  - If yes, check if the Wlan being accessed is allowed on the group
  - Check if time of access restrictions permit the user.

C.3.2.4 Time of Restriction configured does not work

Ensure that date on the system matches your time

C.3.2.5 Authentication fails at exchange of certificates

Ensure the following have been attempted:

- Verify that valid certificates were imported.
- If the Supplicant has "Validate Server Certificate" option set, then make sure that the right certificates are installed on the MU.

C.3.2.6 When using another RFS7000 (switch 2) as RADIUS server, access is rejected

Ensure the following have been attempted:

- Make sure that the user, group and access policies are properly defined on switch 2
- Add a AAA client on switch 2 with a VLAN interface IP address which can communicate with switch 1
- Save the current configuration

C.3.2.7 Authentication using LDAP fails

Ensure the following have been attempted:

- Is LDAP server reachable?
- Have all LDAP attributes been configured properly?
- Dbtype must be set to LDAP in AAA configuration
- Save the current configuration

C.3.2.8 VPN Authentication using onboard RADIUS server fails

Ensure the following have been attempted:

- Ensure that the VPN user is present in AAA users
- This VPN user MUST NOT added to any group.
- Save the current configuration

C.3.2.9 Accounting does not work with external RADIUS Accounting server

Ensure that accounting is enabled.

- Ensure that the RADIUS Accounting server reachable
- Verify that the port number being configured on accounting configuration matches that of external RADIUS Accounting Server
- Verify that the shared secret being configured on accounting configuration matches that of external RADIUS Accounting Server

C.3.3 Troubleshooting RADIUS Accounting Issues

Use the following guidelines when configuring RADIUS Accounting

- The RADIUS Accounting records are supported for clients performing 802.1X EAP based authentication or using the Hotspot functionality.
- The user name present in the accounting records, could be that of the name in the outer tunnel in authentication methods like: TTLS, PEAP.
- If the switch crashes for whatever reason, and there were active EAP clients, then there would be no corresponding STOP accounting record.
- If using the on-board RADIUS Accounting server, one can delete the accounting files, using the del command in the enable context.
- If using the on-board RADIUS Accounting server, the files would be logged under the path: /flash/log/radius/radacct/

C.4 Rogue AP Detection Troubleshooting

Motorola recommends adhereing to the following guidelines when configuring Rogue AP detection:

- Basic configuration required for running Rogue AP detection:
  - Enable any one of the detection mechanism.
  - Enable rogueap detection global flag.
- After enabling rogueap and anyone of the detection mechanisms, look in the roguelist context for detected APs. If no entries are found, do the following:
  - Check the global rogueap flag by doing a show in rogueap context. It should display Rogue AP status as "enable" and should also the status of the configured detection scheme.
  - Check for the "Motorola AP" flag in rulelist context. If it is set to "enable", then all the detected APs will be added in approved list context.
  - Check for Rulelist entries in the rulelist context. Verify it does not have an entry with MAC as "FF:FF:FF:FF:FF:FF" and ESSID as "*"

- If you have enabled AP Scan, ensure that at least a single radio is active. AP scan does not send a scan request to an inactive or unavailable radio.
- Just enabling detectorscan will not send any detectorscan request to any adopted AP. User should also configure at least a single radio as a detectorAP. This can be done using the set detectorap command in rogueap context.

C.5 Troubleshooting Firewall Configuration Issues

Motorola recommends adhereing to the following guidelines when dealing with problems related to RFS7000 Firewall configuration:

- *A Wired Host (Host-1) or Wireless Host (Host-2) on the untrusted side is not able to connect to the Wired Host (Host-3) on the trusted side*
- *A wired Host (Host-1) on the trusted side is not able to connect to a Wireless Host (Host-2) or Wired Host (Host-3) on the untrusted side*

C.5.1 A Wired Host (Host-1) or Wireless Host (Host-2) on the untrusted side is not able to connect to the Wired Host (Host-3) on the trusted side

1. Check that IP Ping from Host1/Host2 to the Interface on the Trusted Side of the Motorola RF Series Switch works.

   CLI (from any context) - ping <host/ip_address>
2. If it works then there is no problem in connectivity.
3. Check whether Host-1/Host-2 and Host-3 are on the same IP subnet.

   If not, add proper NAT entries for configured LANs under FireWall context.
4. After last step, check again, that IP Ping from Host1 to the Interface on the Trusted Side of the Motorola RF Series Switch works.

   If it works then problem is solved.

C.5.2 A wired Host (Host-1) on the trusted side is not able to connect to a Wireless Host (Host-2) or Wired Host (Host-3) on the untrusted side

1. Check that IP Ping from Host1 to the Interface on the Untrusted Side of the switch works.
2. If it works then there is no problem in connectivity.
3. Now check whether Host-1 and Host-2/Host-3 are on the same IP subnet.

   If not, add proper NAT entries for configured LANs under FireWall context.
4. Once step 3 is completed, check again, that IP Ping from Host1 to the Interface on the Untrusted Side of the switch works.

   If it works then problem is solved.

C.5.2.1 Disabling of telnet, ftp and web traffic from hosts on the untrusted side does not work.

1. Check the configuration for the desired LAN under FW context (which is under configure context).

   CLI - configure fw <LAN_Name>
2. Check whether ftp, telnet and web are in the denied list. In this case, web is https traffic and not http.

3. Ensure that "network policy" and "Ethernet port" set to the LAN is correct.

C.5.2.2 How to block the request from host on untrusted to host on trusted side based on packet classification.

1. Add a new Classification Element with required Matching Criteria
2. Add a new Classification Group and assigned the newly created Classification Element. Set the action required.
3. Add a new Policy Object. This should match the direction of the packet flow i.e. Inbound or Outbound.
4. Add the newly created PO to the active Network Policy.
5. Associate WLAN and Network Policy to the active Access Port Policy.

   Any request matching the configured criteria should take the action configured in the Classification Element.

Appendix D "How To" Tutorials

This appendix provides "*How To*" style tutorials for many of the more important features supported by the switch:

- *Adopted AP300 Sensor Conversion*
- *Integrated WLAN RTLS*
- *MU to MU Disallow*
- *Secure Beacons*
- *Secure Device Management*
- *Secure WISPe*
- *Wireless IDS*
- *Wireless Filters*
- *802.11i Support*

D.1 Adopted AP300 Sensor Conversion

As enterprises become increasingly mobile and wireless networks more pervasive, security has become an increasing concern and is central for IT organizations. IT professionals are faced with keeping wireless networks up, running at peak levels, preserving network integrity and protecting digital assets from theft and misuse, all while complying with government and financial regulations such as Sarbanes-Oxley, HIPAA and VISA-CISP.

Motorola's AirDefense solution provides enterprises with the tools to continuously safeguard WLANs from external threats and provide continuous performance monitoring. The AirDefense Enterprise server system notifies IT staff when network vulnerabilities, attacks or performance issues occur in real-time allowing for proactive response.

This section provides an overview of how to configure the RF Switch to convert AP300 Access Ports into sensors and revert AP300 sensors back to Access Ports.

The Motorola AirDefense solution seamlessly integrates with the Motorola switches and AP300 Access Ports in the following ways:

- AP300s can be converted into dedicated AirDefense sensors
- The AirDefense Enterprise server can detect and trust APs managed by the RF Switch
- The AirDefense Enterprise server can blacklist suspicious clients by creating wireless filters on the RF Switch

- Administrators can launch the AirDefense UI from within RFMS
- The AirDefense Enterprise server can forward SMNP traps to RFMS to provide centralized alarm reporting and correlation

D.1.1 About the Motorola AirDefense System

The Motorola AirDefense System is intended for customer environments with Motorola or third-party WLAN infrastructure to provide dedicated threat and performance monitoring and compliance. The Motorola AirDefense System provides the following advanced services:

- *24x7 Dedicated Sensors* - Real-time identification of hackers, attacks and system weak spots.
- *Historical Database* - By storing and managing more than 270 data points per connection per wireless device per minute, the product provides a highly accurate assessment of wireless threats including anomalies and zero-day attacks.
- *Forensic Support* - Pertinent historical data supports advanced forensics, such as time of attack/breach, entry point used, length of exposure, systems compromised, device activity logs and transfers of data.
- *Multiple Detection Technologies* - Provides accurate and comprehensive detection by applying multiple detection technologies including signature analysis, protocol abuse and anomalous behavior in conjunction with correlation across multiple sensors.
- *Location Based Security* - Provides location of unauthorized devices and activities using Motorola WLAN infrastructure.
- *Reports* - Provides built-in reports for PCI, HIPAA, Sarbanes-Oxley, GLBA, FDIC and DOD, as well as forensic support to determine compliance level after the fact, should a security event occur.
- *Plug-and-Play Operation* - Auto-classification allows for a quick policy-based authorization of APs and devices. Network traffic can be monitored within minutes of installation, complete with the tools to quickly interpret information for fast response to Wireless LAN threats.
- *Centralized Detection Engine* - Eliminates the need to upgrade sensors individually - a single server upgrade provides new functionality and protection against the latest attacks and new threats.
- *Report Builder* - Allows customized reports to suit specific needs.
- *Advanced Forensics* - Adds a new level of depth and flexibility to forensic investigations, allowing the user to increase/decrease the analysis interval, graph data for easier analysis and conduct historical location tracking.

D.1.2 Defining an AP300 Sensor Conversion Configuration

The following outlines the requirements, components and steps required to configure a RF Switch to convert AP300 Access Ports into sensors and revert AP300 sensors back to Access Ports.

To view the running configuration on the RFS6000 switch used to create this MU to MU disallow tutorial, refer to *RF Switch Running Configuration on page D-8*.

D.1.2.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One (or more) RF Switches are installed and operational on the network
- One (or more) AirDefense Enterprise servers is installed and operational on the network
- One (or more) Access Ports configured and adopted by the RF Switch

- A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration

D.1.2.2 Components

The information in this section is based on the following Motorola hardware and software versions:

- 1 RFS6000 model switch
- 1 AirDefense Enterprise Server Version 7.3 (or higher)
- 5 AP300 model Access Ports

D.1.2.3 Switch Web UI Configuration

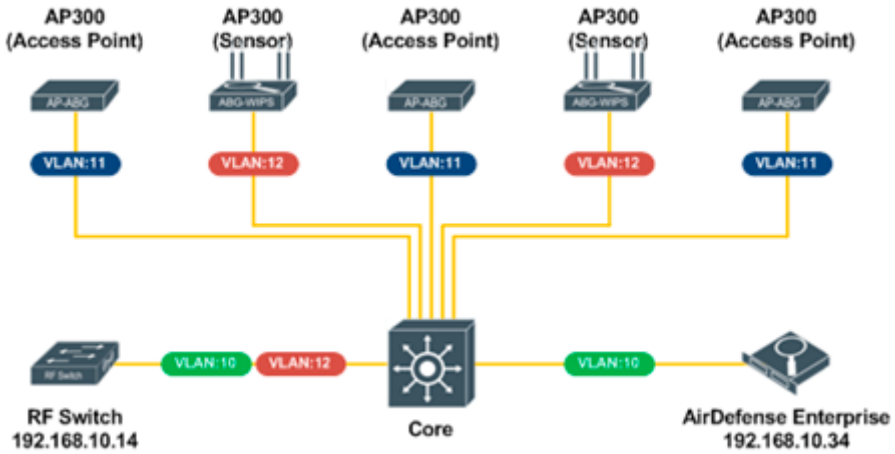
The following outlines the steps required to convert adopted AP300s into AirDefense Sensors on a RF Switch:

Converting AP300s Into Sensors

For this example, five AP300s have been deployed at a site supported by a RF Switch and a Motorola AirDefense Enterprise server. Three AP300s provide WLAN services to users and the remaining two AP300s are dedicated as AirDefense sensors.

Three of the AP300s provide WLAN services, are connected to VLAN 11 and are L3 adopted to the RF Switch. The AP300s discover and connect to the switch using DHCP scope options configured on a DHCP server providing IP addressing services to VLAN 11.

The two remaining AP300 sensors are connected to a sensor (VLAN 12 which is 802.1Q tagged to the RF Switch). The AP300s are L2 adopted, then converted into dedicated AirDefense sensors. Once converted, the AP300s will maintain a management connection with the RF Switch while monitoring the RF environment and forwarding information to the AirDefense Enterprise server.

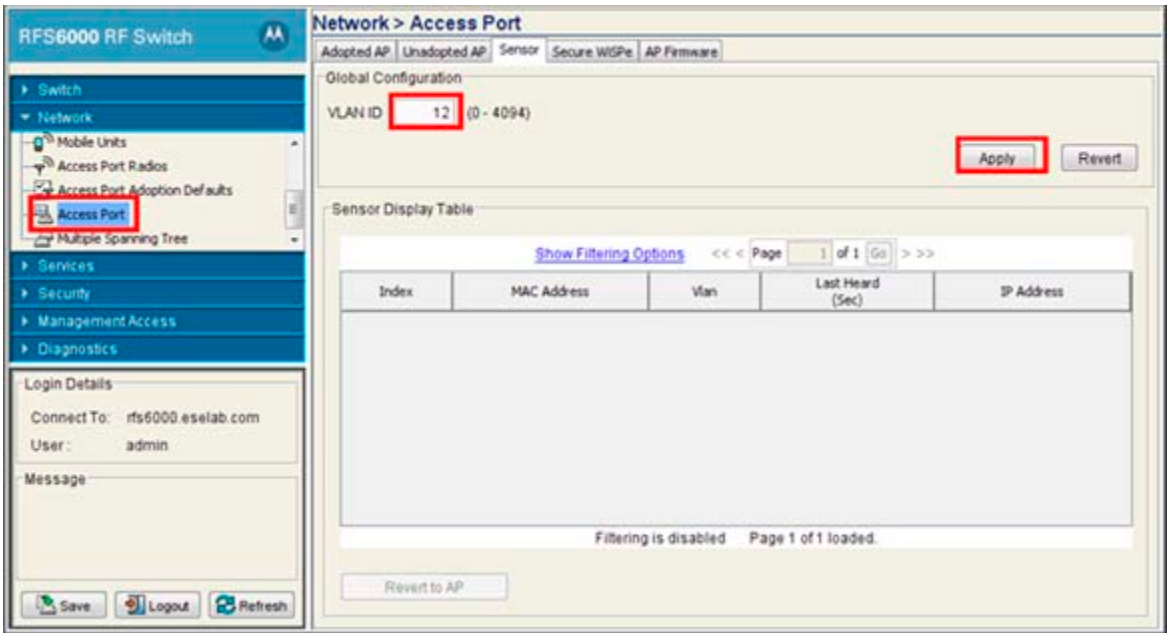


VLAN ID	*Description*	*Subnet*
10	Management VLAN	192.168.10.0/24
11	Access Point VLAN	192.168.11.0/24
12	Sensor VLAN	192.168.12.0/24

CAUTION: For the AP300 sensor conversion process to work, an AP300s must be L2 adopted to the RF Switch. L3 adopted AP300s cannot be converted into AirDefense sensors.

To convert the AP300s into sensors:

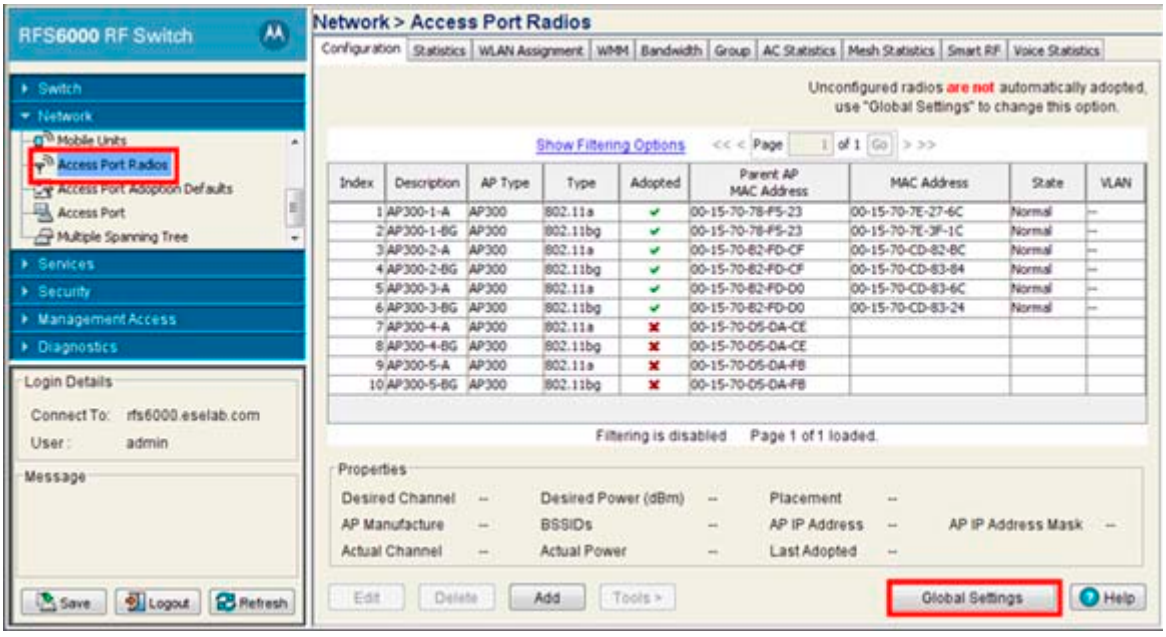
1. From the switch menu tree select **Network** > **Access Port.**
2. Select the **Sensor** tab.



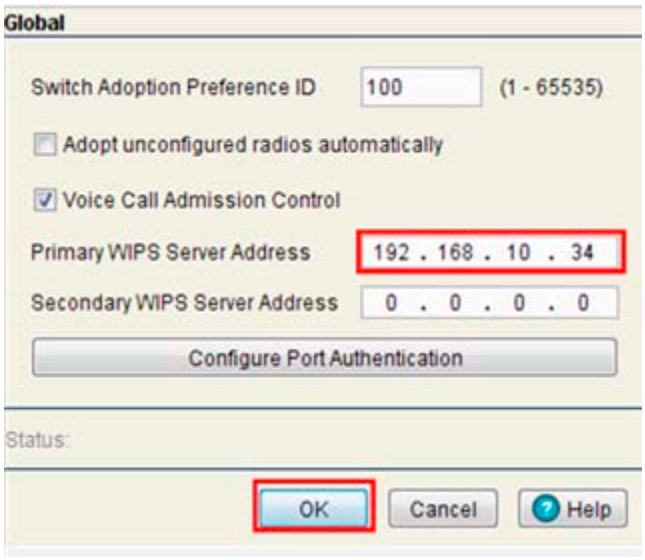
3. In the **VLAN ID** field, enter the VLAN ID where sensors are installed.

   In this example sensors are located on VLAN 12. Click **Apply**.

4. From the switch menu tree select **Network** > **Access Port Radios.**



5. Select the **Configuration** tab then click **Global Settings** in the bottom right-hand side of the screen.

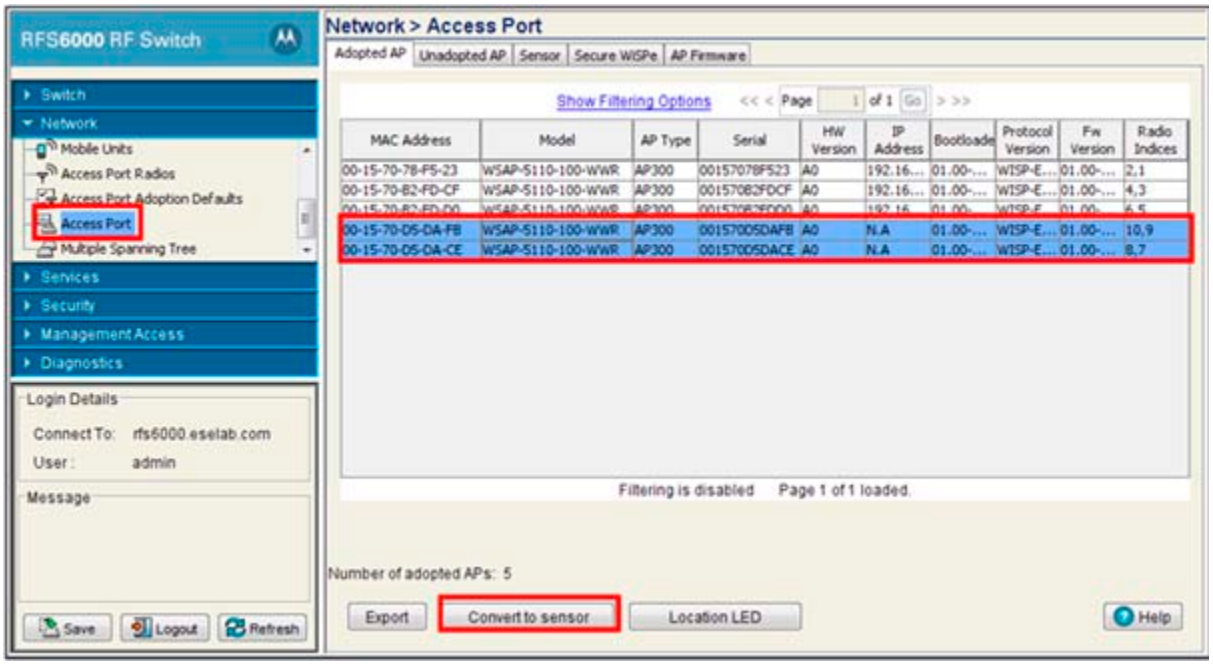


6. Enter the **Primary WIPS Server Address**.

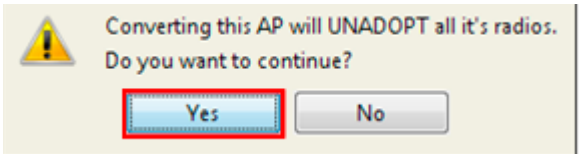
   If applicable, enter a **Secondary WIPS Server Address**. In this example, a single AirDefense Enterprise server has been deployed using 192.168.10.34 as the IP address. Click **OK**.

7. From the switch menu tree select **Network** > **Access Port.**

8. Select the **Adopted AP** tab.



9. Highlight the AP300s to convert into sensors and select the **Convert to sensor** button.



A confirmation screen displays the following message: **Converting the AP will UNADOPT all its radios. Do you want to continue?**

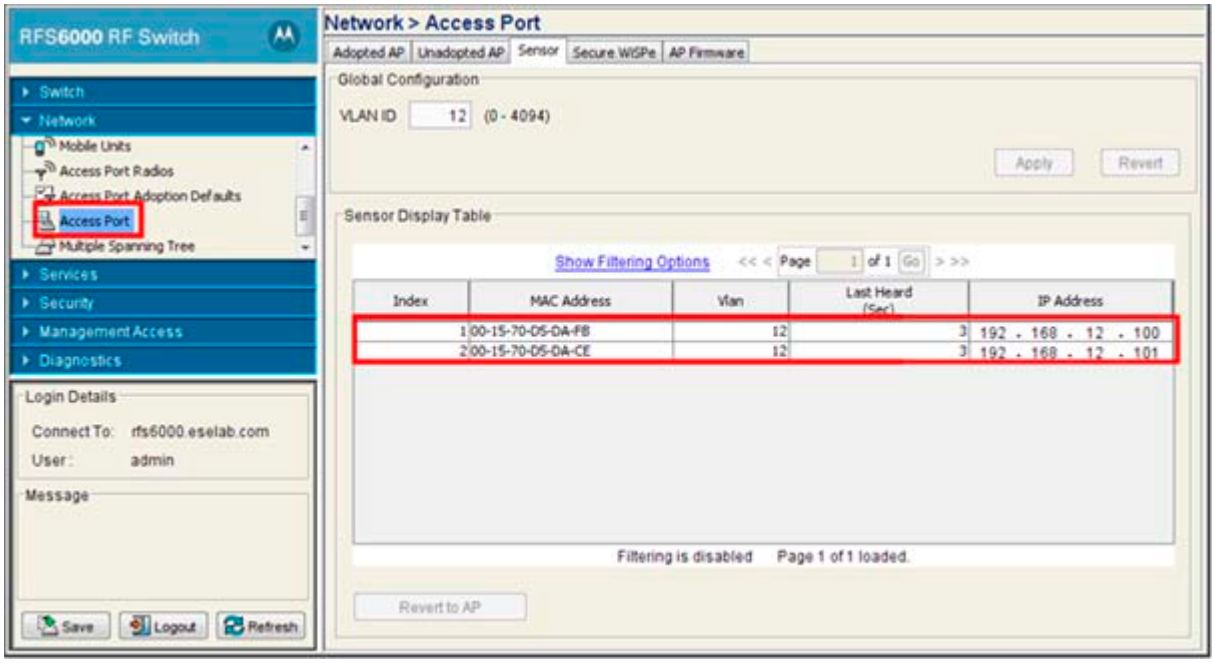
10. Select **Yes** to confirm the conversion.

    A **Conversion in progress**.....screen displays.

11. Select **OK** to proceed.

12. Select **Save** (from the lower left-hand corner) to apply the changes.

    After several minutes, select **Network** > **Access Port Radios** from the switch menu tree.



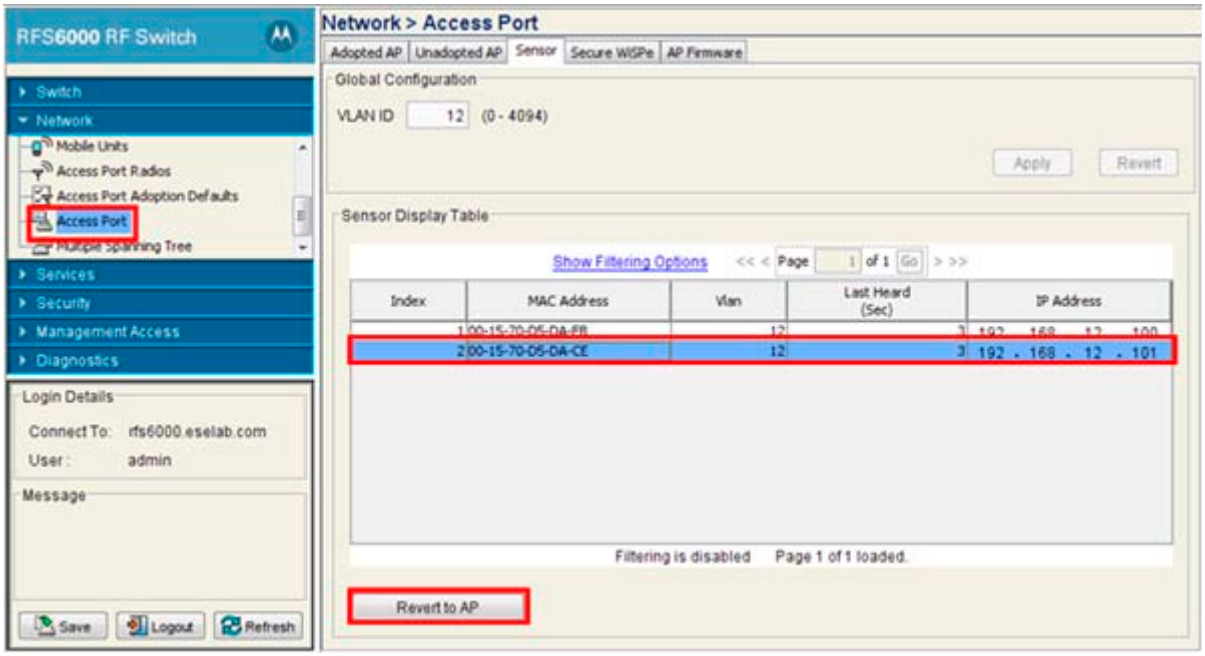
13. Select the **Sensor** tab.

    The converted sensors display within in the **Sensor Display Table.**

Reverting Sensors Into Access Ports

To revert a sensor back into an Access Port:

1. From the switch menu tree select **Network** > **Access Port.**
2. Select the **Sensor** tab.



3. Highlight the sensor MAC address to convert back to an AP, then select the **Revert to AP** button.

   A **Do you really want to revert selected Sensor(s)?** message displays.

4. Select **Yes** to confirm the conversion.

D.1.3 RF Switch Running Configuration

The following is the running configuration on the RFS6000 switch used to create this AP300 sensor conversion tutorial:

```
RFS6000# show running-config
!
! configuration of RFS6000 version 3.3.0.0-029R
!
version 1.2
!
!
aaa authentication login default local none
service prompt crash-info
!
username "admin" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc."
"WLAN Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v3
```

```
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
timezone America/New_York
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d04677
7fbed80f433b68ea
!
wireless
 secure-wispe-default-secret 0 defaultS
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
 wlan 1 dot11i preauthentication
 wlan 2 enable
 wlan 2 description MOTO-GUEST
 wlan 2 ssid MOTO-GUEST
 wlan 2 vlan 70
 wlan 2 authentication-type hotspot
 wlan 2 hotspot webpage-location advanced
 wlan 2 radius server primary 192.168.10.14
 wlan 2 radius server primary radius-key 0 ESELAB
 wlan 2 radius accounting server primary 192.168.10.14
 wlan 2 radius accounting server primary radius-key 0 ESELAB
```

```
wlan 3 enable
wlan 3 description MOTO-VOICE
wlan 3 ssid MOTO-VOICE
wlan 3 vlan 80
wlan 3 encryption-type tkip
wlan 3 dot11i phrase 0 motovoicetest
wlan 3 dot11i preauthentication
radio add 1 00-15-70-78-F5-23 11a ap300
radio 1 description AP300-1-A
radio 1 bss 1 1
radio 1 channel-power indoor 36 15
radio 1 on-channel-scan
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
radio 5 description AP300-3-A
radio 5 bss 1 1
radio 5 channel-power indoor 44 15
radio 5 on-channel-scan
radio 5 adoption-pref-id 100
```

```
 radio add 6 00-15-70-B2-FD-D0 11bg ap300
 radio 6 description AP300-3-BG
 radio 6 bss 1 1
 radio 6 bss 2 2
 radio 6 bss 3 3
 radio 6 channel-power indoor 11 18
 radio 6 on-channel-scan
 radio 6 short-preamble
 radio 6 adoption-pref-id 100
 radio add 7 00-15-70-D5-DA-CE 11a ap300
 radio 7 description AP300-4-A
 radio 7 channel-power indoor 48 17
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 radio add 9 00-15-70-D5-DA-FB 11a ap300
 radio 9 description AP300-5-A
 radio 9 channel-power indoor 149 20
 radio 9 on-channel-scan
 radio add 10 00-15-70-D5-DA-FB 11bg ap300
 radio 10 description AP300-5-BG
 radio 10 channel-power indoor 6 4
 radio 10 on-channel-scan
 no ap-ip default-ap switch-ip
 ap-detection enable
 sensor vlan 12
 sensor default-config wips-server-ip primary 192.168.10.34
!
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
```

```
!
radius-server local
 authentication eap-auth-type all
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
switchport access vlan 10
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
```

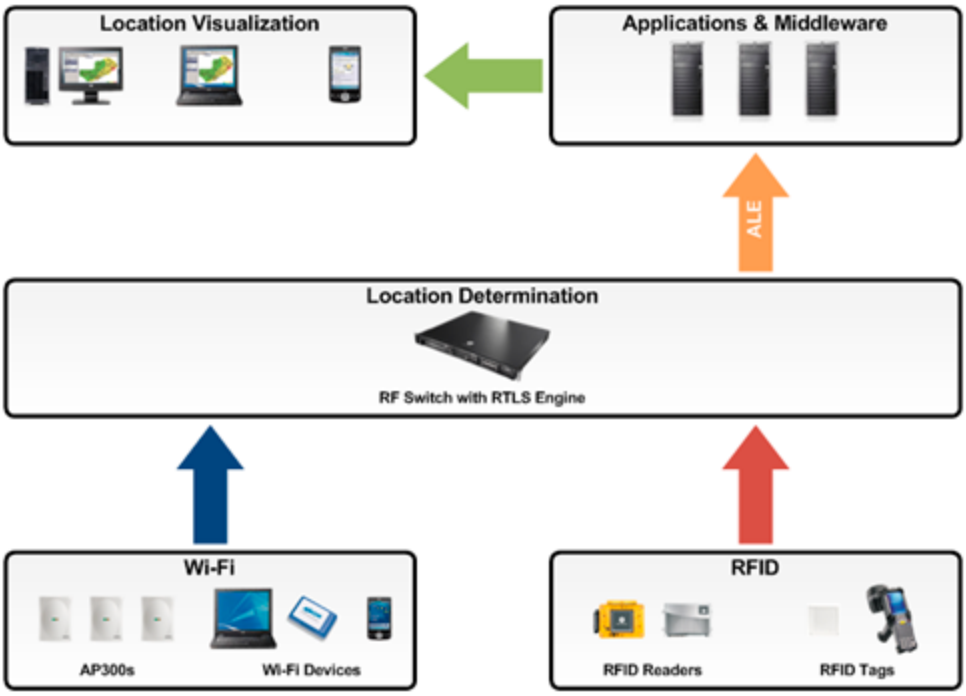
```
interface vlan1
 no ip address
 shutdown
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
!
interface vlan70
 description GUEST
 ip address 192.168.70.14/24
!
!
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
end
```

D.2 Integrated WLAN RTLS

The *Motorola Real Time Locationing System* (RTLS) is a wireless radio frequency solution that continually monitors and reports (in real-time) the location of tracked resources. Unlike competing solutions, which are solely based on Wi-Fi, the Motorola RTLS solution is RF agnostic supporting Passive RFID, Active RFID and other emerging RF and non-RF technologies.

The Motorola RTLS solution leverages standards based 802.11a/b/g Access Points and the *Low Level Reader Protocol* (LLRP) allowing the RF Switch to provide location services for standard 802.11 devices and tags as well as RFID enabled devices and tags.

By eliminating the need to purchase overlay location engines, the Motorola WLAN system can provide standard data, video and voice WLAN services to users while simultaneously tracking Wi-Fi and RFID devices.



D.2.1 Wi-Fi Location Determination

To provide 802.11 locationing, the integrated RTLS engine uses a signal propagation model which is constantly updated using real time values of RSSI measurements from APs and trilateration to determine client location. Using this signal propagation model, the integrated RTLS engine can avoid time consuming calibration.

The RTLS processing consists of several discrete steps:

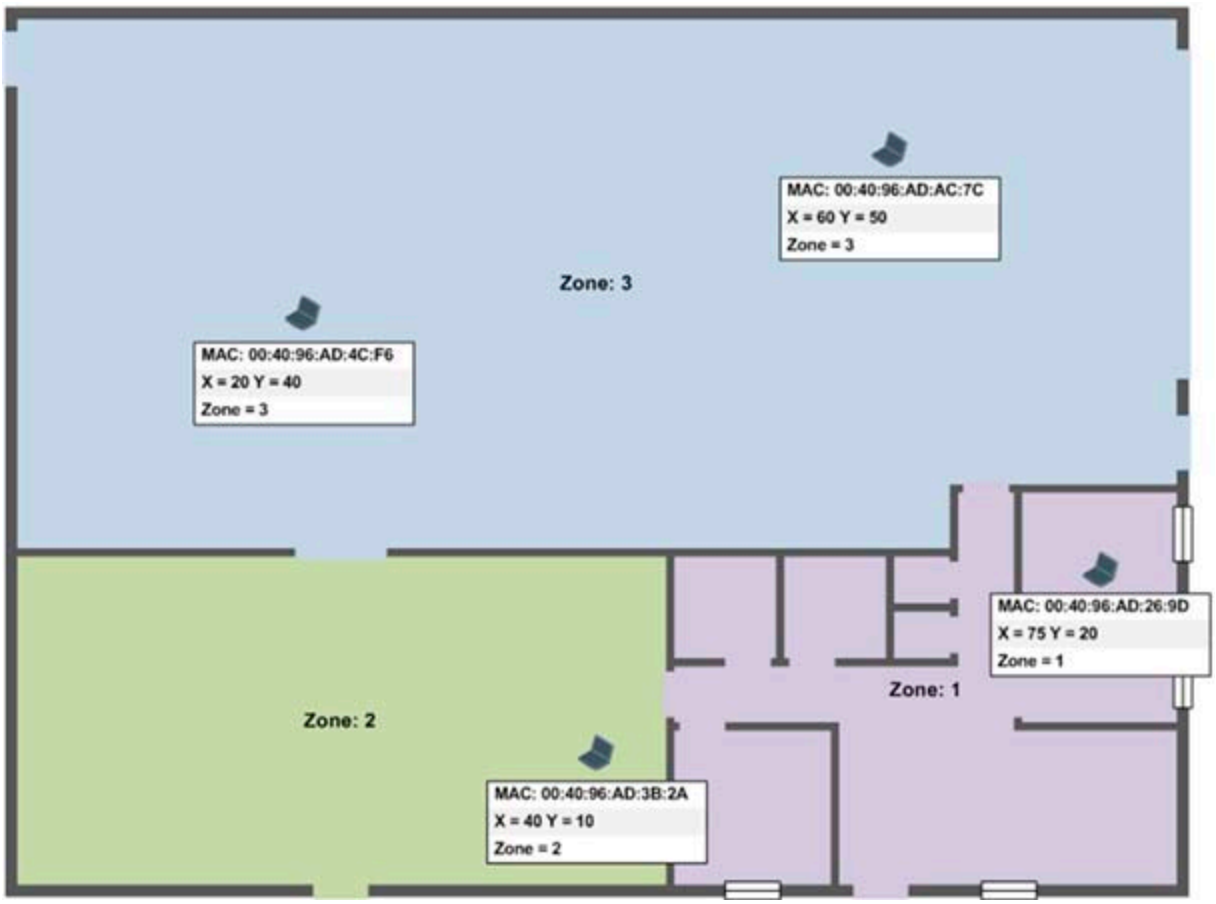
- Devices transmit probe requests to APs.
- APs forward these probes to the integrated RTLS engine on the RF Switch.
- The integrated RTLS Engine collects the RSSI values from all the APs that are within reach of each client.
- The RTLS engine computes the location of each client using the RSSI values and trilateration.

The integrated RTLS engine uses RSSI information received from clients 802.11 *Probe Requests* to compute a client's location. For the RTLS engine to update the clients location in real-time, it needs to constantly receive *Probe Request* packets from the clients. However, the transmission of Probe Request packets is client-dependent and may only occur when a client roams. Consequently, Motorola recommends Wi-Fi clients run the following client software to ensure the periodic transmission of 802.11 Probe Request packets:

- *Motorola Handhelds* - MUSTAT.exe
- *Non Motorola Wi-Fi Clients* - NetStumbler

D.2.2 Location Presentation

Once the RTLS engine has been enabled, the RF Switch discovers clients and computes each client's location to provide an estimated X/Y coordinate for the clients.

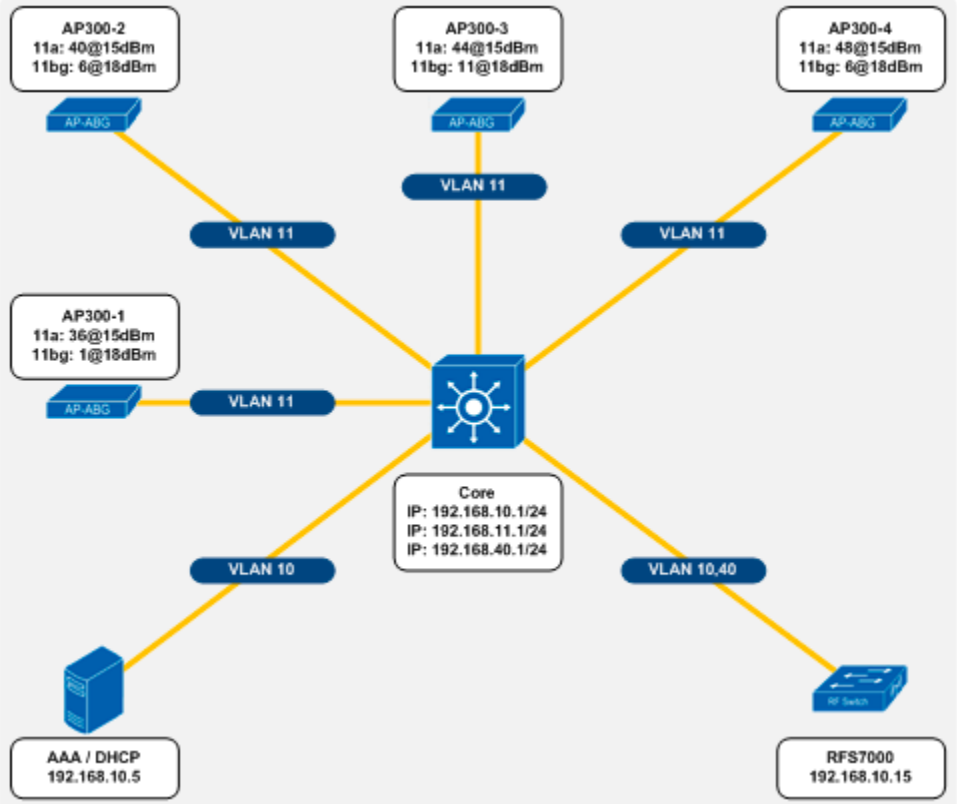


The computed X/Y coordinate and zone for each client can be viewed directly on the RF Switch using CLI or Web-UI or exported to a third-party application for visualization on a floor plan using the standards based ALE application interface.

Location Attribute	*Description*
MAC Address	The MAC Address for each client discovered by the switch.
X coordinate	The estimated X coordinate for each client in relation to the defined origin point (0,0) of the site.
Y coordinate	The estimated Y coordinate for each client in relation to the defined origin point (0,0) of the site.
Timestamp	The last time each client's location was computed by the switch.
Zone	The last known zone for each client. When no zones are defined the RF Switch will list clients in a default zone.

D.2.3 Network Topology

The following network topology was used for this Integrated WLAN RTLS “how to” tutorial:



NOTE: The configuration outlined in the Network Topology is not necessarily applicable to all customer environments.

D.2.4 Defining an Integrated WLAN RTLS Configuration

This section provides the following RFS7000 tasks to enable the integrated real-time locationing engine:

- *Site Information*
- *Access Point Location*
- *Location Zones*
- *Locating Clients*

NOTE: For a listing of the radio, switch and Ethernet switch configurations used in the development of this tutorial, see *Baseline Configurations on page D-27*.

D.2.4.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One (or more) RF Switches are installed and operational on the network
- Radio adoption parameters are configured on all the RF Switches in the cluster so each AP can be adopted by any cluster member RF Switch

- A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration

D.2.4.2 Components

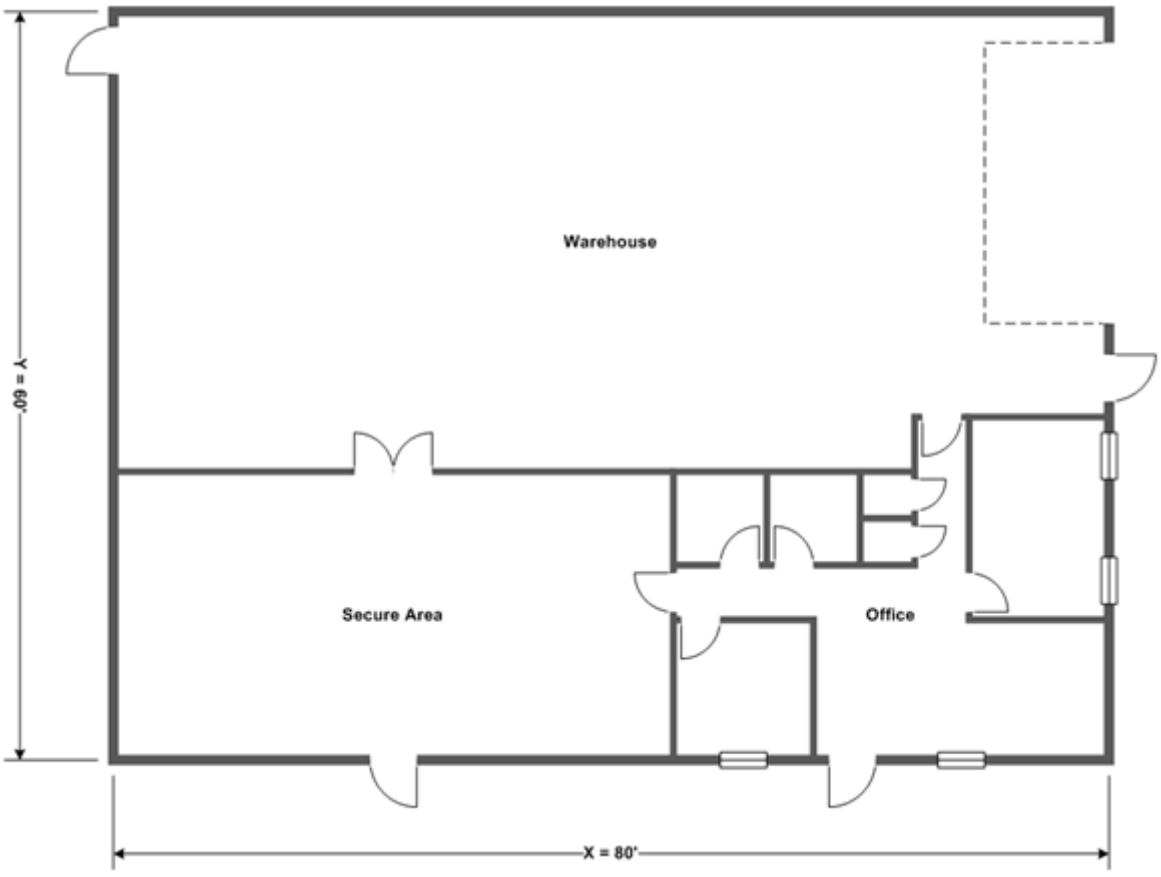
The information in this section is based on the following Motorola hardware and software versions:

- 1 RFS7000 model switch (version 2.3 or higher)
- 4 AP300 model Access Ports

D.2.4.3 Site Information

The first step for enabling the real-time locationing engine is to provide information about the site where clients are to be located. Required information includes the name of the site, site dimensions and the dimensional measurement unit (feet or meters). The following site information must be entered into the RF Switch for the site:

- *Site Name* - Acme Inc.
- *Site Description* - Acme Inc. San Jose CA.
- *Dimensional Units* - Feet
- *Building Dimensions* - X (Width) = 80, Y (Length) = 60, Z (Height) = 18



Defining the Site Name and Dimensions

For a listing of the radio, switch and Ethernet switch configurations used in the development of this tutorial, see *Baseline Configurations on page D-27*.

The following steps demonstrate how to define a location sites name and dimensions using the switch CLI:

1. Enter the global configuration context by issuing a ***configure terminal*** command.

   ```
   RFS7000# configure terminal
   RFS7000(config)#
   ```

2. Enter the RTLS configuration context by issuing the ***rtls*** command.

   ```
   RFS7000(config)# rtls
   RFS7000(config-rtls)#
   ```

3. Specify a name for the location site by issuing the ***site name*** command. In this example the site name ***Acme Inc***. will be used.

   ```
   Syntax: site <site-name>
   RFS7000(config-rtls)# site name Acme Inc.
   ```

4. Specify a description for the location site by issuing the ***site description*** command. In this example the site description ***Acme Inc. San Jose CA*** is used.

   ```
   Syntax: site description <site-description>
   RFS7000(config-rtls)# site description Acme Inc. San Jose CA
   ```

5. Specify the site dimensional measurement unit type by issuing the ***site dimension unit*** command. For this example dimensions are entered in feet.

   ```
   Syntax: site dimension unit [feet | meters]
   RFS7000(config-rtls)# site dimension unit feet
   ```

6. Specify the building dimensions for the site by issuing the ***site dimensions*** command. The site dimensions 80' x 60' x 18' are used.

   ```
   Syntax: site dimension length <X> width <Y> height <Z>
   RFS7000(config-rtls)# site dimension length 80 width 60 height 18
   ```

7. Verify site location information by issuing a ***show rtls site*** command.

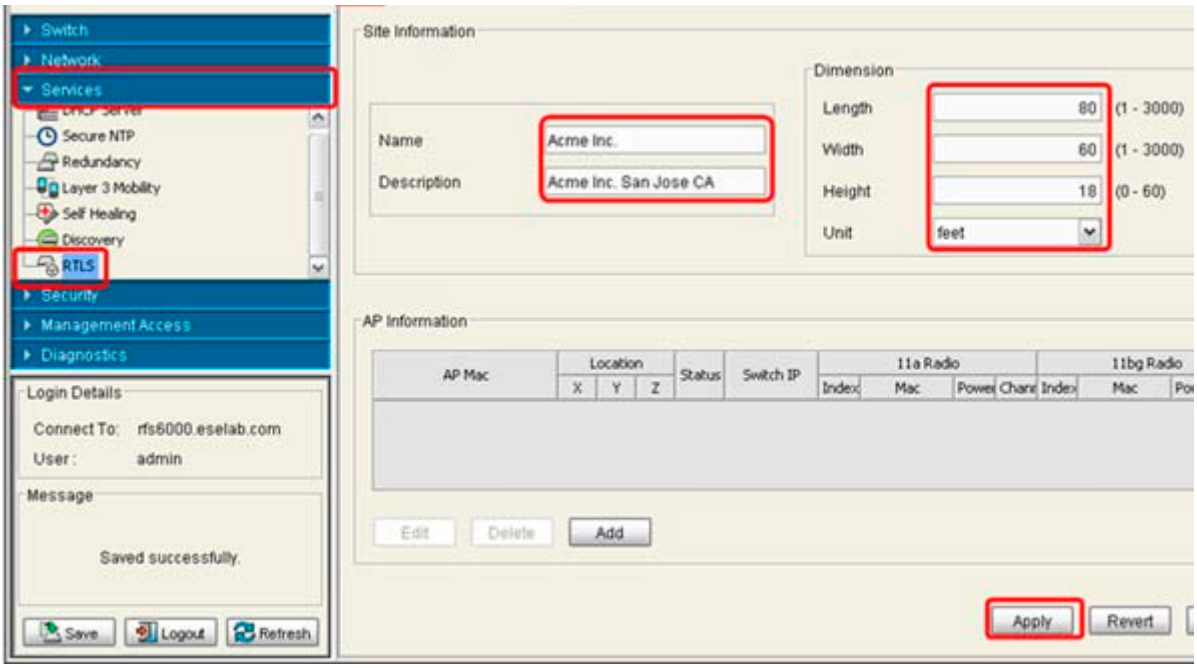
   ```
   RFS7000# show rtls site
   ```

- *Site Name* - Acme Inc.
- *Site Description* - Acme Inc. San Jose CA
- *Site Unit* - feet
- *Site Dimension* - 80L X 60W X 18H
- *Site Scale Factor* - 1.000000
- *Switch Coordinates* - 0:0:0
- *Switch Geo Coordinates* - Not configured

Switch Web UI Configuration

The following steps demonstrate how to define a location's sites name and dimensions:

1. From the switch menu tree select **Services** > **RTLS.**

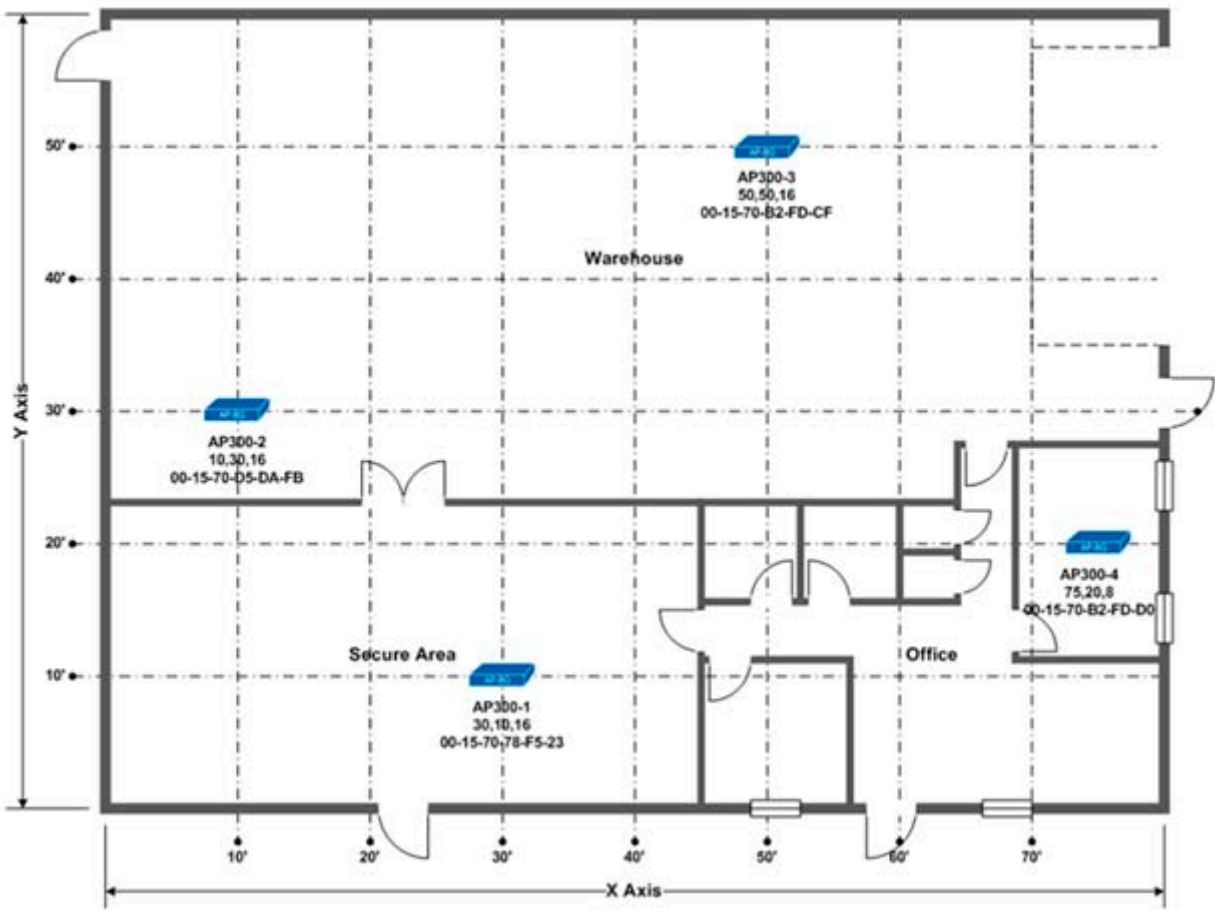


2. Provide a **Name** and **Description** for the site as well as the site's **Length**, **Width**, **Height** and **Unit** dimensional information. Click **Apply** when completed.

D.2.4.4 Access Point Location

Once initial site information has been defined, the location of deployed APs need to be entered. The location of any deployed APs is important, as the location engine uses AP location when estimating the locations of tracked devices.

For this example, the MAC addresses and X, Y, Z coordinates of four adopted APs are defined using the information provided in table below. Since the site is using feet as the dimensional measurement unit, all AP coordinates represent feet.



AP Number	*MAC Address*	*X Axis*	*Y Axis*	*Z Axis*
1	00-15-70-78-F5-23	30	10	16
2	00-15-70-D5-DA-FB	10	30	16
3	00-15-70-B2-FD-CF	50	50	16
4	00-15-70-B2-FD-D0	75	20	8

Defining the AP Information

The following steps demonstrate how to define AP location using the switch CLI:

1. In the ***RTLS*** configuration context, add each Access Point and specify the ***MAC Address*** and ***X,Y,Z*** coordinates by issuing the ***ap*** command. In this example four APs are added to the site:

```
Syntax: ap <ap-mac> coordinates x <value> y <value> z <value>
RFS7000(config-rtls)# ap 00-15-70-78-F5-23 coordinates x 30 y 10 z 16
RFS7000(config-rtls)# ap 00-15-70-D5-DA-FB coordinates x 10 y 30 z 16
RFS7000(config-rtls)# ap 00-15-70-B2-FD-CF coordinates x 50 y 50 z 16
RFS7000(config-rtls)# ap 00-15-70-B2-FD-D0 coordinates x 75 y 20 z 8
```

2. Verify the location site AP configuration by issuing the ***show rtls site*** command.

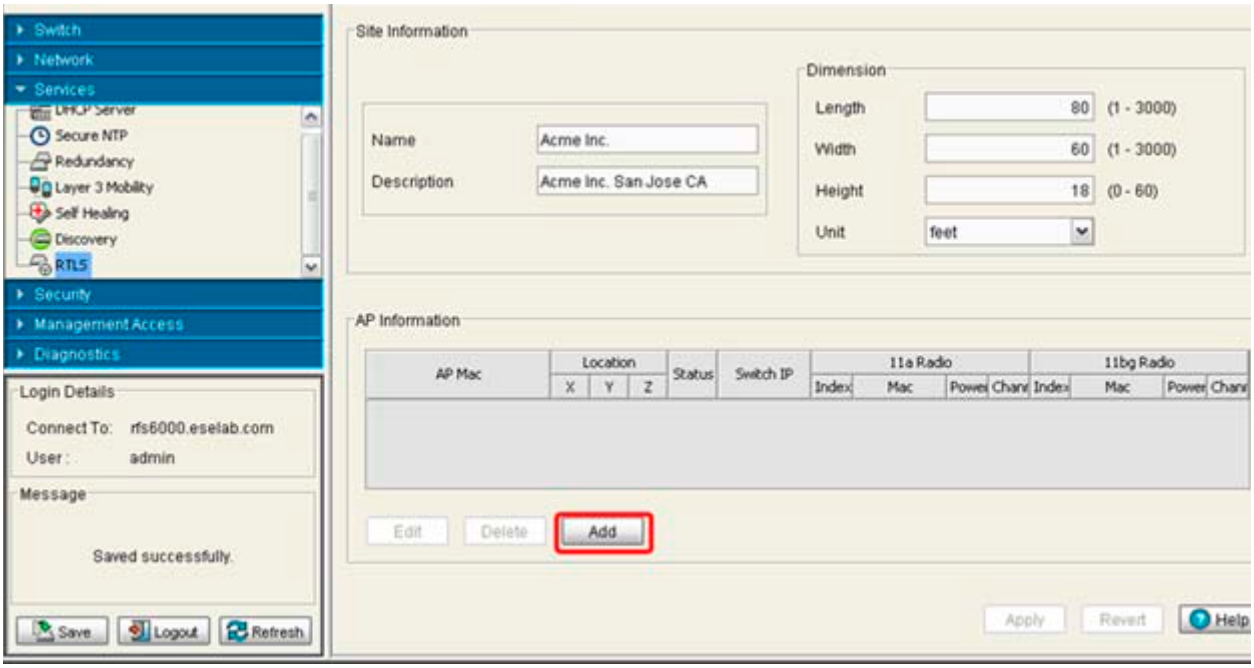
```
RFS7000# show rtls site
```

```
                                                                  11a Radio info.                11bg Radio info.
      AP MAC              Status    Location        Switch IP    idx|      MAC      | Pow|Ch    idx | MAC | Pow | Ch
-------------------------------------------------------------------------------------------------------------------------
1] 00-15-70-D5-DA-FB      Adopted   10: 30: 16      localhost    7|00-15-70-D0-25-64|15| 48    8|00-15-70-D0-26-54|
3] 00-15-70-B2-FD-CF      Adopted   50: 50: 16      localhost    3|00-15-70-CD-82-BC|15| 40    4|00-15-70-CD-83-84|
4] 00-15-70-78-F5-23      Adopted   30: 10: 16      localhost    1|00-15-70-7E-27-6C|15| 36    2|00-15-70-7E-3F-1C|
5] 00-15-70-B2-FD-D0      Adopted   75: 20:  8      localhost    5|00-15-70-CD-83-6C|15| 44    6|00-15-70-CD-83-24|
```

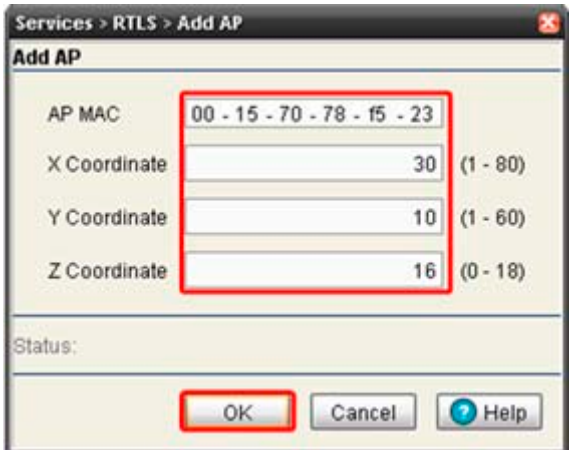
Switch Web UI Configuration

The following steps demonstrate how to define access point information for the site:

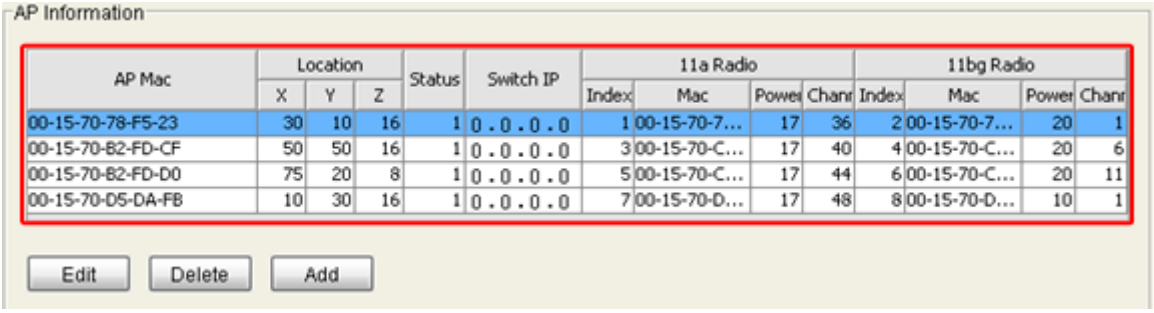
1. From the switch menu tree select **Services** > **RTLS.**



2. Select the **Add** button.



3. Enter the **APs MAC** address and **X,Y, Z Coordinates.** Click **OK**.
4. Repeat for each additional AP.

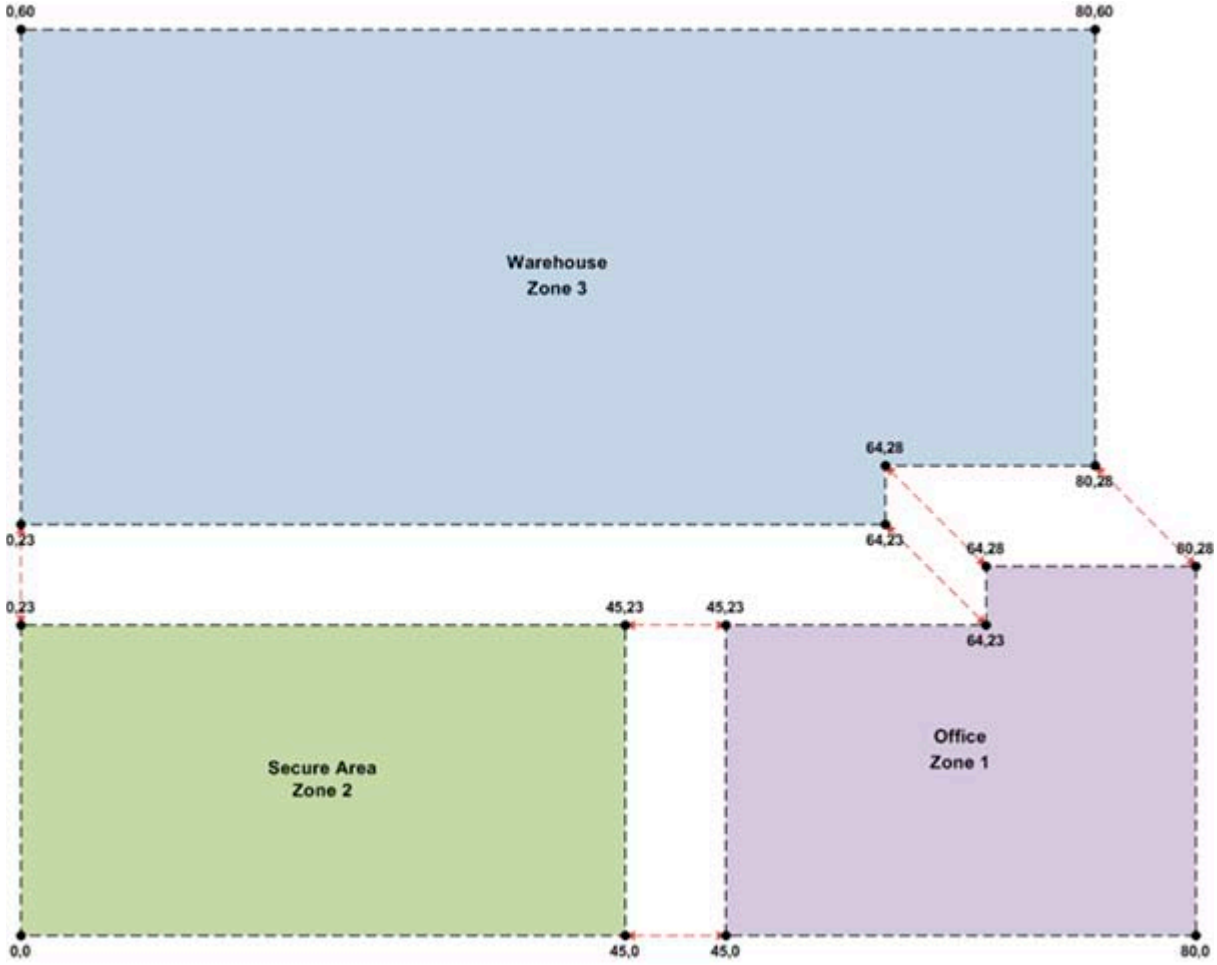


Once completed, the four APs display in the **AP Information** table.

D.2.4.5 Location Zones

The final step for defining the site is specifying zones where tracked clients are placed. When tracking clients, the integrated location engine associates each tracked client with a zone and provides a more specific X, Y coordinate zone estimation for the client. Tracked clients that cannot associate to a zone are placed in a default zone.

For this example, the location site contains three zones (*Office*, *Secure Area* and *Warehouse*). Each zone is assigned a unique zone ID. Each zone's perimeter is defined by entering the X, Y coordinates for each point of the zones perimeter in order (clockwise or counterclockwise). A zone's perimeter must include a minimum of 3 points, and must not exceed 16 points. Additionally, a zone's perimeter must not overlap another defined zone.



Defining Zone Perimeters

The following steps demonstrate how to name and define the perimeter of three zones at the site:

1. In the ***RTLS*** configuration context, define the name for zone 1 by issuing a ***zone*** command.

   Syntax: ***zone <zone-id> <name>***

   RFS7000(config-rtls)# ***zone 1 name Office***

2. Enter each point on the perimeter for zone 1 (in order).

   In this example, zone 1 includes 6 points which will each be entered in order (counterclockwise).

   RFS7000(config-rtls)# ***zone <zone-id> perimeter x <value> y <value>***
   RFS7000(config-rtls)# ***zone 1 perimeter x 45 y 0***
   RFS7000(config-rtls)# ***zone 1 perimeter x 80 y 0***
   RFS7000(config-rtls)# ***zone 1 perimeter x 80 y 28***
   RFS7000(config-rtls)# ***zone 1 perimeter x 64 y 28***
   RFS7000(config-rtls)# ***zone 1 perimeter x 64 y 23***
   RFS7000(config-rtls)# ***zone 1 perimeter x 45 y 23***

3. Define the name for zone 2 by issuing a ***zone*** command.

   Syntax: ***zone <zone-id> <name>***

   RFS7000(config-rtls)# ***zone 2 name Secure Area***

4. Using the ***zone*** command, enter each point on the perimeter for zone 2 (in order). In this example, zone 2 includes 4 points which should each be entered in order (counterclockwise).

   Syntax: zone <zone-id> ***perimeter x <value> y <value>***

   RFS7000(config-rtls)# ***zone 2 perimeter x 0 y 0***

   RFS7000(config-rtls)# ***zone 2 perimeter x 45 y 0***

   RFS7000(config-rtls)# ***zone 2 perimeter x 45 y 23***

   RFS7000(config-rtls)# ***zone 2 perimeter x 0 y 23***

5. Define the name for zone 3 by issuing ***zone*** command.

   Syntax: ***zone <zone-id> <name>***

   RFS7000(config-rtls)# ***zone 3 name Warehouse***

6. Using the ***zone*** command enter each point on the perimeter for zone 3 (in order).

   In this example, zone 3 includes 6 points which should each be entered in order (counterclockwise).

   Syntax: ***zone <zone-id> perimeter x <value> y <value>***

   RFS7000(config-rtls)# ***zone 3 perimeter x 0 y 23***

   RFS7000(config-rtls)# ***zone 3 perimeter x 64 y 23***

   RFS7000(config-rtls)# ***zone 3 perimeter x 64 y 28***

   RFS7000(config-rtls)# ***zone 3 perimeter x 80 y 28***

   RFS7000(config-rtls)# ***zone 3 perimeter x 80 y 60***

   RFS7000(config-rtls)# ***zone 3 perimeter x 0 y 60***

7. Verify location site zone information and configuration by issuing a ***show rtls zone detail*** command.

```
Zone Config:
Index      : 1
Name[01]   : Office
Perimeter   : (45 : 0) (80 : 0) (80 : 28) (64 : 28) (64 : 23) (45 : 23)
Num of RFID reader-antennas: 0
Zone Config:
Index      : 2
Name[02]   : Secure Area
Perimeter  : (0 : 0) (45 : 0) (45 : 23) (0 : 23)
Num of RFID reader-antennas: 0
Zone Config:
Index      : 3
Name[03]   : Warehouse
Perimeter   : (0 : 23) (64 : 23) (64 : 28) (80 : 28) (80 : 60) (0 : 60)
Num of RFID reader-antennas: 0
```

NOTE: Zone information can only be entered and viewed using the CLI. Web UI support will be available in a future release.

D.2.4.6 Locating Clients

Once the site has been defined, the RTLS engine can be enabled and devices tracked. The following steps demonstrate how to enable the integrated RTLS engine and track Wi-Fi clients at the site:

1. In the RTLS configuration context, enter the Location Engine Parameters configuration context by issuing a ***sole*** command.

```
RFS7000(config-rtls)# sole
RFS7000(config-rtls-sole)#
```

2. Enable client locationing by issuing a ***locate mobile-unit*** command.

```
Syntax: [no] locate mobile-unit enable
RFS7000(config-rtls-sole)# locate mobile-unit enable
```

3. The default location interval (30 seconds) can be changed by issuing allocate ***mobile-unit*** command.

   Syntax: ***locate mobile-unit interval <5-3600>***

4. Verify client locationing is enabled by issuing a ***show rtls sole*** command.

```
RFS7000(config-rtls-sole)# show rtls sole
  #  Type  On-board  Interval
  1  mobile-unit  enabled   30
  #  mobile-unit MAC
  1  00-40-96-AD-4C-F6
```

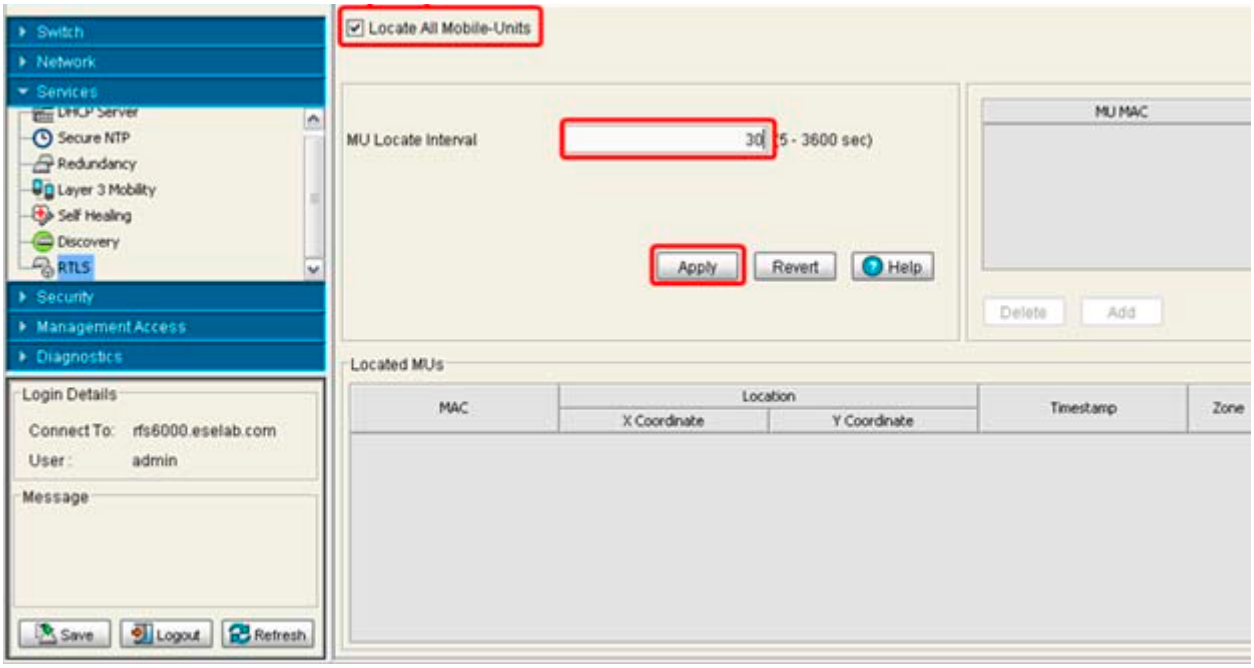
5. View client location by issuing a ***show rtls tags*** command. This command displays each clients X,Y coordinate and zone.

   ```
   RFS7000(config-rtls-sole)# show rtls tags
   ```

Switch Web UI Configuration

The following steps demonstrate how to enable the integrated RTLS engine and track Wi-Fi clients at a site:

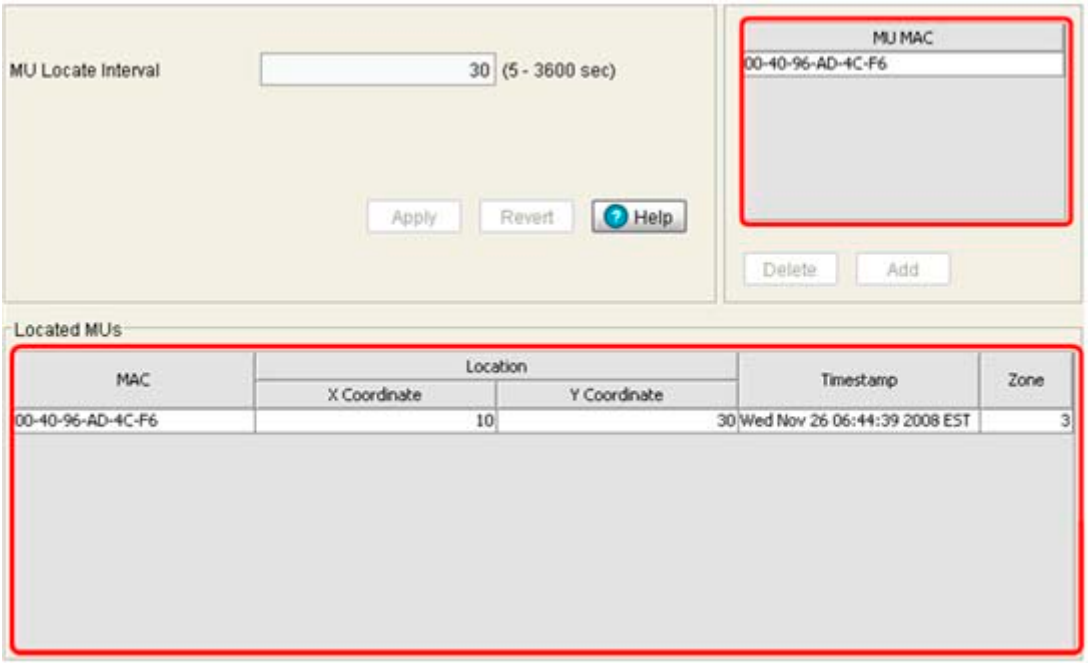
1. From the switch menu tree select **Services** > **RTLS.**
2. Select the **SOLE** tab



3. Enable locationing for all clients by clicking the **Locate All Mobile-Units** checkbox.

   You can also modify the default location interval by changing the value in the **MU Locate Interval** field. Click **Apply** when completed.

   All associated MUs display in the MU MAC table.



Location information for each associated MU (including X,Y coordinates and zone) display in the Located MU's table.

D.2.5 Baseline Configurations

This section displays the radio, switch and Ethernet switch configurations used in for this tutorial.

D.2.5.1 Radio Configuration

The following displays the adopted AP300 radio configuration and operating state:

```
RFS7000# show wireless radio
IDX   AP MAC             RADIO-BSSID       TYPE STATE    CHANNEL  POWER  ADOPTED-BY
1     00-15-70-78-F5-23  00-15-70-7E-27-6C 11a   normal   36 (36 ) 15(15) 192.168.10.15
2     00-15-70-78-F5-23  00-15-70-7E-3F-1C 11bg  normal   1  (1  ) 18(18) 192.168.10.15
3     00-15-70-B2-FD-CF  00-15-70-CD-82-BC 11a   normal   40 (40 ) 15(15) 192.168.10.15
4     00-15-70-B2-FD-CF  00-15-70-CD-83-84 11bg  normal   6  (6  ) 18(18) 192.168.10.15
5     00-15-70-B2-FD-D0  00-15-70-CD-83-6C 11a   normal   44 (44 ) 15(15) 192.168.10.15
6     00-15-70-B2-FD-D0  00-15-70-CD-83-24 11bg  normal   11 (11 ) 18(18) 192.168.10.15
7     00-15-70-D5-DA-FB  00-15-70-D0-25-64 11a   normal   48 (48 ) 15(15) 192.168.10.15
8    00-15-70-D5-DA-FB  00-15-70-D0-26-54 11bg  normal   6  (6  ) 18(18) 192.168.10.15
```

D.2.5.2 RF Switch Running Configuration

The following shows the running configuration of the switch:

```
!
! configuration of RFS6000 version 3.3.0.0-023R
!
version 1.1
!
!
aaa authentication login default local none
```

```
service prompt crash-info
!
username "admin" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc." "WLAN
Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
timezone America/New_York
```

```
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d046777fbed8
0f433b68ea
!
wireless
 secure-wispe-default-secret 0 defaultS
 adoption-pref-id 100
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
 wlan 1 dot11i preauthentication
 radio add 1 00-15-70-78-F5-23 11a ap300
 radio 1 description AP300-1-A
 radio 1 bss 1 1
 radio 1 channel-power indoor 36 15
 radio 1 on-channel-scan
 radio 1 adoption-pref-id 100
 radio add 2 00-15-70-78-F5-23 11bg ap300
 radio 2 description AP300-1-BG
 radio 2 bss 1 1
 radio 2 bss 2 2
 radio 2 bss 3 3
 radio 2 channel-power indoor 1 18
 radio 2 on-channel-scan
 radio 2 short-preamble
 radio 2 adoption-pref-id 100
 radio add 3 00-15-70-B2-FD-CF 11a ap300
 radio 3 description AP300-2-A
 radio 3 bss 1 1
 radio 3 channel-power indoor 40 15
```

```
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
radio 5 description AP300-3-A
radio 5 bss 1 1
radio 5 channel-power indoor 44 15
radio 5 on-channel-scan
radio 5 adoption-pref-id 100
radio add 6 00-15-70-B2-FD-D0 11bg ap300
radio 6 description AP300-3-BG
radio 6 bss 1 1
radio 6 bss 2 2
radio 6 bss 3 3
radio 6 channel-power indoor 11 18
radio 6 on-channel-scan
radio 6 short-preamble
radio 6 adoption-pref-id 100
radio add 7 00-15-70-D5-DA-FB 11a ap300
radio 7 description AP300-4-A
radio 7 bss 1 1
radio 7 channel-power indoor 48 15
radio 7 on-channel-scan
radio 7 adoption-pref-id 200
radio add 8 00-15-70-D5-DA-FB 11bg ap300
radio 8 description AP300-4-BG
radio 8 bss 1 1
radio 8 bss 2 2
radio 8 bss 3 3
radio 8 channel-power indoor 6 18
radio 8 on-channel-scan
radio 8 short-preamble
```

```
 radio 8 adoption-pref-id 200
 no ap-ip default-ap switch-ip
 ap-detection enable
!
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-25-64
  radio 8 radio-mac 00-15-70-D0-26-54
!
!
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
 switchport access vlan 10
!
interface me1
```

```
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,40,
!
interface vlan1
 no ip address
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
!
rtls
 zone 1 name Office
 zone 1 perimeter x 45 y 0
 zone 1 perimeter x 80 y 0
 zone 1 perimeter x 80 y 28
 zone 1 perimeter x 64 y 28
 zone 1 perimeter x 64 y 23
 zone 1 perimeter x 45 y 23
 zone 2 name Secure Area
 zone 2 perimeter x 0 y 0
 zone 2 perimeter x 45 y 0
 zone 2 perimeter x 45 y 23
 zone 2 perimeter x 0 y 23
 zone 3 name Warehouse
 zone 3 perimeter x 0 y 23
 zone 3 perimeter x 64 y 23
 zone 3 perimeter x 64 y 28
 zone 3 perimeter x 80 y 28
 zone 3 perimeter x 80 y 60
 zone 3 perimeter x 0 y 60
 rfid
 espi
```

```
 site name Acme Inc.
 site description Acme Inc. San Jose CA
 site dimension length 80 width 60 height 18
 ap 00-15-70-D5-DA-FB coordinates x 10 y 30 z 16
 ap 00-15-70-B2-FD-CF coordinates x 50 y 50 z 16
 ap 00-15-70-78-F5-23 coordinates x 30 y 10 z 16
 ap 00-15-70-B2-FD-D0 coordinates x 75 y 20 z 8
 sole
  locate mobile-unit enable
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
end
```

D.2.5.3 Ethernet Switch Running Configuration

The following displays the core Ethernet switch running configuration:

```
! Last configuration change at 07:23:22 PST Wed Oct 22 2008
! NVRAM config last updated at 07:23:23 PST Wed Oct 22 2008
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname C3750
!
enable password symbol
!
no aaa new-model
clock timezone PST -4
switch 1 provision ws-c3750g-24ps
system mtu routing 1500
ip subnet-zero
ip routing
!
no file verify auto
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/0/1
 description INTERNET
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description DHCP SERVER
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 description RFS6000
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 description RFS7000
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
```

```
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
 description AP300-1
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/13
 description AP300-2
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/14
 description AP300-3
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/15
 description AP300-4
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/16
 description AP300-5
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
```

```
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan11
 ip address 192.168.11.1 255.255.255.0
!
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.2
ip http server
!
control-plane
!
!
line con 0
line vty 0 4
 password symbol
 login
```

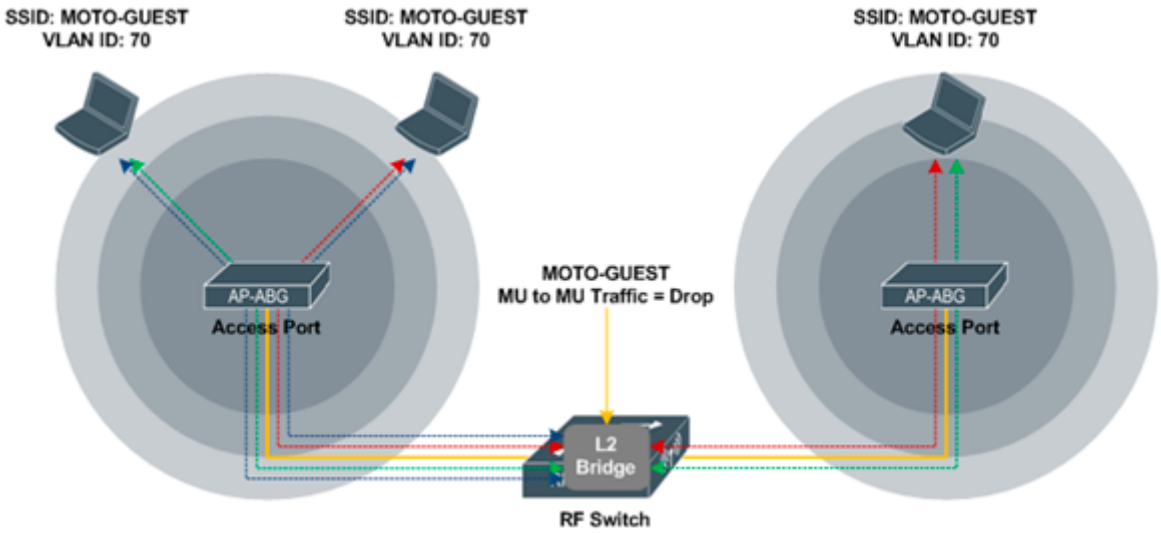
```
line vty 5 15
 login
!
ntp clock-period 36028926
ntp server 192.168.0.5 prefer
end
```

D.3 MU to MU Disallow

The MU to MU disallow feature allows the RF Switch to block communications exchanged between clients associated to a WLAN.

With the Motorola WLAN architecture, all MU traffic is forwarded to the RF Switch from adopted *Access Ports* (APs). When MUs communicate with other MUs, traffic is forwarded from the source AP to the RF Switch and then onto the AP when the destination MU resides.

The RF Switch can be configured to disallow traffic exchanged between the MUs on individual WLANs. Once enabled on a WLAN, the RF Switch will block (at layer 2) any communication attempts made between all MU MAC addresses associated to the WLAN. Unlike autonomous AP deployments, which can only block MU to MU traffic within the AP, the RF Switch can block direct MU to MU communications system-wide regardless of the AP and radio the MUs are currently associated to.



The primary application for disabling MU to MU communications is a hotspot, using guest user designations. Since user devices within a hotspot are typically un-managed, disabling MU to MU communications protects MUs from other MUs that could be infected with worms and viruses. Additionally, disabling MU to MU communications also protects devices malicious attacks from other MUs and prevents undesired peer-to-peer file sharing and on-line gaming from dominating bandwidth.

The MU to MU disallow feature will only block communications exchanged between MUs on the same WLAN, and does not block MU to MU communications between MUs associated on different WLANs and subnets. To block communications between MUs associated on different WLANs or subnets, the integrated stateful firewall must be used.

D.3.1 Defining an MU to MU Disallow Configuration

The following sections outline the requirements, components and steps required to disable MU to MU communications for a WLAN configured on a RF Switch.

To view the running configuration on the RFS6000 switch used to create this MU to MU disallow tutorial, refer to *RF Switch Running Configuration on page D-40*.

D.3.1.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One (or more) RF Switches are installed and operational on the network
- One (or more) Access Ports configured and adopted by the RF Switch
- One (or more) WLAN profiles are configured and assigned to adopted radios
- A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration
- Two wireless workstations are available to test and verify MU to MU communications

D.3.1.2 Components

The information in this section is based on the following Motorola hardware and software versions:

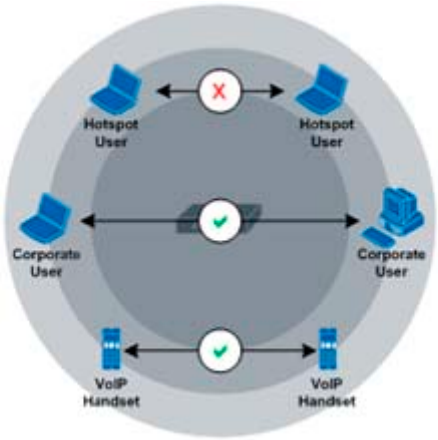
- 1 RFS6000 model switch
- 5 AP300 model Access Ports

D.3.1.3 Switch Web UI Configuration

The following configuration example demonstrates how to disable MU to MU communications for a WLAN:

As illustrated in the figure below, three WLANs have been created at a site. MOTO-DATA and MOTO-VOICE are corporate WLANs providing data and voice services to corporate users and VoIP handsets. MOTO-GUEST is a hotspot WLAN providing guest access to visitors and contractors.

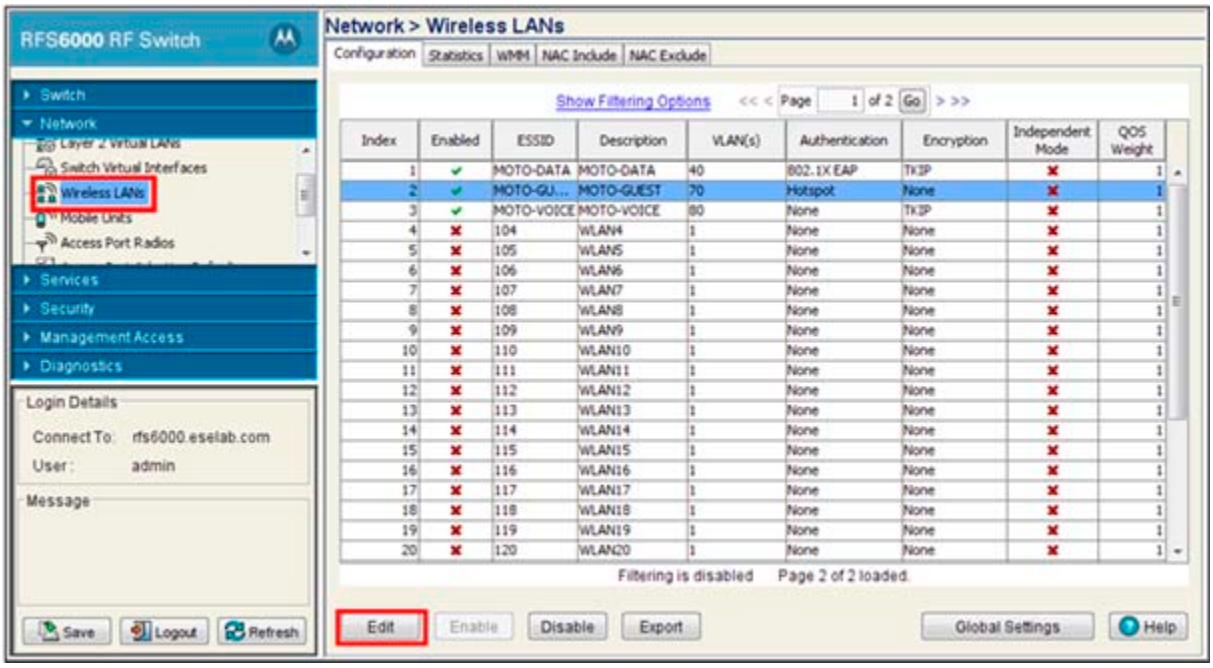
In this example, the company has deployed VoIP handsets and converged communication clients with instant messaging and voice communications potentially occurring between any wired or WLAN client. As a result, MU to MU traffic on MOTO-DATA and MOTO-VOICE WLANs will be allowed so it will not impact instant messaging or voice communications. On MOTO-GUEST, MU to MU traffic is disallowed since MOTO-GUEST is an isolated network servicing visitors and contractors who do not require direct client to client communications.



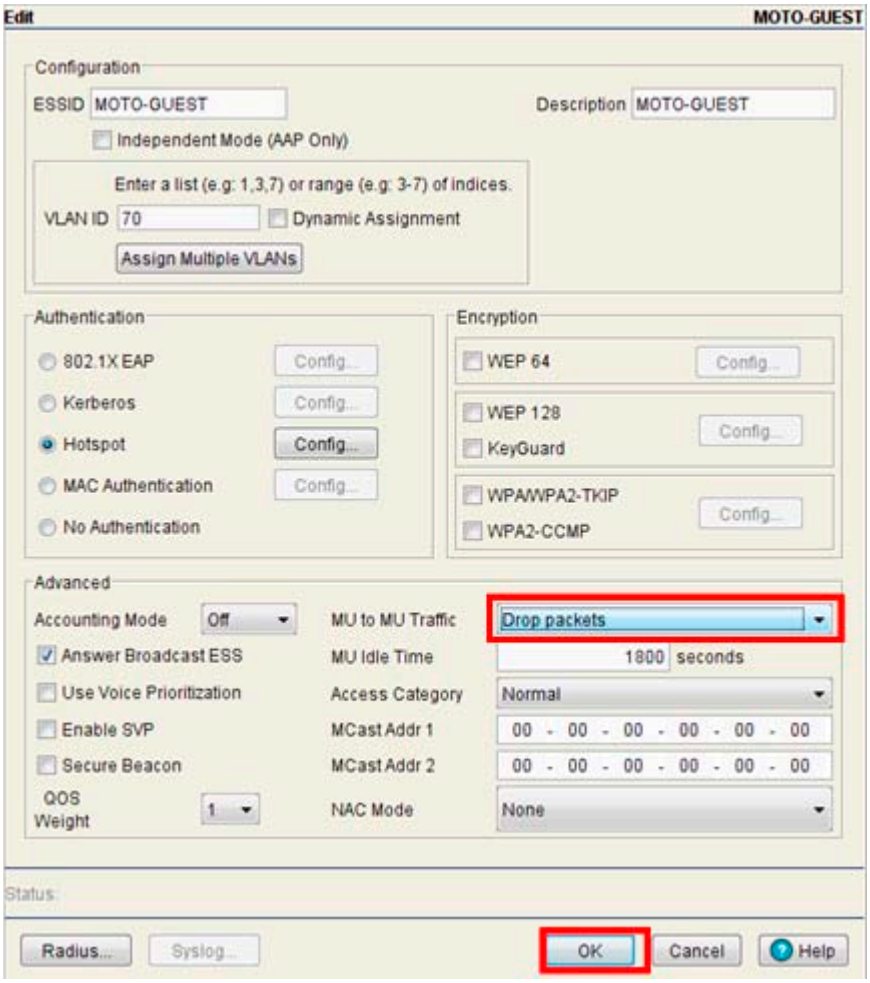
SSID	*Authentication*	*Encryption*	*MU-MU Traffic*
MOTO-DATA	802.1x	WPA2-CCMP	Allow
MOTO-GUEST	Hotspot	None	Drop
MOTO-VOICE	PSK	WPA2-CCMP	Allow

To disable MU to MU communications:

1. From the switch menu tree select **Network** > **Wireless LANs.**
2. Select the **Configuration** tab.



3. Select an available SSID (to modify) and select the **Edit** button.



4. Change the default **MU to MU Traffic** option from Allow Packets to **Drop Packets**.

   This will disable MU to MU communications for all users associated with the SSID. Click **OK**.

5. Select **Save** (from the lower left-hand corner) to apply the changes.

D.3.2 RF Switch Running Configuration

The following is the running configuration on the RFS6000 switch used to create this MU to MU disallow tutorial:

```
RFS6000# show running-config
!
! configuration of RFS6000 version 3.3.0.0-029R
!
version 1.2
!
!
aaa authentication login default local none
service prompt crash-info
!
```

```
username "admin" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc."
"WLAN Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
timezone America/New_York
service radius
```

```
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d04677
7fbed80f433b68ea
!
wireless
 secure-wispe-default-secret 0 defaultS
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
 wlan 1 dot11i preauthentication
 wlan 2 enable
 wlan 2 description MOTO-GUEST
 wlan 2 ssid MOTO-GUEST
 wlan 2 vlan 70
 wlan 2 authentication-type hotspot
 wlan 2 mu-mu-disallow
 wlan 2 hotspot webpage-location advanced
 wlan 2 radius server primary 192.168.10.14
 wlan 2 radius server primary radius-key 0 ESELAB
 wlan 2 radius accounting server primary 192.168.10.14
 wlan 2 radius accounting server primary radius-key 0 ESELAB
 wlan 3 enable
 wlan 3 description MOTO-VOICE
 wlan 3 ssid MOTO-VOICE
 wlan 3 vlan 80
 wlan 3 encryption-type tkip
 wlan 3 dot11i phrase 0 motovoicetest
 wlan 3 dot11i preauthentication
 radio add 1 00-15-70-78-F5-23 11a ap300
 radio 1 description AP300-1-A
 radio 1 bss 1 1
 radio 1 channel-power indoor 36 15
 radio 1 on-channel-scan
```

```
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
radio 5 description AP300-3-A
radio 5 bss 1 1
radio 5 channel-power indoor 44 15
radio 5 on-channel-scan
radio 5 adoption-pref-id 100
radio add 6 00-15-70-B2-FD-D0 11bg ap300
radio 6 description AP300-3-BG
radio 6 bss 1 1
radio 6 bss 2 2
radio 6 bss 3 3
radio 6 channel-power indoor 11 18
radio 6 on-channel-scan
radio 6 short-preamble
radio 6 adoption-pref-id 100
radio add 7 00-15-70-D5-DA-CE 11a ap300
radio 7 description AP300-4-A
radio 7 channel-power indoor 48 17
```

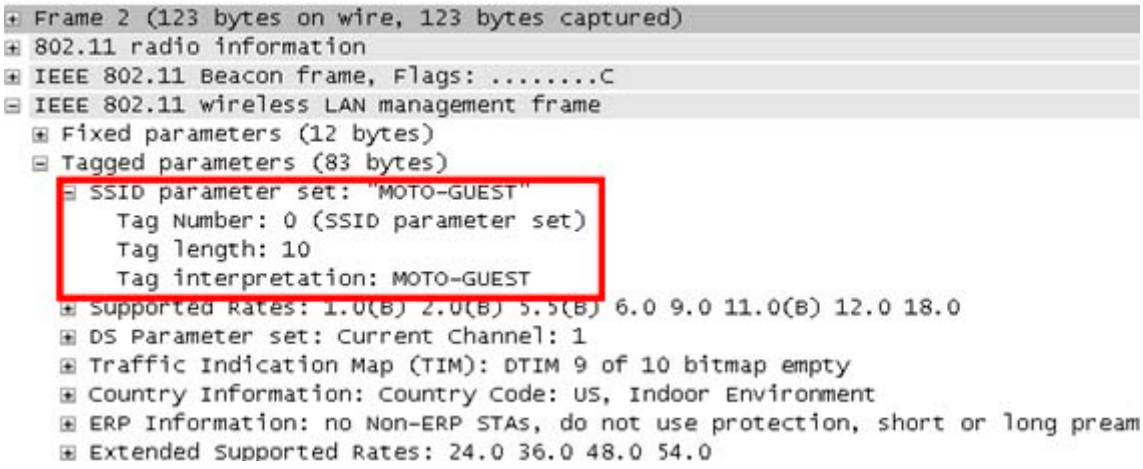
```
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 radio add 9 00-15-70-D5-DA-FB 11a ap300
 radio 9 description AP300-5-A
 radio 9 channel-power indoor 149 20
 radio 9 on-channel-scan
 radio add 10 00-15-70-D5-DA-FB 11bg ap300
 radio 10 description AP300-5-BG
 radio 10 channel-power indoor 6 4
 radio 10 on-channel-scan
 no ap-ip default-ap switch-ip
 ap-detection enable
!
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
!
radius-server local
 authentication eap-auth-type all
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
```

```
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
switchport access vlan 10
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
interface vlan1
 no ip address
 shutdown
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
!
interface vlan70
 description GUEST
 ip address 192.168.70.14/24
!
!
```

```
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
end
```

D.4 Secure Beacons

Secure beacons allows a SSID name to be masked for a WLAN (in the beacon) so MUs are unable to see or view the SSID. MUs discover WLAN services by listening to beacons advertised from APs. An AP advertises a beacon (10 per second) for each WLAN service enabled on the radio which includes specific information about the WLAN service. Each beacon is forwarded in clear text and includes a *Service Set Identifier* (SSID) name for the WLAN. The SSID must be known by the MU before the MU can associate to the WLAN.



Default Beacon Frame Example

```
⊞ Frame 2 (114 bytes on wire, 114 bytes captured)
⊞ 802.11 radio information
⊞ IEEE 802.11 Beacon frame, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (74 bytes)
    ⊟ SSID parameter set: "\000"
        Tag Number: 0 (SSID parameter set)
        Tag length: 1
        Tag interpretation:
    ⊞ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 6.0 9.0 11.0(B) 12.0 18.0
    ⊞ DS Parameter set: Current Channel: 1
    ⊞ Traffic Indication Map (TIM): DTIM 9 of 10 bitmap empty
    ⊞ Country Information: Country Code: US, Indoor Environment
    ⊞ ERP Information: no Non-ERP STAs, do not use protection, short or long pream
    ⊞ Extended Supported Rates: 24.0 36.0 48.0 54.0
```

Secure Beacon Frame Example

With certain applications (such as a hotspot uses guest access), it may be desirable to mask the SSID name to make it harder for casual eavesdroppers to discover the SSID and connect to a WLAN. It is not recommended secure beacons be used for real-time applications (such a Voice) requiring fast roaming.

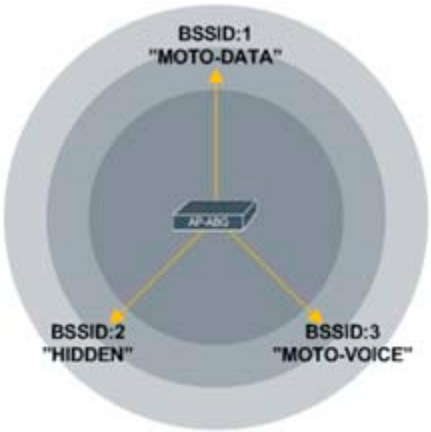
The SSID name is not intended as a password and should not be used as one. If security is required, the appropriate authentication and encryption should be used. While secure beacon can be used to mask the SSID in the beacon, the SSID name can still be discovered by monitoring probe response frames.

D.4.1 Configuring a Secure Beacon Deployment

The following sections outline the configuration steps required to enable secure beacon for a WLAN on an RF Switch:

To view the running configuration on the RFS6000 switch used to create this secure beacon tutorial, refer to *RF Switch Running Configuration on page D-49*.

As shown in the illustration below, enabling secure beacon prevents the SSID being advertised in the beacon frame. WLAN clients scanning for WLAN services display the SSID as blank. Clients wishing to associate with the WLAN have to specify the correct SSID in their client software before the client associates to the WLAN.



BSSID	*SSID*	*Secure Beacon*
1	MOTO-DATA	Disabled
2	MOTO-GUEST	Enabled
3	MOTO-VOICE	Disabled

CAUTION: The SSID is not designed nor intended as a security mechanism. Motorola does not recommend using the SSID as a mode of security.

CAUTION: Disabling SSID broadcasts may have adverse effects on Wi-Fi interoperability for mixed-client deployments. In addition disabling the SSID in the beacon is not recommended for WLANs providing real-time services (such as VoIP) as roaming can be impacted.

D.4.1.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One or more RF Switches are installed and operational on the network
- One or more AP300 Access Ports configured and adopted by the switch
- One (or more) WLAN profiles are configured and assigned to adopted radios
- A Windows XP workstation with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration and verify secure network management
- One (or more) wireless workstations are available to verify the SSID in the beacon is disabled

D.4.1.2 Components

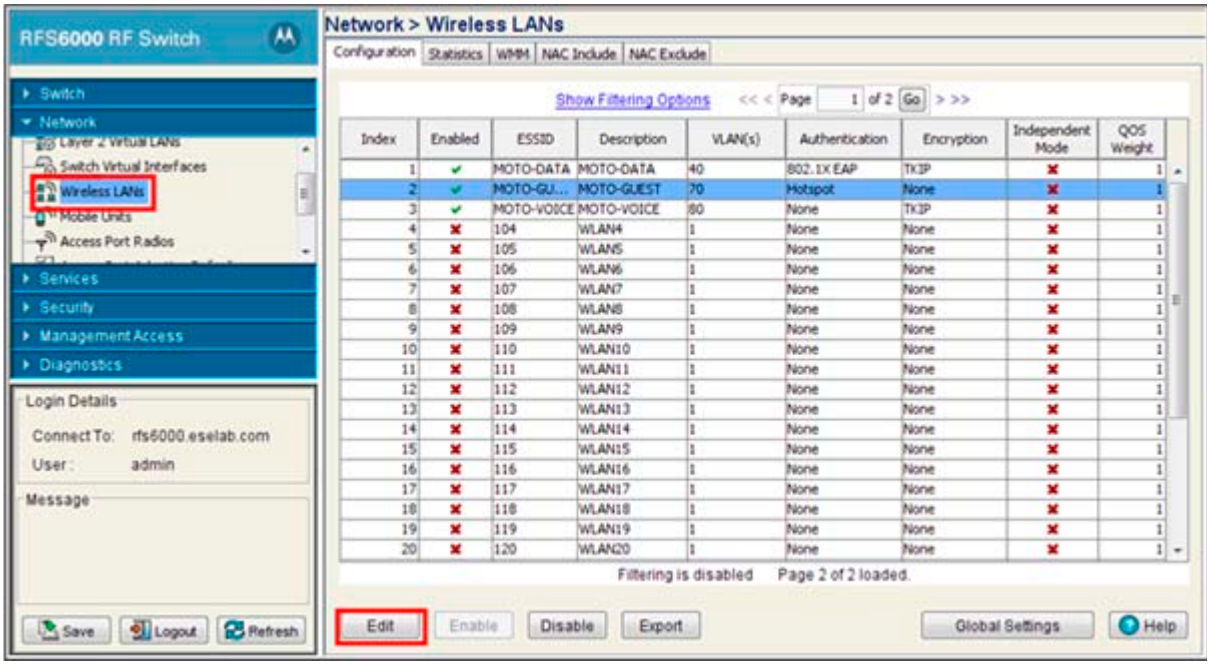
The information in this section is based on the following Motorola hardware and software versions:

- 1 RFS6000 model switch
- 5 AP300 model Access Ports

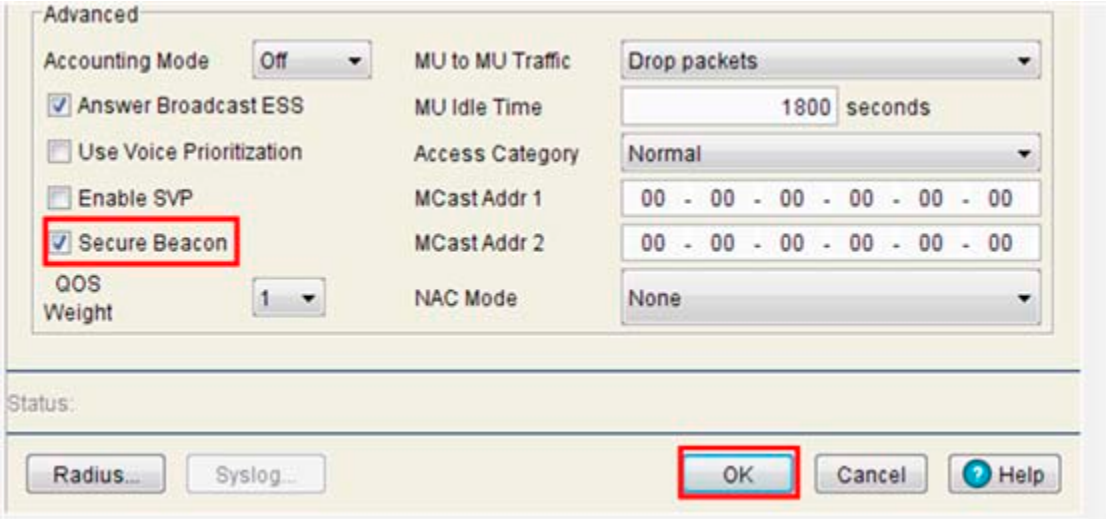
D.4.1.3 Switch Web UI Configuration

The following configuration example demonstrates how to enable Secure Beacon on a hotspot SSID named MOTO-GUEST:

1. From the switch menu tree select **Network** > **Wireless LANs.**
2. Select the **Configuration** tab.



3. Highlight a SSID to modify and select **Edit**.



4. Select the **Secure Beacon** checkbox.

   This disables the SSID advertised in the beacon. Click **OK**.

5. Select **Save** (from the lower left-hand corner) to apply the changes.

D.4.2 RF Switch Running Configuration

The following is the running configuration on the RFS6000 switch used to create this secure beacon tutorial:

```
RFS6000# show running-config
!
! configuration of RFS6000 version 3.3.0.0-029R
!
```

```
version 1.2
!
!
aaa authentication login default local none
service prompt crash-info
!
username "admin" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc."
"WLAN Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
```

```
ip telnet
no service pm sys-restart
timezone America/New_York
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d04677
7fbed80f433b68ea
!
wireless
 secure-wispe-default-secret 0 defaultS
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
 wlan 1 dot11i preauthentication
 wlan 2 enable
 wlan 2 description MOTO-GUEST
 wlan 2 ssid MOTO-GUEST
 wlan 2 vlan 70
 wlan 2 authentication-type hotspot
 wlan 2 secure-beacon
 wlan 2 hotspot webpage-location advanced
 wlan 2 radius server primary 192.168.10.14
 wlan 2 radius server primary radius-key 0 ESELAB
 wlan 2 radius accounting server primary 192.168.10.14
 wlan 2 radius accounting server primary radius-key 0 ESELAB
 wlan 3 enable
 wlan 3 description MOTO-VOICE
 wlan 3 ssid MOTO-VOICE
 wlan 3 vlan 80
 wlan 3 encryption-type tkip
 wlan 3 dot11i phrase 0 motovoicetest
 wlan 3 dot11i preauthentication
 radio add 1 00-15-70-78-F5-23 11a ap300
```

```
radio 1 description AP300-1-A
radio 1 bss 1 1
radio 1 channel-power indoor 36 15
radio 1 on-channel-scan
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
radio 5 description AP300-3-A
radio 5 bss 1 1
radio 5 channel-power indoor 44 15
radio 5 on-channel-scan
radio 5 adoption-pref-id 100
radio add 6 00-15-70-B2-FD-D0 11bg ap300
radio 6 description AP300-3-BG
radio 6 bss 1 1
radio 6 bss 2 2
radio 6 bss 3 3
radio 6 channel-power indoor 11 18
radio 6 on-channel-scan
radio 6 short-preamble
```

```
 radio 6 adoption-pref-id 100
 radio add 7 00-15-70-D5-DA-CE 11a ap300
 radio 7 description AP300-4-A
 radio 7 channel-power indoor 48 17
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 radio add 9 00-15-70-D5-DA-FB 11a ap300
 radio 9 description AP300-5-A
 radio 9 channel-power indoor 149 20
 radio 9 on-channel-scan
 radio add 10 00-15-70-D5-DA-FB 11bg ap300
 radio 10 description AP300-5-BG
 radio 10 channel-power indoor 6 4
 radio 10 on-channel-scan
 no ap-ip default-ap switch-ip
 ap-detection enable
!
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
!
radius-server local
 authentication eap-auth-type all
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
interface ge1
 switchport access vlan 10
```

```
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
switchport access vlan 10
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
interface vlan1
 no ip address
 shutdown
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
!
interface vlan70
```

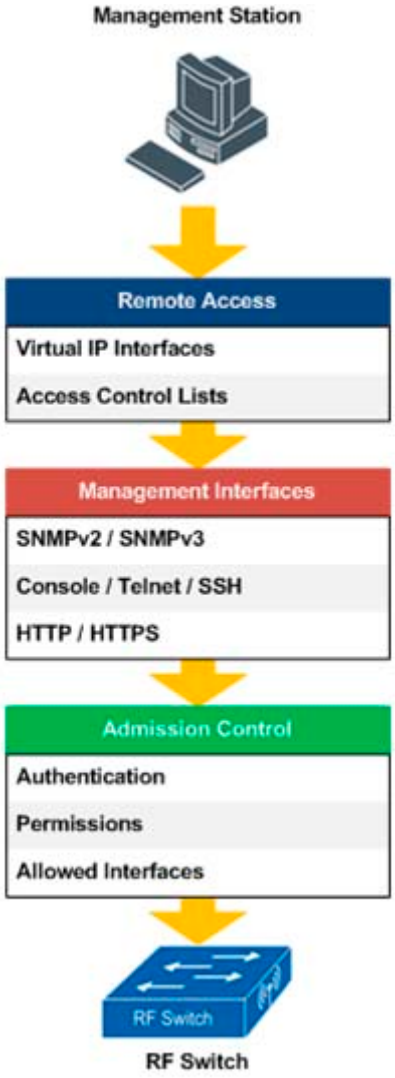
```
 description GUEST
 ip address 192.168.70.14/24
!
!
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
end
```

D.5 Secure Device Management

A RF Switch can be managed by multiple interfaces, including SNMP, CLI and Web UI. By default, management access to the RF Switch is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security on the RF Switch, administrators can apply various restrictions as needed that can be used to:

- Restrict SNMP, CLI and Web UI access to a specific IP interface
- Restrict SNMP, CLI and Web UI access to specific hosts or subnets
- Disable un-used or insecure management interfaces
- Provide authentication for management users
- Apply access restrictions and permissions to management users based on identity



Management restrictions can be applied to meet specific company policies or industry requirements mandating only certain devices or staff be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of a device when guest credentials are used.

D.5.1 Configuring a Secure Device Deployment

The following sections outline the configuration steps required to restrict management access on an RF Switch:

- *Restricting Management Access*
- *Disabling Insecure Management Interfaces*
- *Management User Authentication*

To view the running configuration on the RFS6000 switch used to create this secure device management tutorial, refer to *RF Switch Running Configuration on page D-68*.

D.5.1.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One or more RF Switches are installed and operational on the network
- One or more AP300 Access Ports configured and adopted by the switch
- One (or more) WLAN profiles are configured and assigned to adopted radios
- A Windows XP workstation with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration and verify secure network management

D.5.1.2 Components

The information in this section is based on the following Motorola hardware and software versions:

- 1 RFS6000 model switch

D.5.1.3 Restricting Management Access

Restricting remote access to the RF Switch ensures only trusted hosts can communicate with enabled management services on the switch. This ensures only trusted hosts can perform management tasks and provide protection from brute force attacks from hosts attempting to break into the switch.

Secure Management

By default, management connections can be established with any enabled IP interface on the RF Switch, including IP interfaces used to provide hotspot guest services. Management access can be restricted by limiting management access to a specific IP interface on the RF Switch.

1. The first step for securing management access is selecting a management IP interface. For security, it is a best practice to use a dedicated VLAN which has limited (or no) access from WLAN devices.
2. The second step for securing management access, is enabling the secure management feature. The secure management feature will restrict management access to only the management IP interface.

Interface	*Description*	*IP Address*	*Management*
vlan10	SERVICES	192.168.10.14/24	Yes
vlan70	GUEST	192.168.70.14/24	No

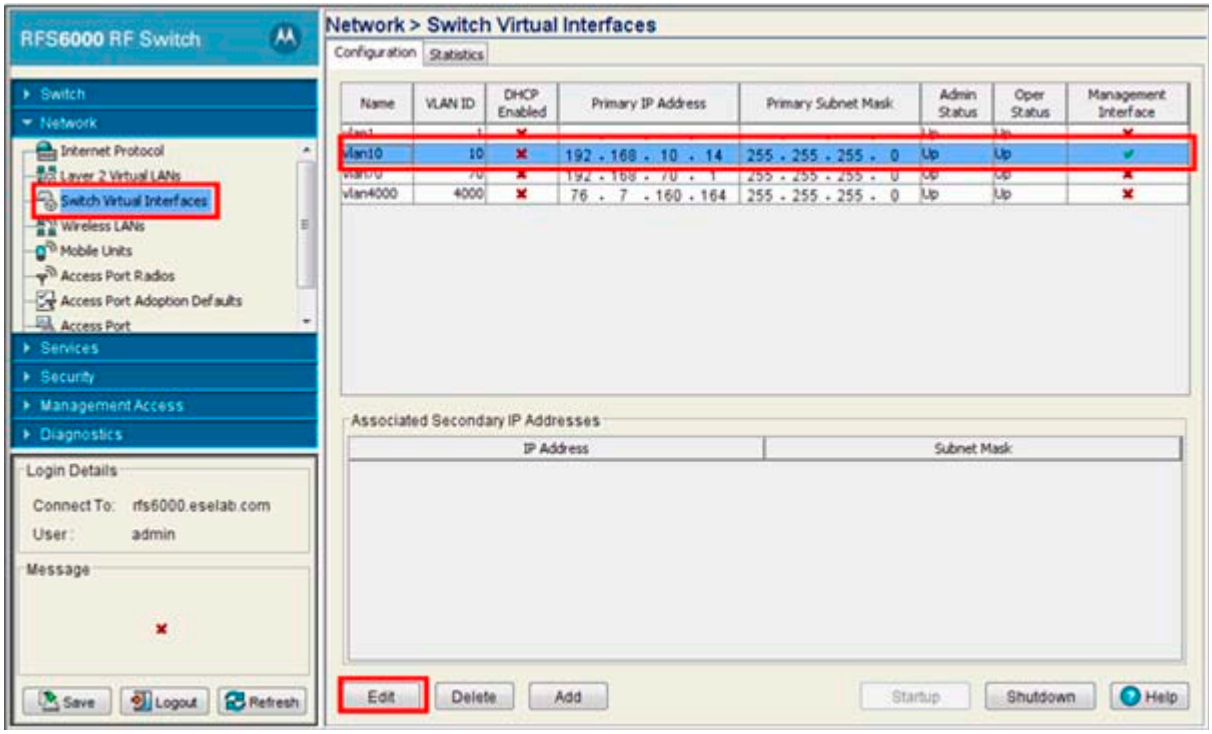
As shown in the figure above, the RF Switch has two IP interfaces defined, vlan10 hosting management and network services and vlan70 providing guest services. For security, the guest network is separated from all trusted VLANs by a firewall.

In this scenario, by default, RF Switch management services are accessible on both interface vlan10 and interface vlan70. This is not desirable. By selecting interface vlan10 as the management interface and enabling secure management, the RF Switch only accepts management sessions on interface vlan10. Management access from vlan70 is no longer available.

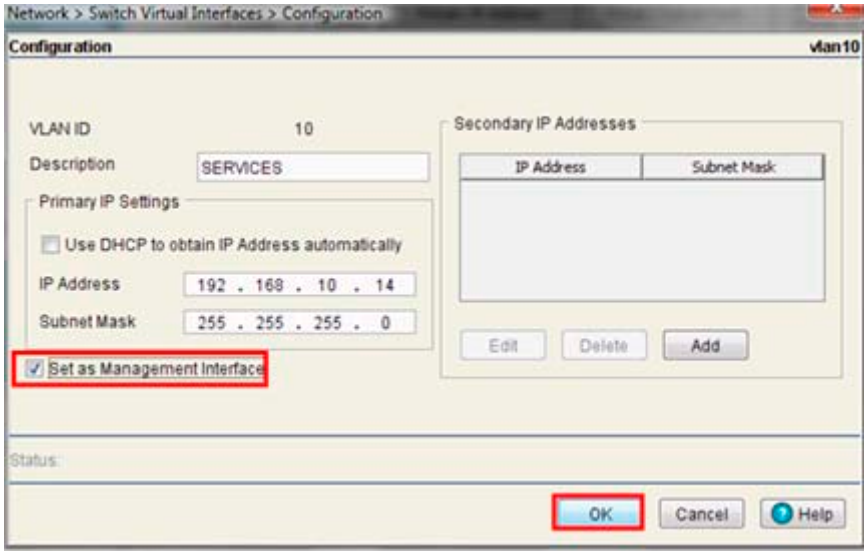
Switch Web UI Configuration

The following configuration example demonstrates how to define a management IP interface and enable secure management:

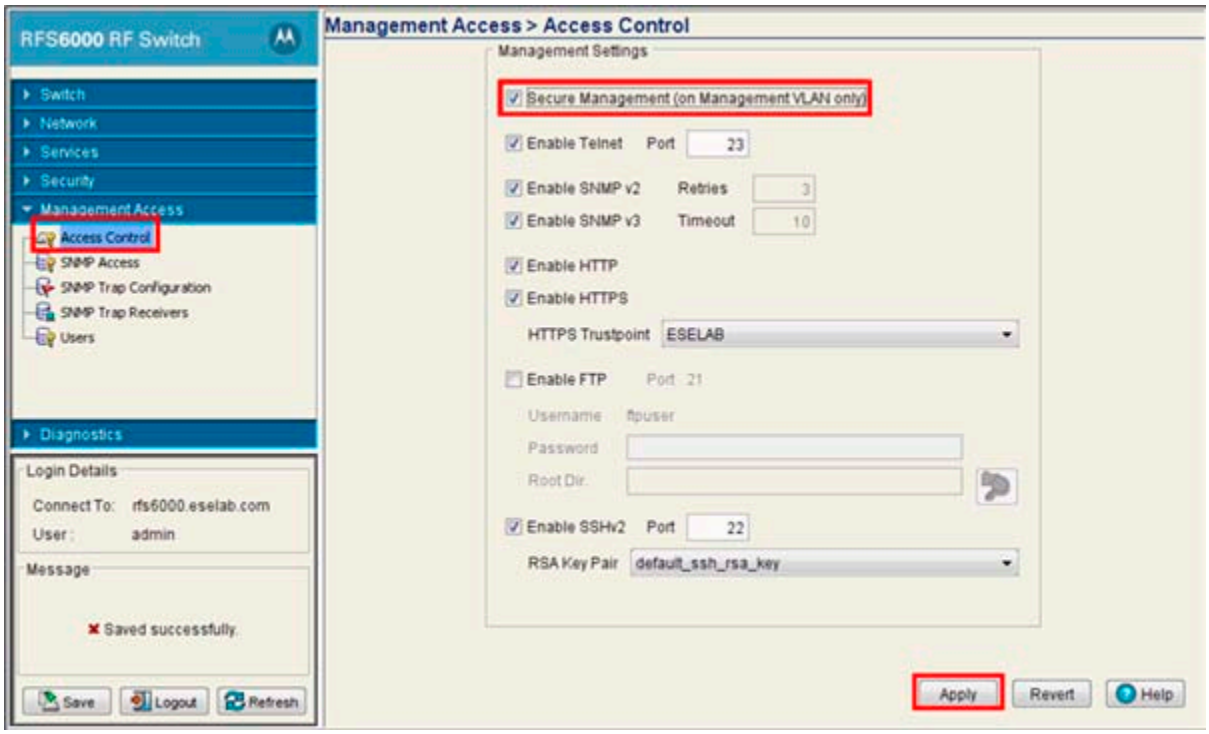
1. From the switch menu tree select **Network** > **Switch Virtual Interface.**
2. Select the **Configuration** tab.
3. Highlight the interface used for management and select **Edit**.



4. Select the **Set as Management** Interface checkbox.



5. Click **OK.**
6. From the switch menu tree select **Management Access** > **Access Control.**

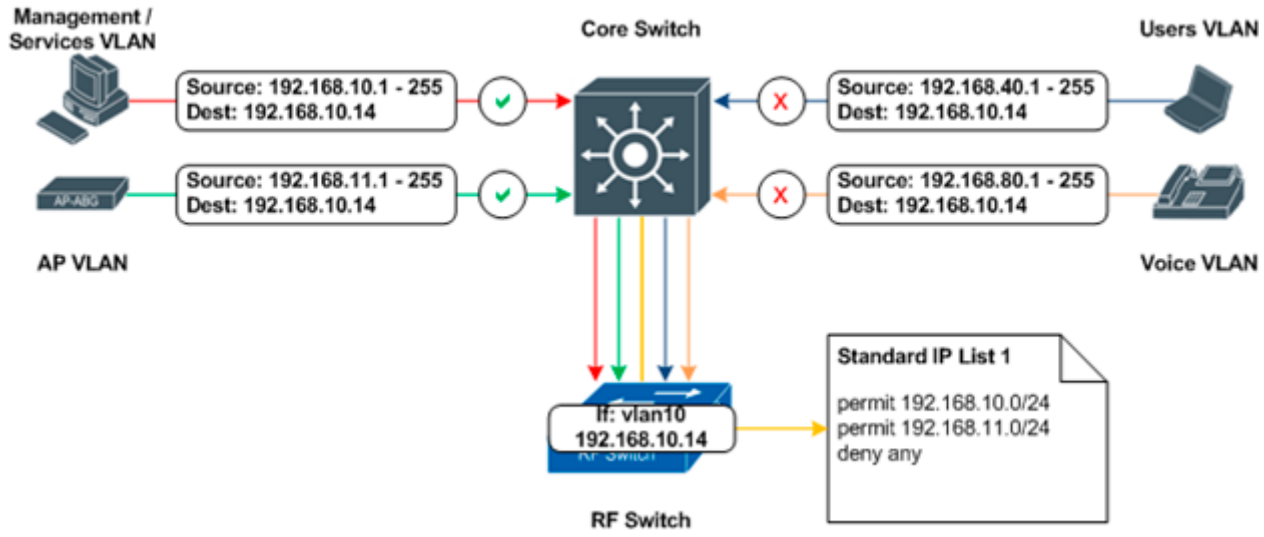


7. Select the **Secure Management (on Management VLAN only)** checkbox then click **Apply.**
8. Select **Save** (from the lower left-hand corner) to apply the changes.

Access Control Lists

Secure management is an effective way to limit management access to a specific IP interface on the RF Switch. However secure management does not restrict access to specific hosts or VLANs which have IP access through a router or routing switch.

Management access can be further restricted by creating an *Access Control List* (ACL) and applying the ACL to the management interface to allow access from specific hosts or subnets. The ACL can be customized to suit the specific environment, and can either be a standard IP or extended IP ACL.

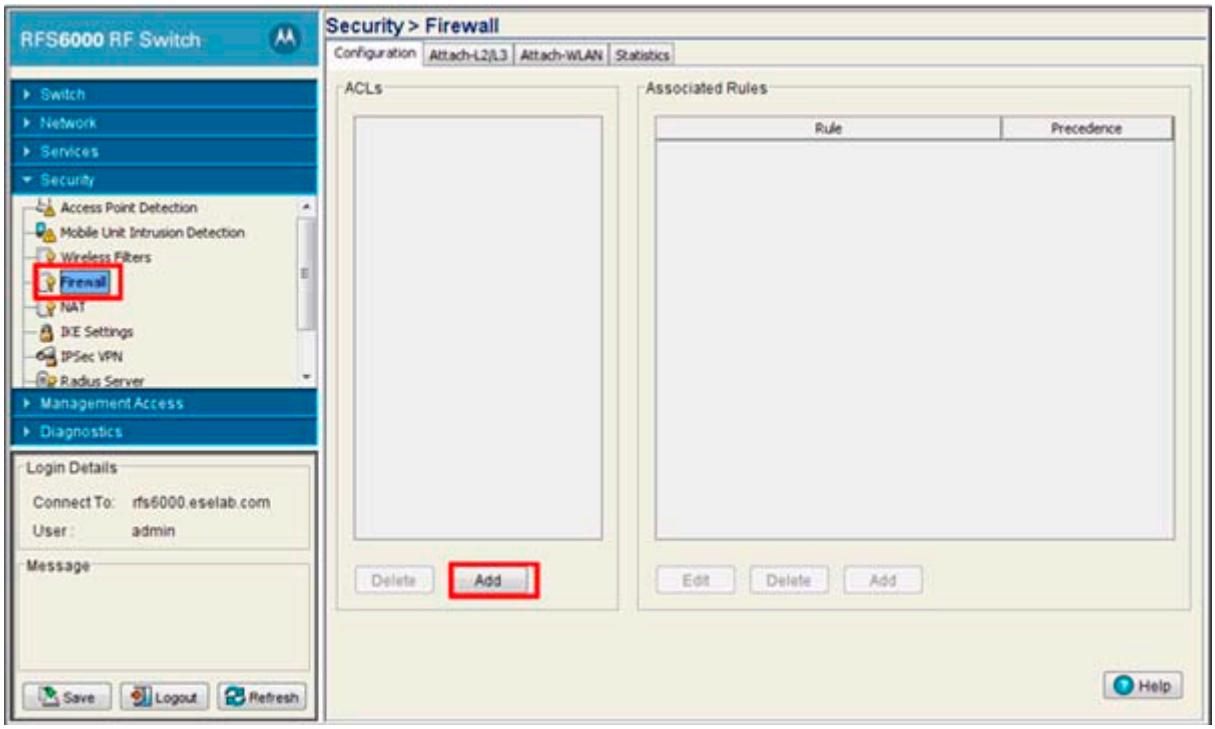


The RF Switch has a standard IP ACL applied to interface vlan10 which permits IP access from the Services / Management and Access Point subnets but denies access from all other subnets. This example provides IP access for management servers, clients and APs while restricting access to all other users and devices.

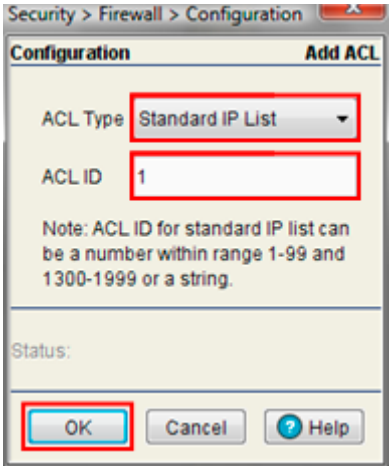
Switch Web UI Configuration

The following demonstrates how to create a standard IP ACL and apply it to the management IP interface:

1. From the switch menu tree select **Security** > **Firewall.**
2. Select the **Configuration** tab.

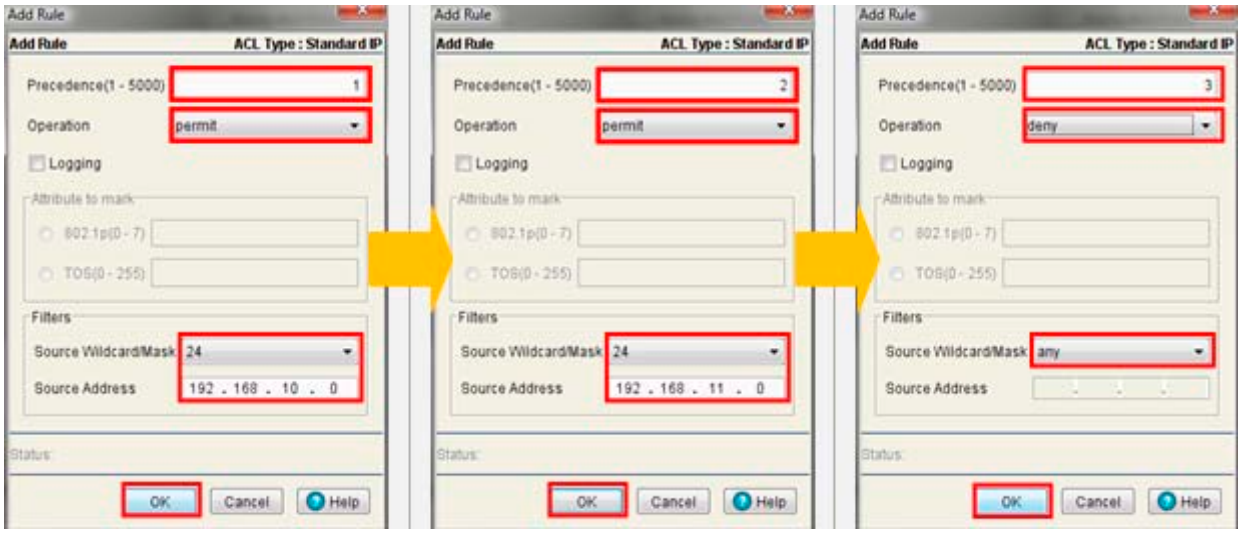


3. Click **Add.**



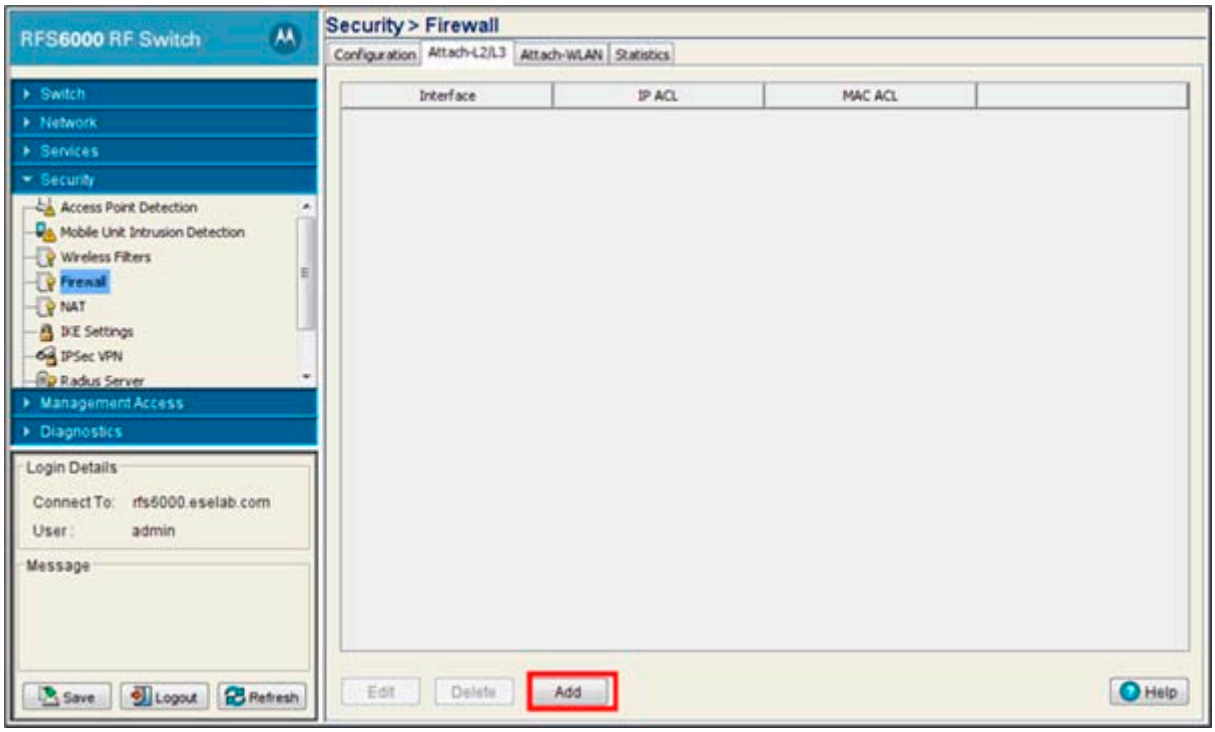
4. Select **Standard IP List** from the ACL Type drop-down menu.
5. Enter an **ACL ID** (1-99) and click **OK**.

6. From back in the Configuration tab, select the ACL created in steps 3 and 4
7. Click **Add** under the Associated Rules field.
8. Within the **Add Rule** window, create the first required permit rule for the subnet or host then click **OK**.

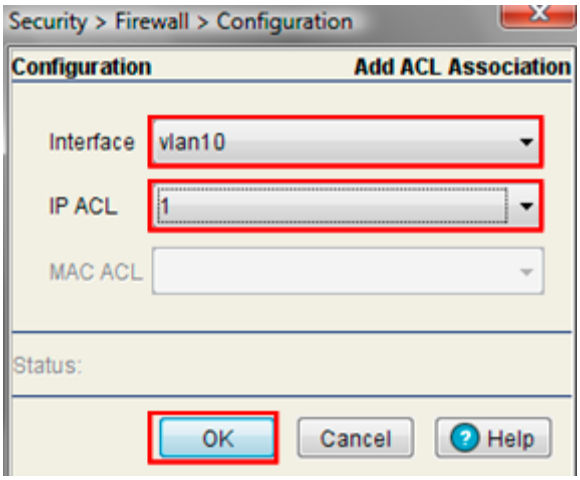


Create additional permit rules as required.

9. Lastly, create the deny rule to deny access to all other hosts and click **OK**.
10. From back at the **Security** > **Firewall** screen, select the **Attach-L2/L3** tab click **Add**.



11. Select the management **Interface**.



12. Select the **IP ACL** you created previously. Click **OK**.
13. Select **Save** (from the lower left-hand corner) to apply the changes.

D.5.1.4 Disabling Insecure Management Interfaces

Network administrators can secure management access to the RF Switch by disabling less secure management interfaces. By default, the switch enables all CLI, SNMP and Web UI management interfaces, of which some do not support encryption or authentication. Security best practices recommend (and certain regulations require) insecure management interfaces (such as Telnet, HTTP and SNMP) be disabled, and only secure management interfaces be used to manage the infrastructure.

The table below shows available management interfaces, encryption and authentication capabilities default states. Again, all management interfaces (except for FTP) are enabled by default.

Management Service	***Encrypted***	***Authenticated***	***Default State***
Telnet	No	Yes	Enabled
SNMP v2	No	No	Enabled
SNMP v3	Yes	Yes	Enabled
HTTP	No	Yes	Enabled
HTTPS	Yes	Yes	Enabled
FTP	No	Yes	Disabled
SSH v2	Yes	Yes	Enabled

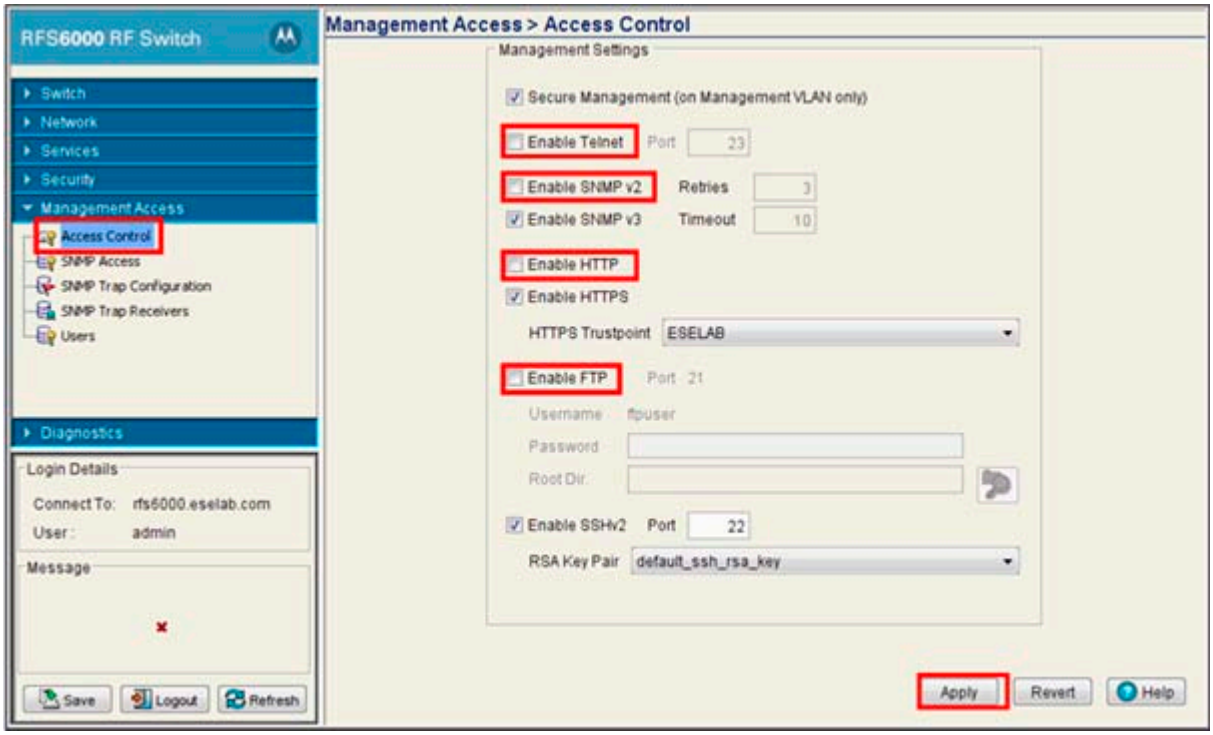
Industry best practice recommendations include:

- Any un-used management interfaces should be disabled. For example, if a device is only being managed by the Web UI and SNMP, there is no need to enable the CLI interface.
- Only use management interfaces that provide encryption and authentication. For example, if CLI access is required, SSHv2 should be used over Telnet.
- If less secure management access is required, access should be restricted to specific hosts and interfaces by leveraging the Secure Management feature and ACLs.

Switch Web UI Configuration

The following demonstrates how to disable insecure telnet, HTTP and SNMPv2 management interfaces:

1. From the switch menu tree select **Management Access** > **Access Control.**



2. Select the **Enable Telnet**, **Enable SNMP v2**, **Enable HTTP** and **Enable FTP** checkboxes.
3. Click **Apply** button.
4. Select **Save** (from the lower left-hand corner) to apply the changes.

D.5.1.5 Management User Authentication

Management services (Telnet, SSHv2, HTTP, HTTPs and FTP) require administrators provide a valid username and password which can be authenticated locally on the RF Switch or centrally on a Radius server. SNMPv3 also requires a valid username and password from a management platform (such as RFMS, which is authenticated by the SNMPv3 module).

For CLI and Web UI users, the RF Switch also requires role information for the user to know what permissions to assign the session:

- If local authentication is used, associated role information is defined on the RF Switch when the user account is created.
- If Radius authentication is used, role information is supplied to the Radius server. If no role information is supplied, the RF Switch can apply default read-only permissions for the management session.

Administrators can also limit management users to specific management interfaces. During authentication, the RF Switch looks at access mode assignments for the user ID to determine if the user has permissions to access the requested management interface:

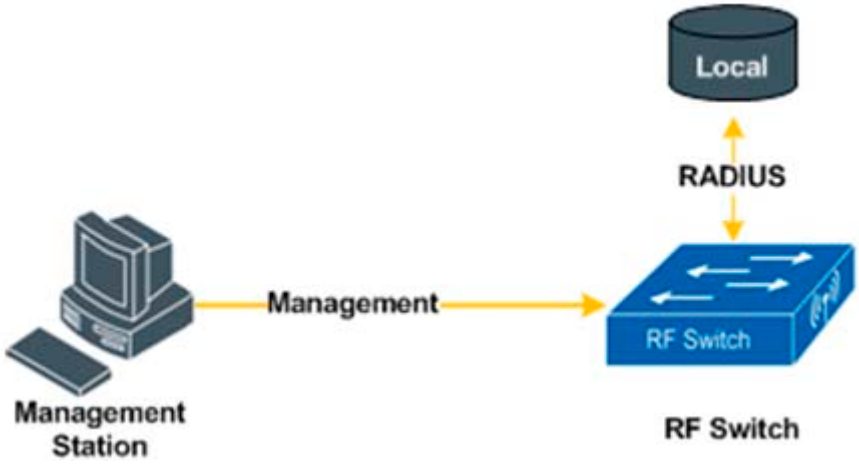
- If local authentication is used, role information is defined on the RF Switch when the user account is created.

- If Radius authentication is used, associated role information is supplied to the Radius server, except when using vendor specific return attributes.

For availability, the RF Switch also supports multiple Radius server definitions and fallback to provide authentication in the event of failure or communication issues. If the primary Radius server is unavailable, the RF Switch attempts authentication with the next RADIUS sever. If no Radius servers are available, the RF Switch can fall back to its local database for authentication. In both the Radius server and local authentication services are unavailable, read-only access can be optionally provided.

Local Management Authentication

By default, the RF Switch authenticates management users with its integrated local database. When management user credentials are presented, the RF Switch validates the username and passwords against its local database and assigns permissions based on associated roles assigned to the account. The RF Switch can also deny authentication requests if the user is attempting to access a management interface not specified in the accounts access mode list.



Associated roles can be assigned to management user accounts to determine switch access privileges. Management users can be assigned a single role, such as a Monitor that provides read-only access, or multiple roles such as Monitor and Web User which provides read-only access in addition to hotspot user creation. The following table lists the supported associated roles supported by the RF Switch:

Associated Role	***Description***
Monitor	Assigns regular user permissions without any administrative rights (read-only).
Help Desk	Provides permissions for someone who typically troubleshoots and debugs problems reported by the customer. The Help Desk Manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the switch.
Network	Provides privileges to configure all wired and wireless parameters like IP configuration, VLANs, L2/L3 security, WLANs, radios, IDS and hotspot.
System Administrator	Provides permissions to configure general settings like NTP, boot parameters, licenses, perform image upgrades, auto install, manager redundancy/clustering and control access.

Associated Role	Description
Web User	Provides privileges to add users for Hotspot authentication.
Super User	Provides full administrative access rights.

Access modes can be assigned to management user accounts to restrict the management interfaces a user can access. As with associated roles, a management user can be assigned a single access role to restrict access to a specific management interface or assign multiple access roles to allow access to multiple management interfaces.

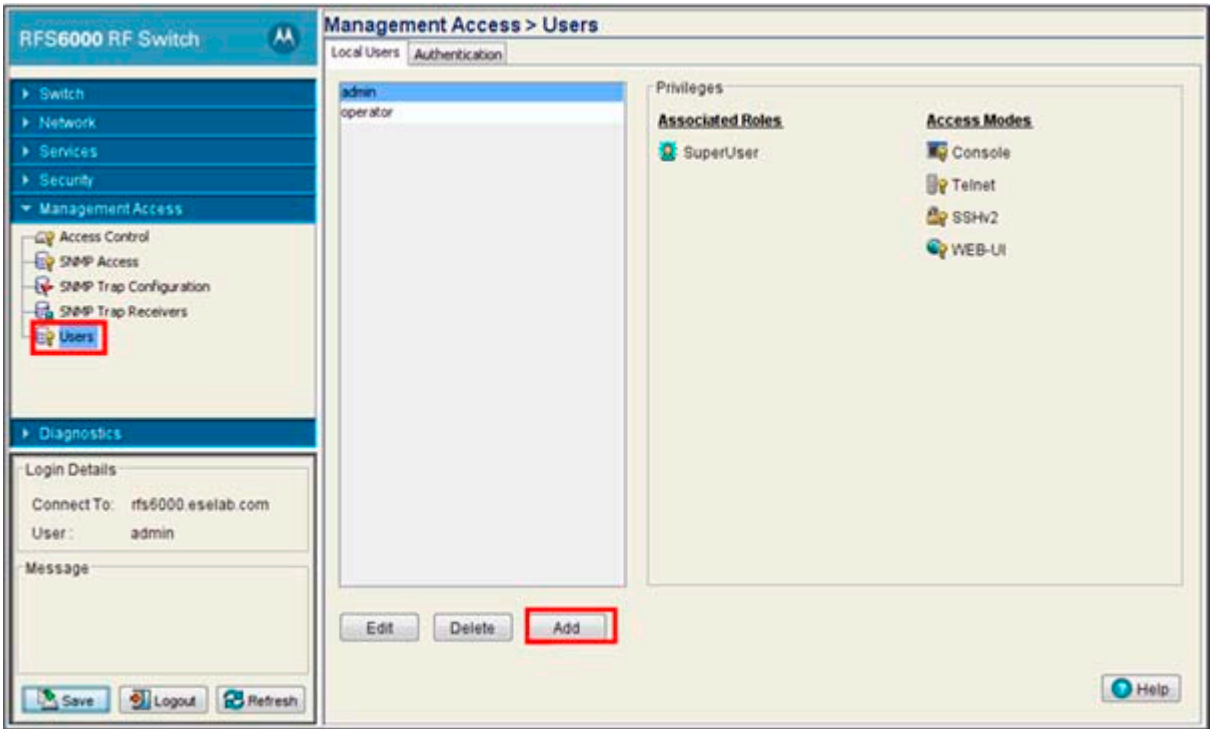
The following table lists the supported access modes supported by the RF Switch:

Access Mode	Description
Console	Provides management access to the switch using the console
Telnet	Provides management access to the switch using Telnet
SSH	Provides management access to the switch using SSH
Web UI (applet)	Provides management access to the switch using HTTP or HTTPS

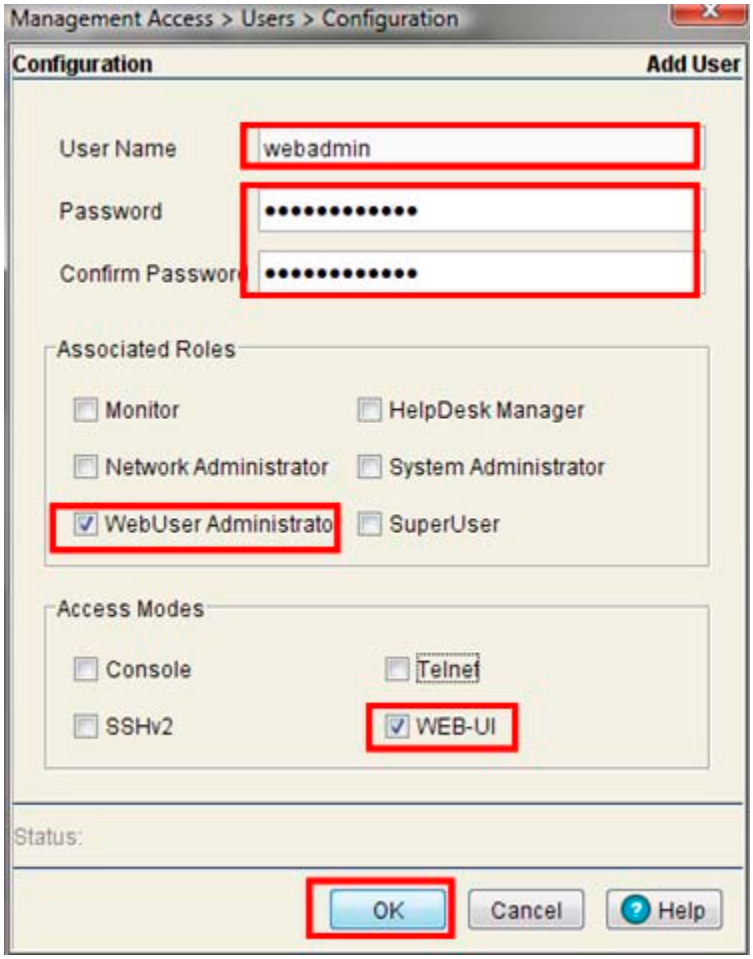
Switch Web UI Configuration

The following demonstrates how to create a local management user with webadmin privileges and Web UI management access:

1. From the switch menu tree select **Management Access** > **Users.**
2. Select the **Local Users** tab (if not already selected).



3. Click the **Add** button.
4. Provide the required **Username** and **Password** information.



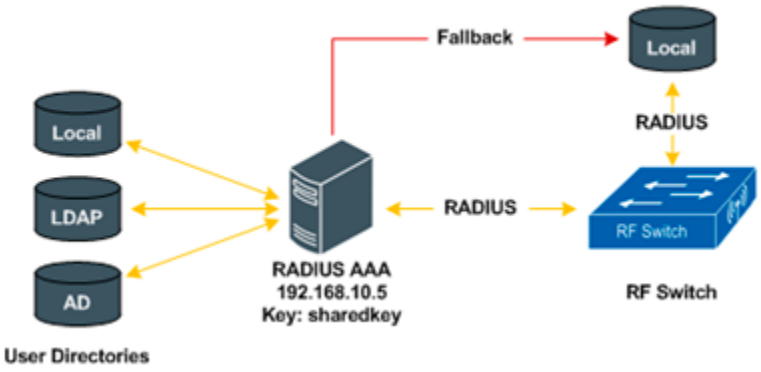
5. Within the Associated Roles field, deselect the **Monitor** role and select **WebUser Administrator**.
6. In the Access Modes field, deselect the **Console**, **Telnet** and **SSHv2** roles and leave the **WEB-UI** role enabled. Click **OK**.
7. Select **Save** (from the lower left-hand corner) to apply the changes.

Radius Management Authentication

The RF Switch can optionally authenticate management users against a Radius server. Radius allows the RF Switch to authenticate management users against a common user database to provide centralized account management, control and accounting.

When Radius authentication is enabled, the RF Switch forwards each management authentication request to the defined Radius server. If the credentials are valid, the Radius server responds with a Radius Accept which must include the associated roles and access methods as return attributes. If the access mode and credentials are valid, the RF Switch grants access. If the access mode or credentials are invalid, the session is rejected. If no associated role information is provided by the Radius server, the RF Switch assigns read-only access permissions for the session.

In the event a Radius server is unavailable, a secondary or tertiary Radius server can be used. If no Radius servers are available, the RF Switch will fall-back to the local user database. If no authentication service is available, the RF Switch can be optionally configured to provide read-only access.



Associated role information is forwarded to the RF Switch from the Radius server as a vendor specific attribute. One or more associated roles must be defined for each management user on the Radius server so the RF Switch knows what permissions to assign the user upon successful authentication. If no associated role is assigned, the user is provided read-only access.

The following table provides details on the associated role vendor specific attribute that can be defined on the Radius server to determine management user permissions:

The following are associated vendor specific attributes:

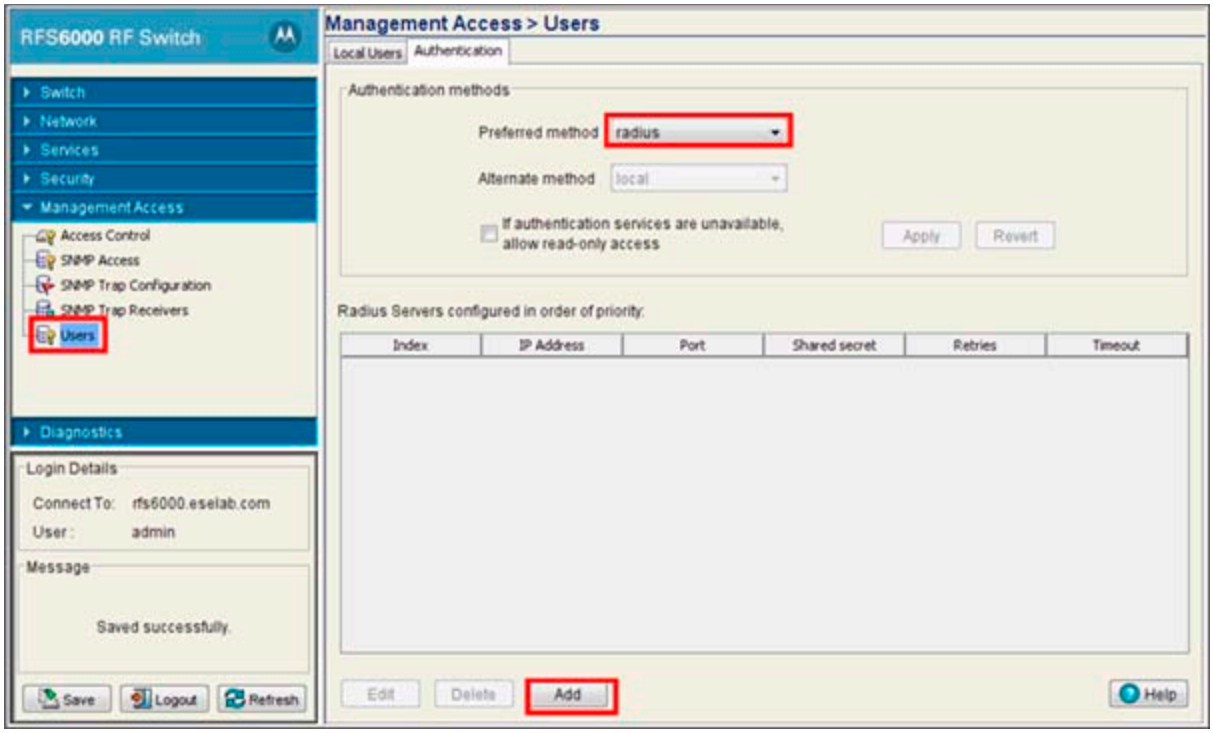
- *IETF Vendor ID* - 388
- *Attribute Number* - 1
- *Attribute Type* - Integer

Integer Value	***Role***
128	Console
64	Telnet
32	SSH
16	Web

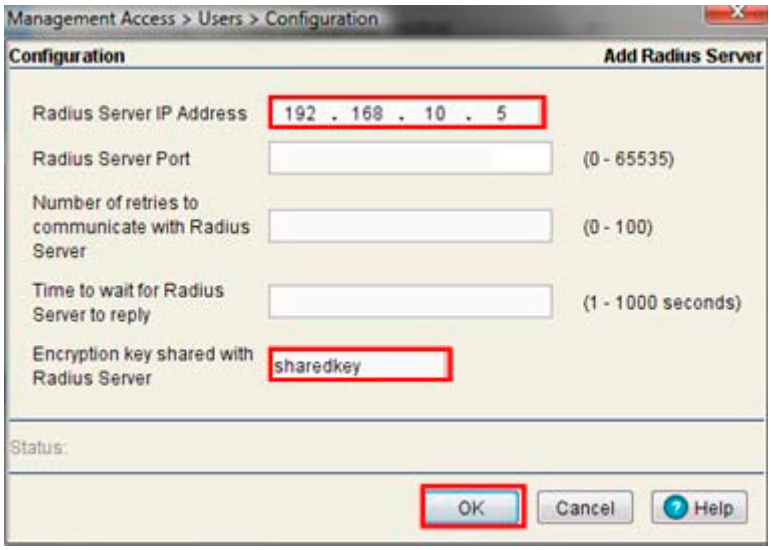
Switch Web UI Configuration

The following demonstrates how to define a Radius server IP address, shared key and how to enable Radius server management authentication:

1. From the switch menu tree select **Management Access** > **Users.**
2. Select the **Authentication** tab.



3. Set the Preferred method to **radius**. Click **Add**.



4. Enter the **Radius Server IP Address** and Radius shared key. Click **OK**.
5. Select **Save** (from the lower left-hand corner) to apply the changes.

D.5.2 RF Switch Running Configuration

The following is the running configuration on the RFS6000 switch used to create this secure device management tutorial:

```
RFS6000# show running-config
!
```

```
! configuration of RFS6000 version 3.3.0.0-029R
!
version 1.2
!
!
aaa authentication login default radius local
service prompt crash-info
!
username "admin" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "webadmin" password 1 3f6e90d89b7cc608717b77f8d49cda24a1c4c518
username "webadmin" access  web
username "webadmin" privilege  webadmin
!
!
ip access-list standard 1
 permit 192.168.10.0/24 rule-precedence 10
 permit 192.168.11.0/24 rule-precedence 20
 deny any rule-precedence 30
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc."
"WLAN Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v3
```

```
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
no service pm sys-restart
timezone America/New_York
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d04677
7fbed80f433b68ea
!
wireless
 secure-wispe-default-secret 0 new-pre-shared-key
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
 wlan 1 dot11i preauthentication
 wlan 2 enable
 wlan 2 description MOTO-GUEST
 wlan 2 ssid MOTO-GUEST
 wlan 2 vlan 70
 wlan 2 authentication-type hotspot
 wlan 2 hotspot webpage-location advanced
 wlan 2 radius server primary 192.168.10.14
 wlan 2 radius server primary radius-key 0 ESELAB
 wlan 2 radius accounting server primary 192.168.10.14
 wlan 2 radius accounting server primary radius-key 0 ESELAB
 wlan 3 enable
```

```
wlan 3 description MOTO-VOICE
wlan 3 ssid MOTO-VOICE
wlan 3 vlan 80
wlan 3 encryption-type tkip
wlan 3 dot11i phrase 0 motovoicetest
wlan 3 dot11i preauthentication
radio add 1 00-15-70-78-F5-23 11a ap300
radio 1 description AP300-1-A
radio 1 bss 1 1
radio 1 channel-power indoor 36 15
radio 1 on-channel-scan
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
radio 5 description AP300-3-A
radio 5 bss 1 1
radio 5 channel-power indoor 44 15
radio 5 on-channel-scan
radio 5 adoption-pref-id 100
radio add 6 00-15-70-B2-FD-D0 11bg ap300
```

```
 radio 6 description AP300-3-BG
 radio 6 bss 1 1
 radio 6 bss 2 2
 radio 6 bss 3 3
 radio 6 channel-power indoor 11 18
 radio 6 on-channel-scan
 radio 6 short-preamble
 radio 6 adoption-pref-id 100
 radio add 7 00-15-70-D5-DA-CE 11a ap300
 radio 7 description AP300-4-A
 radio 7 channel-power indoor 48 17
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 radio add 9 00-15-70-D5-DA-FB 11a ap300
 radio 9 description AP300-5-A
 radio 9 channel-power indoor 149 20
 radio 9 on-channel-scan
 radio add 10 00-15-70-D5-DA-FB 11bg ap300
 radio 10 description AP300-5-BG
 radio 10 channel-power indoor 6 4
 radio 10 on-channel-scan
 no ap-ip default-ap switch-ip
 ap-detection enable
!
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
!
radius-server local
 authentication eap-auth-type all
```

```
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
switchport access vlan 10
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
interface vlan1
 no ip address
 shutdown
```

```
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
 ip access-group 1 in
!
interface vlan70
 description GUEST
 ip address 192.168.70.14/24
!
!
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
radius-server host 192.168.10.5 key 0 sharedkey
line con 0
line vty 0 24
!
end
```

D.6 Secure WISPe

Secure WiSPe is a feature providing secure 128-bit AES encryption for management and control frames exchanged between a RF Switch and adopted AP300s. Secure WiSPe also provides mutual authentication, ensuring only specific APs are allowed to adopted to the RF Switch.

D.6.1 Shared Secrets

Encryption and authentication is provided by defining an 8 to 64 character shared secret on the RF Switch for each AP300 profile. The shared secret authenticates the AP300 during adoption, and derives a unique session key to encrypt the management and control frames. Depending on customer requirements, the same shared secret can be defined for all AP300s on a RF Switch, or a unique shared secret can be configured for each AP.

By default, a shared secret *defaultS* is pre-defined on the RF Switch and is applied to all configured AP300s. Motorola recommends the default shared secret be changed and applied to all AP300s added to the RF Switch. However, when the default shared secret is changed it does not change the shared secret already defined on existing APs.

Shared secrets are forwarded to AP300s during the L2/L3 adoption. When secure WiSPe is first enabled for an AP300, the AP300s must be set for pre staging, then reset. When pre-staging is enabled, the RF Switch forwards the shared key to the AP300 in clear text. If pre staging is not enabled, the AP300 does not have the correct shared key and is rejected by the RF Switch during adoption.

Once the shared key has been forwarded to the AP300s, pre staging can be disabled and subsequent key changes are forwarded to the AP300 over secure WiSPe management/control frames.

NOTE: When a shared secret is changed on a secure WiSPe enabled AP300, the AP300 must be reset before the new shared secret and session keys can be used. Until the AP300 is reset, the existing shared secret and session keys remain in use.

D.6.2 Pre Staging Mode

When secure WiSPe is first enabled on an AP300, pre staging mode must be enabled on the AP300 for the initial shared key to be applied. When pre staging mode is enabled on an AP300, the RF Switch forwards the configured shared key to the AP300 in clear text during L2/L3 adoption. Once applied, the shared secret is used to authenticate the AP300 to the RF Switch and generate unique session keys to encrypt management

and control frames. If pre staging mode is not enabled for the AP300, the AP300 does not have the correct shared secret and will fail to authenticate to the RF Switch.

Once the shared secret is applied to an AP300, pre staging can be disabled on the AP. Subsequent changes to the shared secret, once secure WiSPe is enabled, are applied over secured management and control frames, and pre staging mode is not required.

Pre staging is primarily used when enabling secure WiSPe on an AP300. However, pre staging is also required for the following adoption scenarios:

- A RF Switch adopting AP300s with a default or an outdated shared secret
- A RF Switch adopting AP300s running old firmware with no secure WiSPe support
- A RF Switch adopting AP300s from other RF Switches that use a different shared secret

NOTE: AP300s with a secure WiSPe enabled can be adopted by RF Switches running older firmware, or by RF Switches with secure WiSPe disabled. However, if the shared secret is changed, or the firmware downgraded, pre staging must be enabled before readopting the AP300 on a secure WiSPe supported RF Switch.

D.6.3 Applications

Secure WiSPe is intended for environments requiring security for management and control frames to protect against unauthorized monitoring and potential man-in-the-middle attacks. Secure WiSPe combined with strong WLAN encryption can provide complete end-to-end encryption for all frames exchanged between a RF Switch and adopted AP300s.

D.6.4 Restrictions

Secure WiSPe only provides encryption for management and control frames and does not provide encryption for MU data frames. MU data frame encryption can be provided by enabling WEP, KeyGuard, WPA or WPA2 encryption on each WLAN where encryption is required. Whatever encryption is used to protect the data over the air will be used when exchanging traffic between the APs and RF Switch.

D.6.5 Secure WISPe Configuration

The following configuration activities can be performed to secure WISPe on an AP300:

- *Enabling Secure WISPe on Existing AP300s*
- *Enabling Secure WISPe on New AP300s*

To view the running configuration on the RFS6000 switch used to create this secure WISPe tutorial, refer to *RF Switch Running Configuration on page D-86*.

D.6.5.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One or more RF Switches are installed and operational on the network
- One or more AP300 Access Ports configured and adopted by the RF Switch
- A Windows XP workstation with a console, telnet or SSH client is available to perform configuration on the RF Switches

D.6.5.2 Components

The information in this section is based on the following Motorola hardware and software versions:

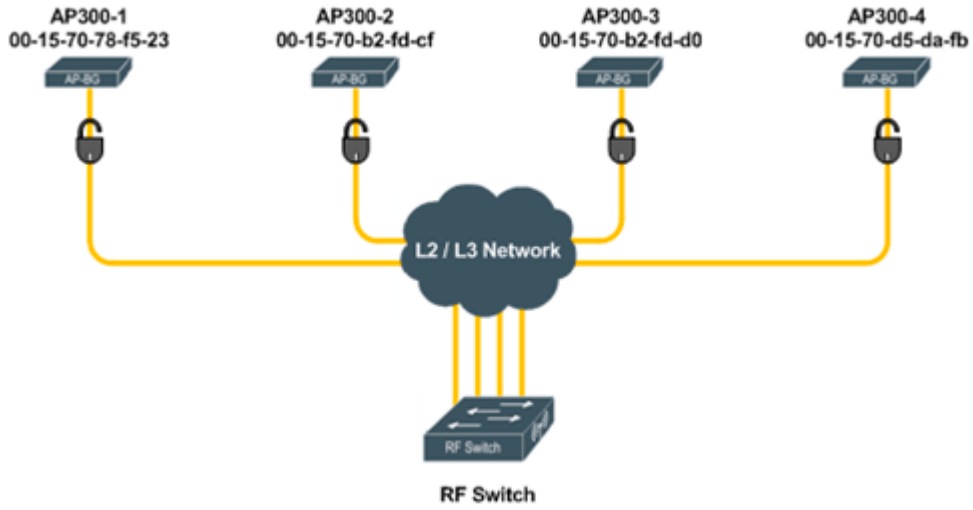
- 1 RFS6000 model switch
- 5 AP300 model access ports

D.6.5.3 Enabling Secure WISPe on Existing AP300s

As depicted in the illustration below, an RF Switch is deployed at a site with four AP300s adopted (at L3). An administrator wants to enable secure WiSPe on the existing AP300s to secure management and control frames and provide authentication.

Enabling secure WiSPe for an existing deployment requires the following:

- A secure WiSPe shared secret for each AP
- Pre staging and secure mode be enabled for each adopted AP300
- The four AP300s be reset during a scheduled maintenance window to allow the shared key to be applied
- Pre staging be disabled once the AP300s have been re-adopted by the RF Switch

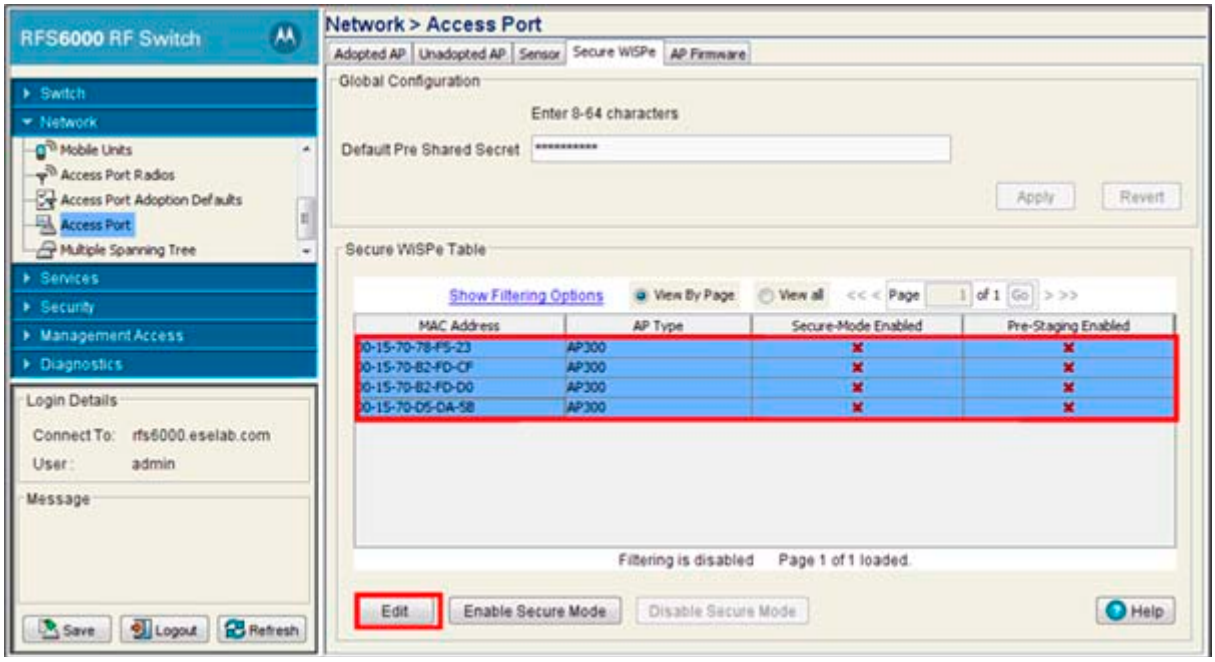


MAC Address	*Secure Mode*	*Pre Staging*	*Shared Secret*
00-15-70-78-f5-23	Enabled	Enabled	pre shared key
00-15-70-b2-fd-cf	Enabled	Enabled	pre shared key
00-15-70-b2-fd-d0	Enabled	Enabled	pre shared key
00-15-70-d5-da-fb	Enabled	Enabled	pre shared key

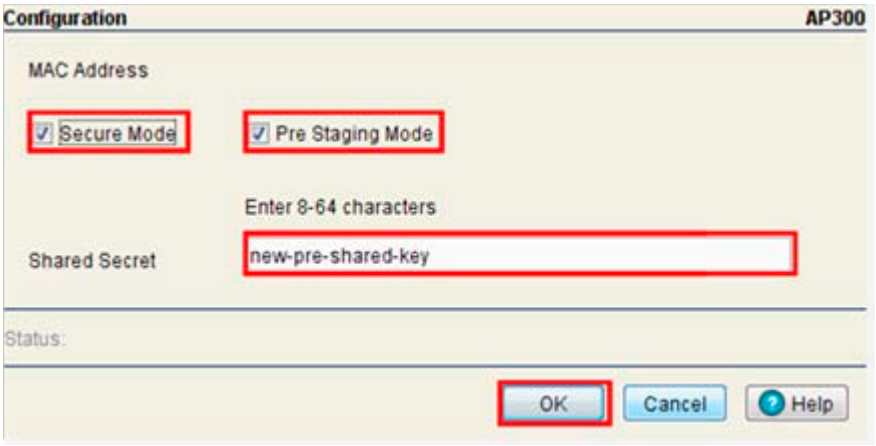
Web UI Configuration

The following configuration example demonstrates how to enable secure WiSPe for existing AP300s on a RF Switch:

1. From the switch menu tree select **Network** > **Access Port.**
2. Select the **WISPe** tab.



3. Highlight and select the AP300s then click **Edit**.



4. Check the **Secure Mode** and **Pre Staging Mode** options.

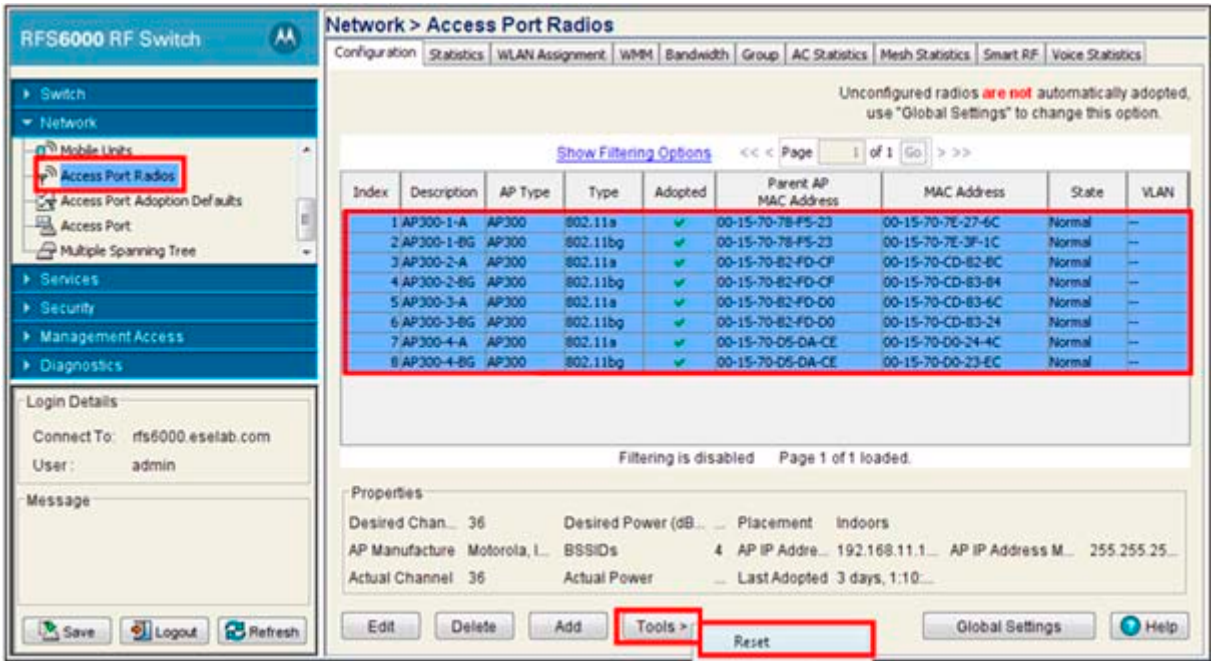
   This enables secure WiSPe on existing AP300s and allows the AP300s to receive the new shared key upon re-adoption.

5. In the **Shared Secret** field enter the new shared secret to be applied to the AP300s. In this example, the shared secret *new-pre-shared-key* is defined. Click **OK**.

   The updates are reflected within the Secure WISPe table.

MAC Address	AP Type	Secure-Mode Enabled	Pre-Staging Enabled
00-15-70-78-F5-23	AP300	✔	✔
00-15-70-B2-FD-CF	AP300	✔	✔
00-15-70-B2-FD-D0	AP300	✔	✔
00-15-70-D5-DA-CE	AP300	✔	✔

6. From the switch menu tree select **Network** > **Access Port Radios.**

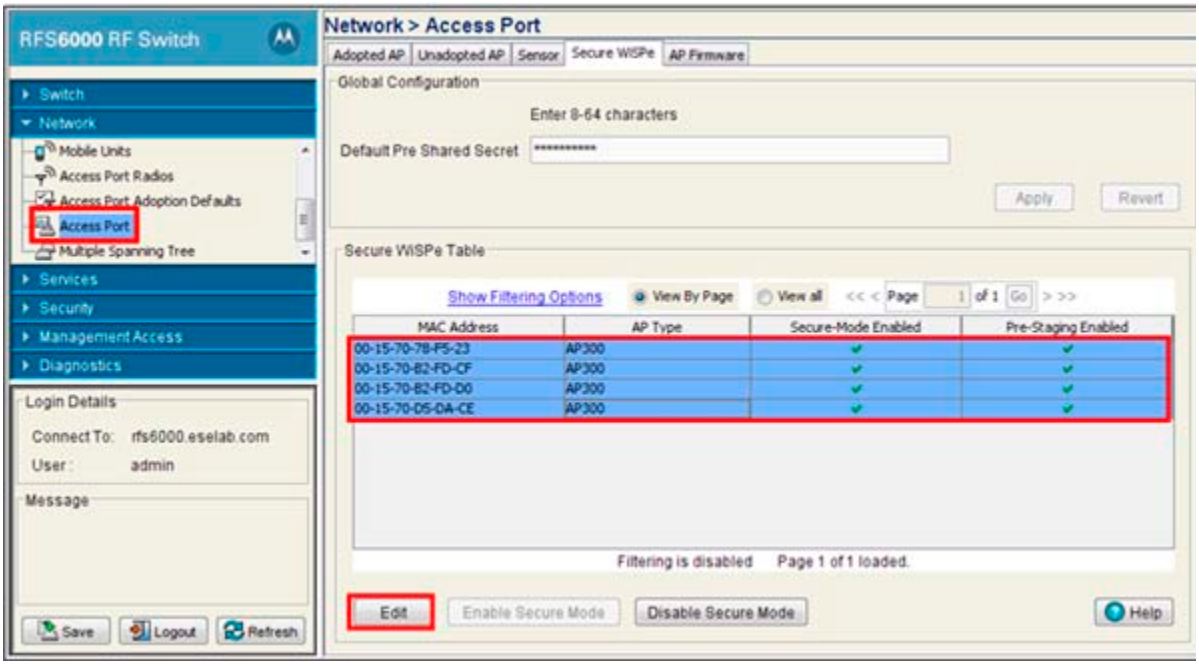


7. Highlight and select the radios to reset.
8. Select **Tools** and **Reset**.

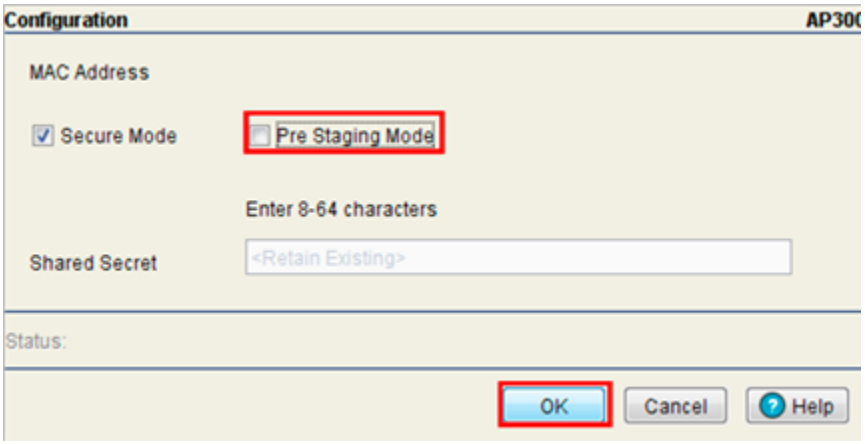
9. Select **Reset entire Access Port**.

   This resets adopted AP300s. During re-adoption with the switch, this action applies the new shared key to each AP300 and enable secure WiSPe.

10. From the switch menu tree select **Network** > **Access Port.**
11. Select the **WISPe** tab.



12.Highlight and select the AP300s then select **Edit.**



13.Un-check the **Pre Staging Mode** option and select **OK**.

The updates are reflected within the Secure WISPe table.

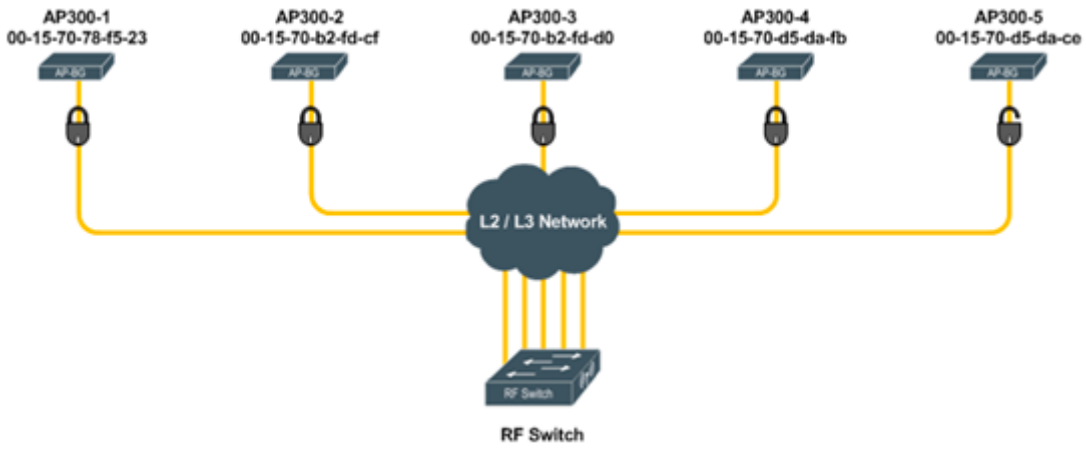
MAC Address	AP Type	Secure-Mode Enabled	Pre-Staging Enabled
00-15-70-78-F5-23	AP300	✔	✖
00-15-70-B2-FD-CF	AP300	✔	✖
00-15-70-B2-FD-D0	AP300	✔	✖
00-15-70-D5-DA-CE	AP300	✔	✖

14.Select **Save** (from the lower left-hand corner) to apply the changes.

D.6.5.4 Enabling Secure WISPe on New AP300s

As depicted in the illustration below, a new AP300 is added to an RF Switch with four existing AP300s with secure WiSPe enabled. Enabling secure WiSPe for new AP300s in an existing WiSPe deployment requires the following:.

- A default pre shared secret be defined on the RF Switch. This configures the shared secret on all AP300s added to the RF Switch
- A new AP300 be added to the RF Switch
- Pre staging and secure mode are enabled for the new AP300
- An AP300 be connected to the network to allow the shared key to be applied
- Pre staging mode be disabled once the a AP300 is adopted by the RF Switch

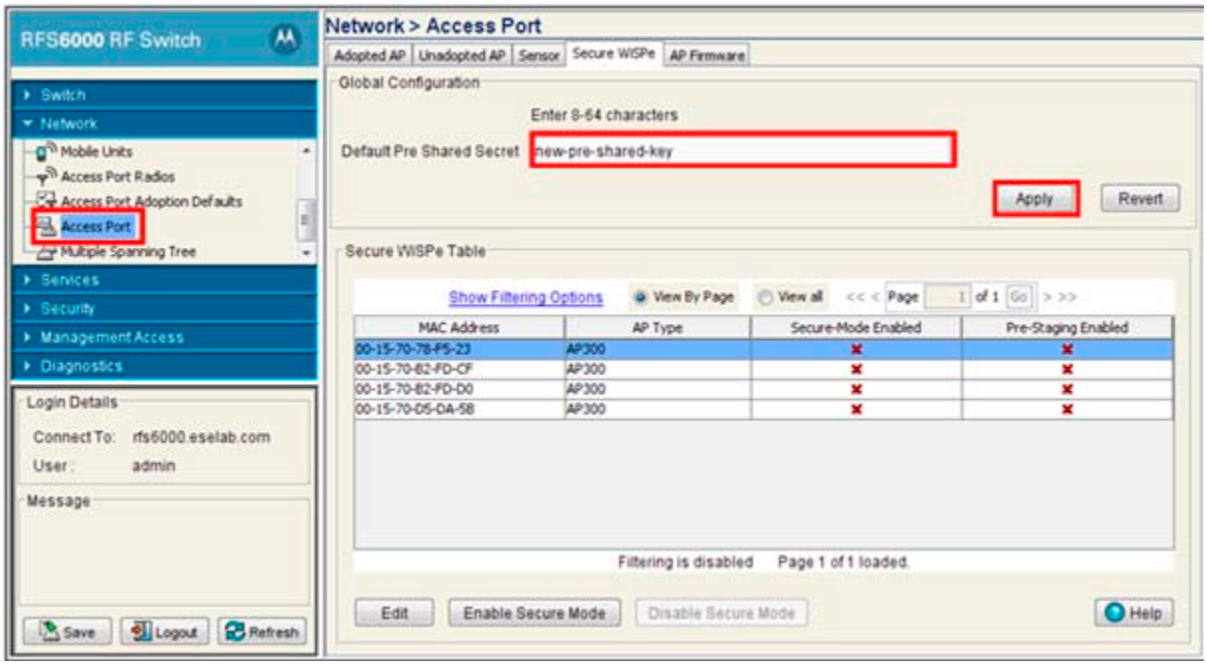


MAC Address	*Secure Mode*	*Pre Staging*	*Shared Secret*
00-15-70-78-f5-23	Enabled	Disabled	pre shared key
00-15-70-b2-fd-cf	Enabled	Disabled	pre shared key
00-15-70-b2-fd-d0	Enabled	Disabled	pre shared key
00-15-70-d5-da-fb	Enabled	Disabled	pre shared key
00-15-70-d5-da-ce	Enabled	Enabled	pre shared key

Web UI Configuration

The following configuration example demonstrates how to enable secure WiSPe on new AP300s:

1. From the switch menu tree select **Network** > **Access Port.**
2. Select the **WISPe** tab.

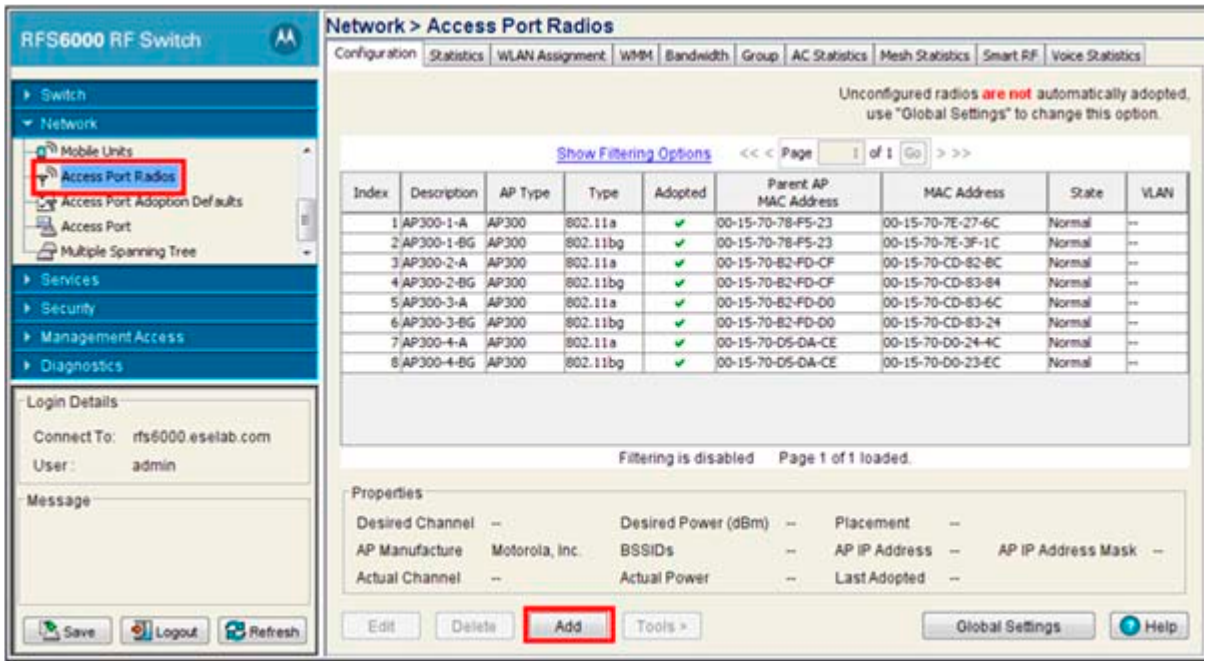


3. In the **Default Pre Shared Secret** field enter the new shared secret to be applied to new AP300s added to the RF Switch.

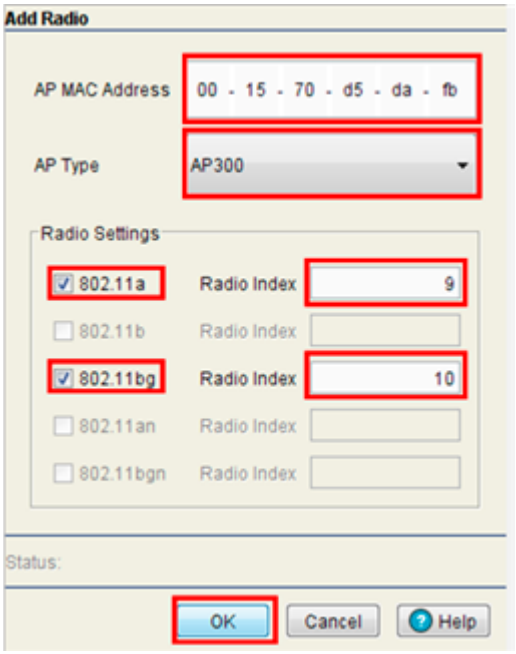
   In this example the shared secret *new-pre-shared-key* is used. Click **Apply**.

4. From the switch menu tree select **Network** > **Access Port Radios**.

5. Select the **Configuration** tab.



6. Select **Add**.

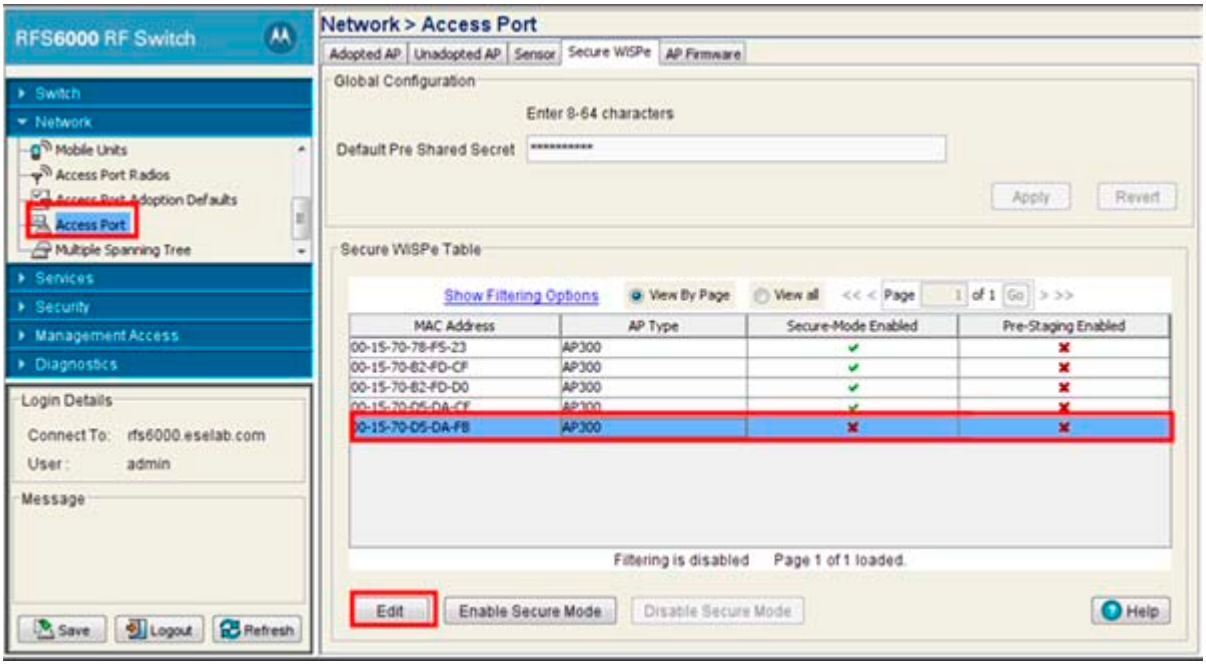


7. In the **AP MAC Address** field enter the MAC address for the new AP.
8. Set the **AP Type** to AP300.
9. Enable the **802.11a** and **802.11bg** radios and specify a **Radio Index**. Click **OK**.

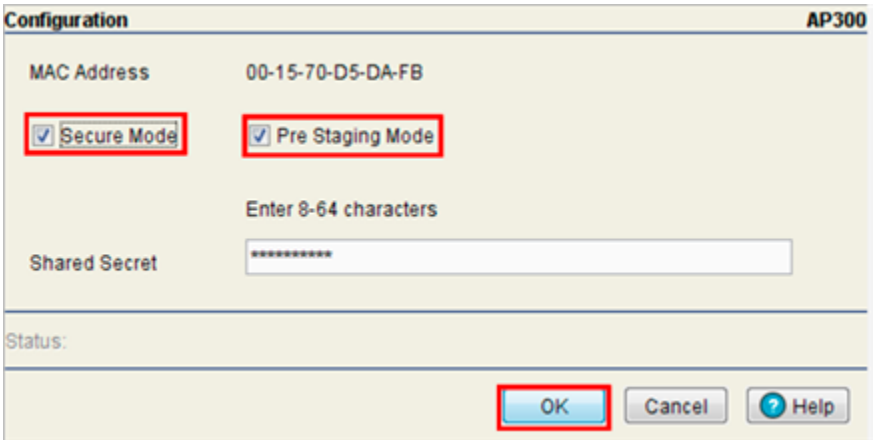
Index	Description	AP Type	Type	Adopted	Parent AP MAC Address	MAC Address	State	VLAN
1	AP300-1-A	AP300	802.11a	✔	00-15-70-78-F5-23	00-15-70-7E-27-6C	Normal	--
2	AP300-1-BG	AP300	802.11bg	✔	00-15-70-78-F5-23	00-15-70-7E-3F-1C	Normal	--
3	AP300-2-A	AP300	802.11a	✔	00-15-70-B2-FD-CF	00-15-70-CD-82-BC	Normal	--
4	AP300-2-BG	AP300	802.11bg	✔	00-15-70-B2-FD-CF	00-15-70-CD-83-84	Normal	--
5	AP300-3-A	AP300	802.11a	✔	00-15-70-B2-FD-D0	00-15-70-CD-83-6C	Normal	--
6	AP300-3-BG	AP300	802.11bg	✔	00-15-70-B2-FD-D0	00-15-70-CD-83-24	Normal	--
7	AP300-4-A	AP300	802.11a	✔	00-15-70-D5-DA-CE	00-15-70-D0-24-4C	Normal	--
8	AP300-4-BG	AP300	802.11bg	✔	00-15-70-D5-DA-CE	00-15-70-D0-23-EC	Normal	--
9	RADIO9	AP300	802.11a	✖	00-15-70-D5-DA-FB			
10	RADIO10	AP300	802.11bg	✖	00-15-70-D5-DA-FB			

The results of the updates are reflected within the From the switch menu tree select **Network** > **Access Port Radios** > **Configuration screen**.

10. From the switch menu tree select **Network** > **Access Port.**
11. Select the **WISPe** tab.

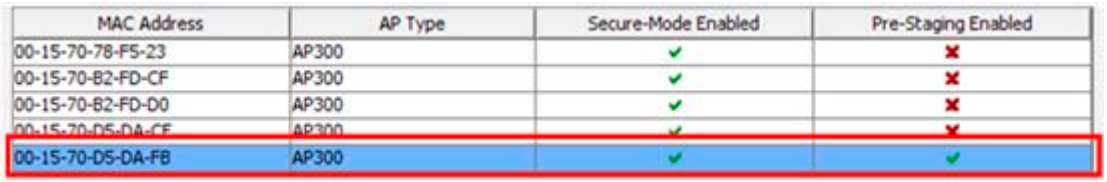


12.Highlight and select the newly added AP300. Click **Edit.**



13.Select the **Secure Mode** and **Pre Staging Mode** options.

The Shared Secret does not need to be defined, as the AP300 are configured with the default shared secret. Click **OK.**



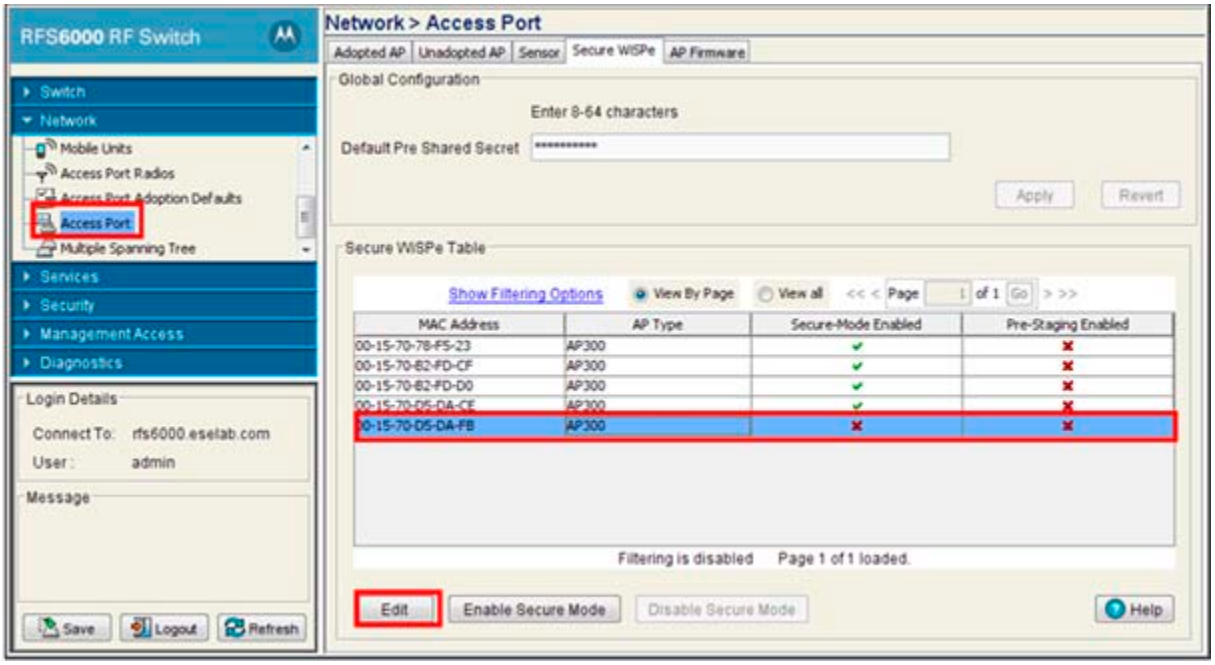
The updates reflect as displayed above.

14.Connect the new AP300 to the network and verify it's adopted by the RF Switch.

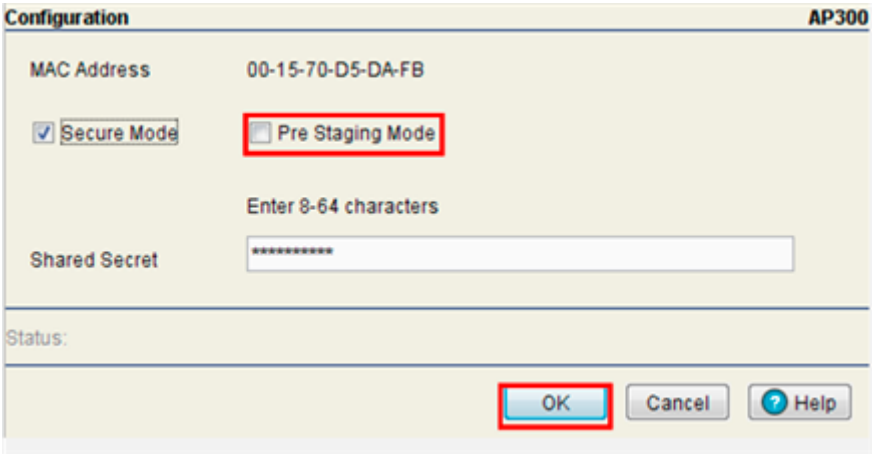
Index	Description	AP Type	Type	Adopted	Parent AP MAC Address	MAC Address	State	VLAN
1	AP300-1-A	AP300	802.11a	✔	00-15-70-78-F5-23	00-15-70-7E-27-6C	Normal	--
2	AP300-1-BG	AP300	802.11bg	✔	00-15-70-78-F5-23	00-15-70-7E-3F-1C	Normal	--
3	AP300-2-A	AP300	802.11a	✔	00-15-70-B2-FD-CF	00-15-70-CD-82-BC	Normal	--
4	AP300-2-BG	AP300	802.11bg	✔	00-15-70-B2-FD-CF	00-15-70-CD-83-84	Normal	--
5	AP300-3-A	AP300	802.11a	✔	00-15-70-B2-FD-D0	00-15-70-CD-83-6C	Normal	--
6	AP300-3-BG	AP300	802.11bg	✔	00-15-70-B2-FD-D0	00-15-70-CD-83-24	Normal	--
7	AP300-4-A	AP300	802.11a	✔	00-15-70-D5-DA-CE	00-15-70-D0-24-4C	Normal	--
8	AP300-4-BG	AP300	802.11bg	✔	00-15-70-D5-DA-CE	00-15-70-D0-23-EC	Normal	--
9	AP300-5-A	AP300	802.11a	✔	00-15-70-D5-DA-FB	00-15-70-D0-25-64	Normal	--
10	AP300-5-BG	AP300	802.11bg	✔	00-15-70-D5-DA-FB	00-15-70-D0-26-54	Normal	--

15.From the switch menu tree select **Network** > **Access Port.**

16.Select the **WISPe** tab.



17.Highlight and select the newly added AP300. Click **Edit.**



18.Un-check the **Pre Staging Mode** option. Click **OK**.

19.Select **Save** (from the lower left-hand corner) to apply the changes.

D.6.6 RF Switch Running Configuration

The following shows the running configuration of the RFS6000 switch used to create this tutorial:

```
RFS6000# show running-config
!
! configuration of RFS6000 version 3.3.0.0-029R
!
version 1.2
!
!
aaa authentication login default local none
service prompt crash-info
!
username "admin" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc." "WLAN
Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v3
```

```
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
timezone America/New_York
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d046777fbed8
0f433b68ea
!
wireless
 secure-wispe-default-secret 0 new-pre-shared-key
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
 wlan 1 dot11i preauthentication
 wlan 2 enable
 wlan 2 description MOTO-GUEST
 wlan 2 ssid MOTO-GUEST
 wlan 2 vlan 70
 wlan 2 authentication-type hotspot
 wlan 2 hotspot webpage-location advanced
 wlan 2 radius server primary 192.168.10.14
 wlan 2 radius server primary radius-key 0 ESELAB
```

```
wlan 2 radius accounting server primary 192.168.10.14
wlan 2 radius accounting server primary radius-key 0 ESELAB
wlan 3 enable
wlan 3 description MOTO-VOICE
wlan 3 ssid MOTO-VOICE
wlan 3 vlan 80
wlan 3 encryption-type tkip
wlan 3 dot11i phrase 0 motovoicetest
wlan 3 dot11i preauthentication
radio add 1 00-15-70-78-F5-23 11a ap300
radio 1 description AP300-1-A
radio 1 bss 1 1
radio 1 channel-power indoor 36 15
radio 1 on-channel-scan
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
```

```
 radio 5 description AP300-3-A
 radio 5 bss 1 1
 radio 5 channel-power indoor 44 15
 radio 5 on-channel-scan
 radio 5 adoption-pref-id 100
 radio add 6 00-15-70-B2-FD-D0 11bg ap300
 radio 6 description AP300-3-BG
 radio 6 bss 1 1
 radio 6 bss 2 2
 radio 6 bss 3 3
 radio 6 channel-power indoor 11 18
 radio 6 on-channel-scan
 radio 6 short-preamble
 radio 6 adoption-pref-id 100
 radio add 7 00-15-70-D5-DA-CE 11a ap300
 radio 7 description AP300-4-A
 radio 7 channel-power indoor 48 17
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 radio add 9 00-15-70-D5-DA-FB 11a ap300
 radio 9 description AP300-5-A
 radio 9 channel-power indoor 149 20
 radio 9 on-channel-scan
 radio add 10 00-15-70-D5-DA-FB 11bg ap300
 radio 10 description AP300-5-BG
 radio 10 channel-power indoor 6 4
 radio 10 on-channel-scan
 no ap-ip default-ap switch-ip
 ap 00-15-70-78-F5-23 secure-mode enable
 ap 00-15-70-B2-FD-CF secure-mode enable
 ap 00-15-70-B2-FD-D0 secure-mode enable
 ap 00-15-70-D5-DA-CE secure-mode enable
 ap 00-15-70-D5-DA-FB secure-mode enable
 ap-detection enable
!
 smart-rf
```

```
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
!
radius-server local
 authentication eap-auth-type all
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
```

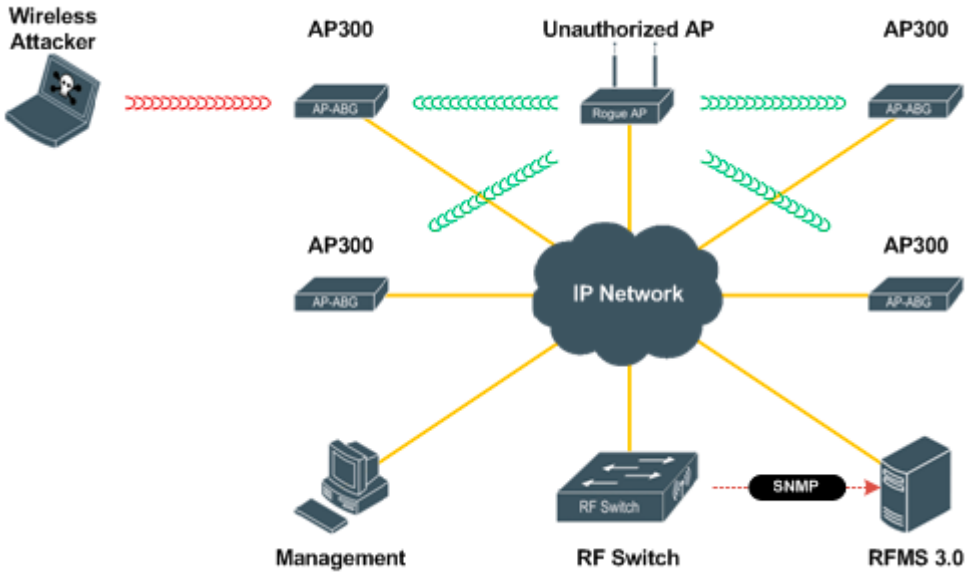
```
interface ge8
switchport access vlan 10
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
interface vlan1
 no ip address
 shutdown
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
!
interface vlan70
 description GUEST
 ip address 192.168.70.14/24
!
!
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
```

```
end
```

D.7 Wireless IDS

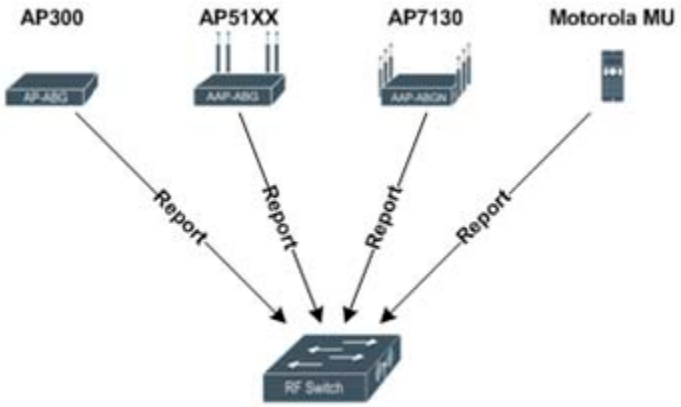
Threats to WLANs are numerous and are potentially devastating to business and day to day operations. Security issues ranging from unauthorized Access Points or 802.11 attacks can plague a WLAN and jeopardize sensitive information as well as performance.

To aid in the detection and defense of potential threats, Motorola offers a layered approach to security that includes integrated unauthorized AP detection, unauthorized AP containment and Wireless Intrusion Detection.



D.7.1 Unauthorized Access Point Detection

Unauthorized AP detection is a feature directly integrated into the RF Switch. When enabled, it allows the switch to monitor the RF environment for unauthorized APs. Unauthorized APs can be reported to the RF Switch from managed radios configured to perform scanning or from Motorola *Mobile Units* (MUs) detecting and reporting visible APs when roaming.



Unauthorized AP scanning is supported on AP100, AP300, AP5131 and AP7131 radios adopted by the RF Switch and is enabled on a per-radio bases. This allows administrators to scan for APs throughout the network or specific areas depending on the need. Each AP supports the following scanning modes:

- *Single Channel Scanning* - Managed radios monitor the RF environment on the operating channel while simultaneously servicing mobile users.
- *Detector* - Managed radios monitors all channels in the regulatory domain but cannot service mobile users.

When an AP is detected by a managed radio or Motorola MU, the RF Switch will compare the reported MAC address and ESSID against an allowed AP rules list. Allowed AP rules can be configured on the RF Switch to exclude trusted or known APs which represent no threat to the network from generating alarms. If a reported AP is matched by an allow rule, the AP is placed in an approved list and no alarm generated. If a reported AP is not matched by a rule, the AP is placed in an unapproved list and an alarm generated.

Detected APs remain in the an approved or unapproved list until timed out by the RF Switch. APs that continued to be detected remain in the approved or unapproved list while APs no longer reported are removed from a list once the configured time-out period has expired.

D.7.2 Unauthorized Access Point Containment

APs categorized as unapproved represent a potential threat to the network. Unauthorized AP containment can provide temporary mitigation against unauthorized APs by attempting to disrupt communications with any associated MUs as well as attempting to prevent new MUs from associating with the AP.

Unauthorized AP containment can be performed by adding APs in the unauthorized AP list to a containment list. Once added the RF Switch will co-ordinate mitigation using AP300s by sending broadcast 802.11 de-authentication frames to each MU spoofing the unauthorized APs MAC address. Depending on the site, one or more AP300 can be used to perform containment and the results will vary depending on the MU driver.

D.7.3 Wireless Intrusion Detection

A Motorola RF Switch can also be configured to monitor and alert administers about unauthorized attempts to access the WLAN. Unauthorized attempts are generally accompanied by malicious MUs attempting to identify network vulnerabilities.

Integrated intrusion detection can be enabled on the RF Switch to provide monitoring for basic attacks without the need of dedicated IPS system or monitoring APs. When intrusion violations occur and a configured threshold is exceeded, the RF Switch generates an alarm and mitigates by blacklisting the MU for a definable length of time.

Excessive Probes	TKIP Countermeasures
Excessive Association	Invalid Frame Length
Excessive Disassociation	Excessive EAP NAKS
Excessive Authentication Failure	Invalid 802.1x Frames
Excessive Crypto Replays	Invalid Frame Type
Excessive 802.11 Replays	Beacon with Broadcast ESSID
Excessive Decryption Failures	Frames with Known Bad ESSID
Excessive Unassociated Frames	Unencrypted Traffic

Excessive Probes	TKIP Countermeasures
Excessive EAP Start Frames	Frames with Non-Changing WEP IV
Null Destination	Detect Adhoc Networks
Same Source / Destination MAC	De-Authentication from Broadcast Source MAC
Source Multicast MAC	Invalid Sequence Number

Wireless Intrusion Detection Violations

As shown in table above, the RF Switch can detect numerous violations, each with a configurable threshold for monitoring the specific violation on an MU, radio and switch. Each threshold defines the number of violations that must occur within a globally configured detection window before an alarm is generated and mitigation is performed.

In addition to a configurable threshold, each violation can also be configured with a specific time-to-filter value which determines how long an MU will be blacklisted when a threshold is reached. This allows the RF Switch to perform automatic mitigation against violations without manual intervention from network administrators.

D.7.4 Applications

Integrated WIDS security features are intended for small, medium and large customer deployments who require basic rogue AP detection, rogue AP containment and wireless intrusion detection. The integrated security features can be deployed in any enterprise environment and industry vertical to provide detection and mitigation from potential threats.

D.7.5 Restrictions

The integrated security features provide basic protection against unauthorized APs and wireless threats. Additional protection can be provided by deploying the Motorola AirDefense Enterprise solution, which is an industry leading Wireless IPS system that seamlessly integrates with Motorola RF Switches and Access Points.

With built-in forensic support and industry standard reports for PCI, HIPAA, Sarbanes-Oxley, GLBA, FDIC and DOD, Motorola's *Wireless Intrusion Protection System* (WIPS) provides powerful tools for standards compliance, as well as around-the-clock 802.11a/b/g wireless network security in a distributed environment. It allows administrators to identify and accurately locate attacks, rogue devices, and network vulnerabilities in real time and permits both wired and wireless lockdown of wireless device connections.

The Motorola AirDefense System provides the following advanced features:

- *24x7 Dedicated Sensors* - Real-time identification of hackers, attacks and system weak spots.
- *Historical Database* - By storing and managing more than 270 data points per connection per wireless device per minute, the product provides a highly accurate assessment of wireless threats including anomalies and zero-day attacks. Allows viewing of events months later to improve network security posture and assist in forensic investigations.
- *Forensic Support* - Pertinent historical data supports advanced forensics such as time of attack/breach, entry point used, length of exposure, systems compromised, device activity logs and transfers of data.

- *Multiple Detection Technologies* - Provides accurate and comprehensive detection by applying multiple detection technologies including signature analysis, protocol abuse and anomalous behavior in conjunction with correlation across multiple sensors.
- *Location Based Security* - Provides location of unauthorized devices and activities using Motorola WLAN infrastructure.
- *Reports* - Provides built-in reports for PCI, HIPAA, Sarbanes-Oxley, GLBA, FDIC and DOD, as well as forensic support to determine compliance level after the fact, should a security event occur.
- *Plug-and-Play Operation* - Auto-classification allows quick policy-based authorization of APs and devices. Network traffic can be monitored within minutes of installation, complete with the tools to quickly interpret information for fast response to Wireless LAN threats.
- *Centralized Detection Engine* - Eliminates the need to upgrade sensors individually. A single server upgrade provides new functionality and protection against the latest attacks and new threats.
- *Report Builder* - Allows customized reports to suit your specific needs.
- *Advanced Forensics* - Adds a whole new level of depth and flexibility to forensic investigations, allowing the user to revise the analysis period in and out, to graph data for easier analysis, and to do historical location tracking.

D.7.6 Configuring a Wireless IDS Deployment

The following sections outline the configuration steps required to enable unauthorized AP detection and intrusion detection on a switch:

- *Unauthorized AP Detection*
- *Unauthorized AP Containment*
- *Mobile Unit Intrusion Detection*
- *SNMP Traps*

To view the running configuration on the RFS6000 switch used to create this Wireless IDS tutorial, refer to *RF Switch Running Configuration on page D-108*.

D.7.6.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One or more RF Switches are installed and operational on the network
- One or more AP300 Access Ports configured and adopted by the switch
- A Windows XP workstation with a console, telnet or SSH client is available to perform configuration on the switches
- One or more standalone Access Points are available to verify unauthorized AP detection and containment.
- One or more wireless workstations are available to test and verify unauthorized AP containment and intrusion detection.

D.7.6.2 Components

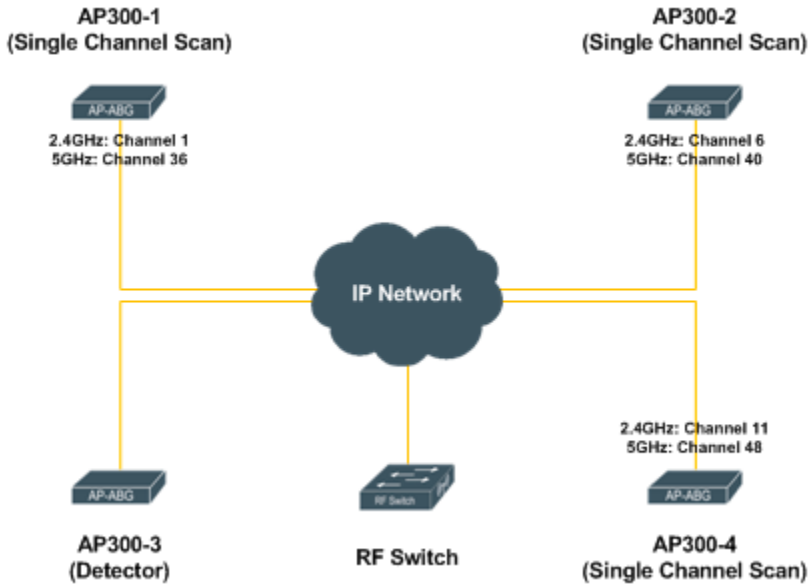
The information in this section is based on the following Motorola hardware and software versions:

- 1 RFS6000 model switch

- 5 AP300 model Access Ports

D.7.6.3 Unauthorized AP Detection

As shown in the figure below, a switch is deployed at a site with four AP300s. The administrator wants to enable unauthorized AP detection to be proactively alerted when any APs are added or removed from the site.

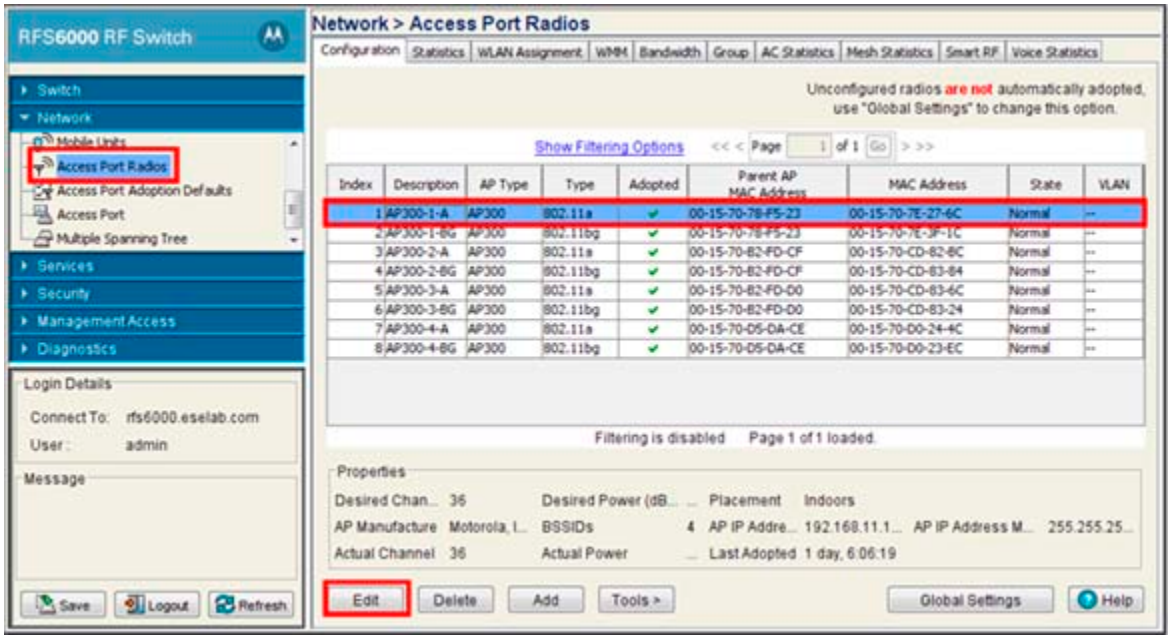


To support the detection of unauthorized APs, three AP300sare configured to perform single channel scanning while simultaneously providing WLAN services to users. The three APs monitor 2.4GHz channels (1, 6 and 11) and 5GHz channels (36, 40 and 48). The fourth AP300 is configured as a dedicated detector AP and monitors all the channels within the regulatory domain. APs provide the switch with complete visibility into the 2.4GHz and 5GHz spectrum at this site using three AP300s with single channel scanning and a dedicated detector.

Switch Web UI Configuration

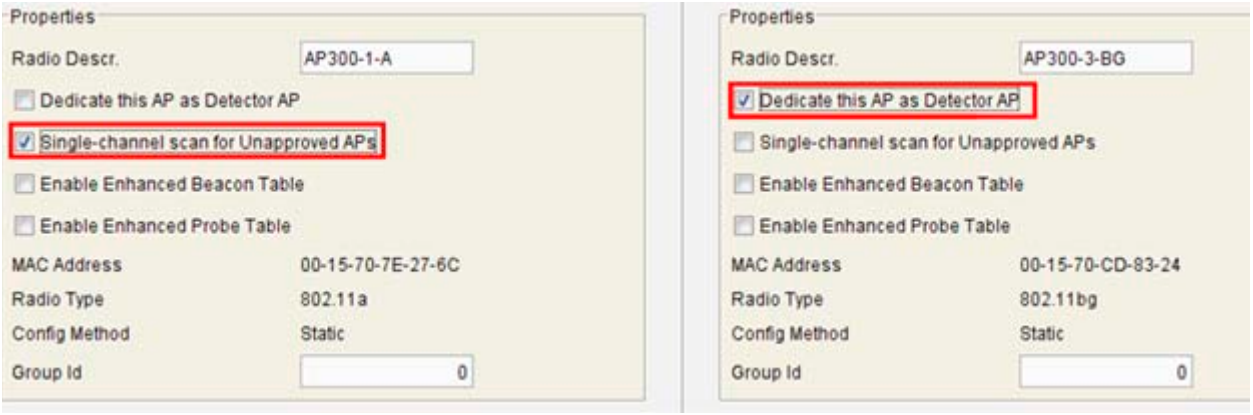
The following configuration example demonstrates how to globally enable unauthorized AP detection on an RF Switch and configure AP300 scanning options:

1. From the switch menu tree select **Network** > **Access Port Radios.**
2. Select the **Configuration** tab.
3. Highlight and select an AP300 radio then click **Edit**.

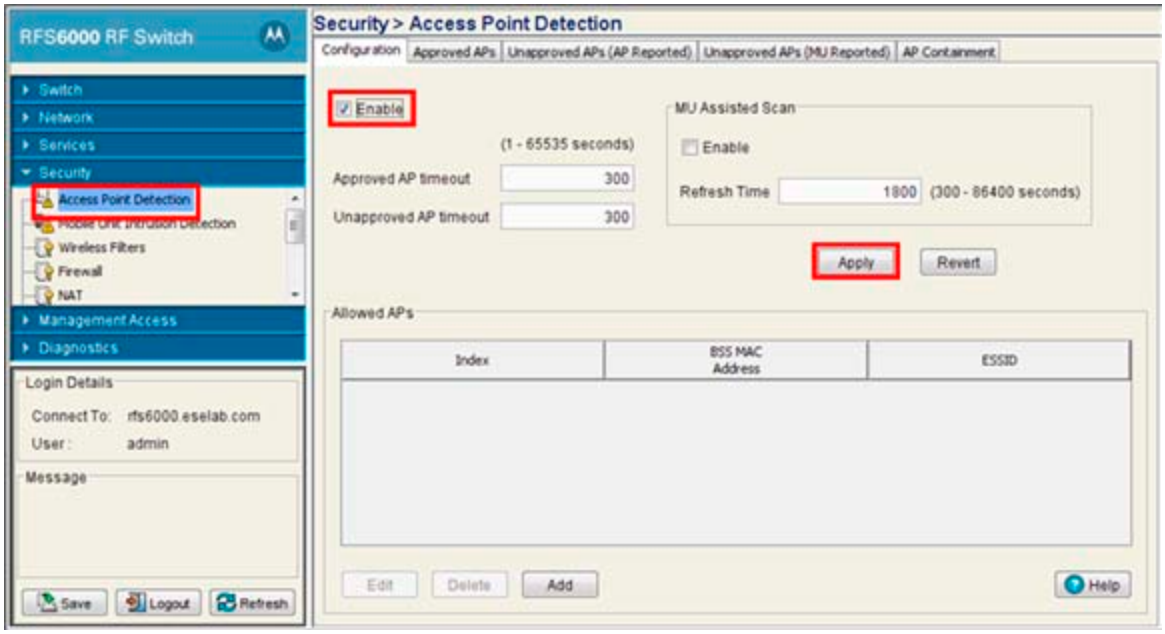


4. Within the **Network** > **Access Port Radio** > **Configuration** screen, refer to the Properties field and check the option **Single-channel scan for Unapproved APs** (for radios 1- 4 and 7-8) and **Dedicate this AP as a Detector AP** (for radios 5-6).

   In this example radios 1-4 and 7-8 will be configured for single channel scanning and radios 5-6 are configured as dedicated detectors.



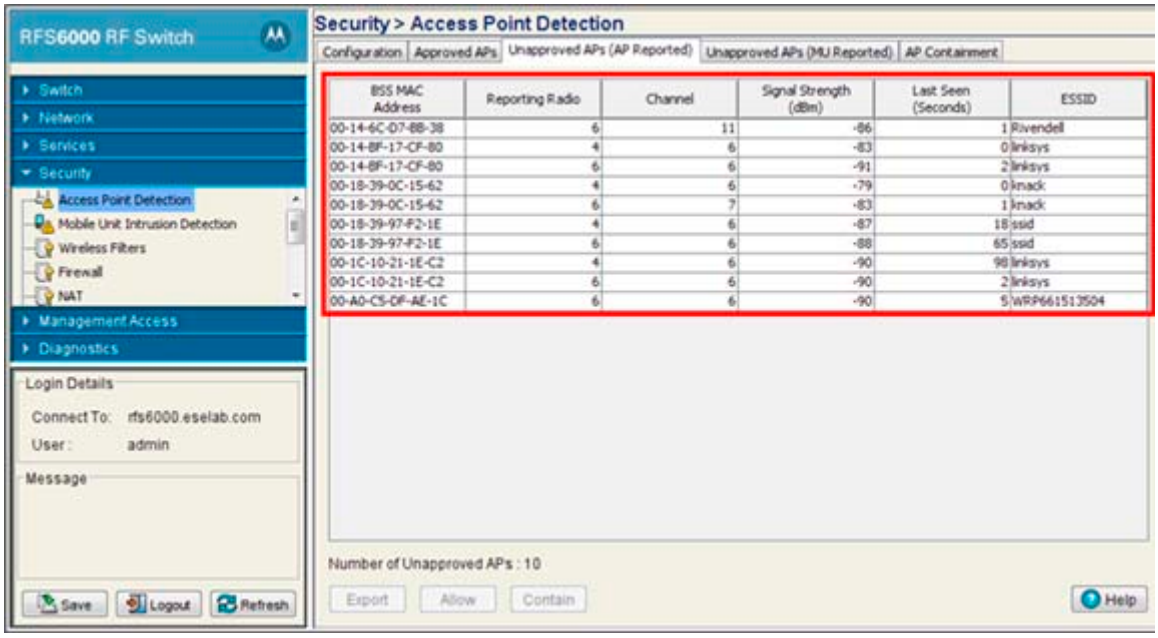
5. From the switch menu tree select **Security** > **Access Point Detection.**
6. Select the **Configuration** tab.



7. Select the **Enable** to checkbox globally enable unauthorized AP detection on the switch. Click **Apply**.

NOTE: If Motorola devices are being deployed, you can optionally enable MU Assisted Scanning, which leverages Motorola client extensions on Motorola devices to provide additional detection.

8. From the switch menu tree select **Security** > **Access Point Detection.**
9. Select the **Unapproved APs (AP Reported)** tab.

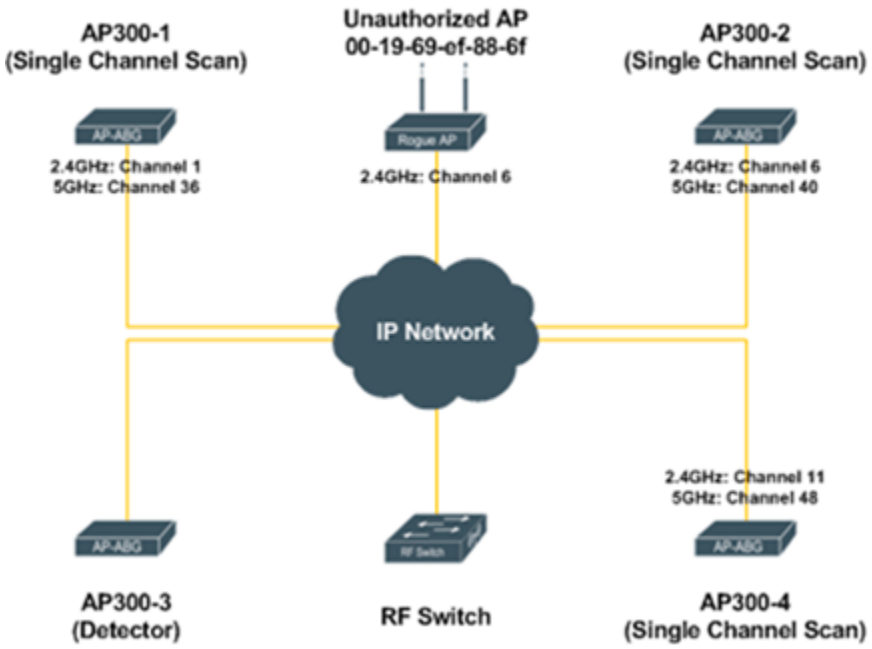


Detected APs are listed in this table.

10. Select **Save** (from the lower left-hand corner) to apply the changes.

D.7.6.4 Unauthorized AP Containment

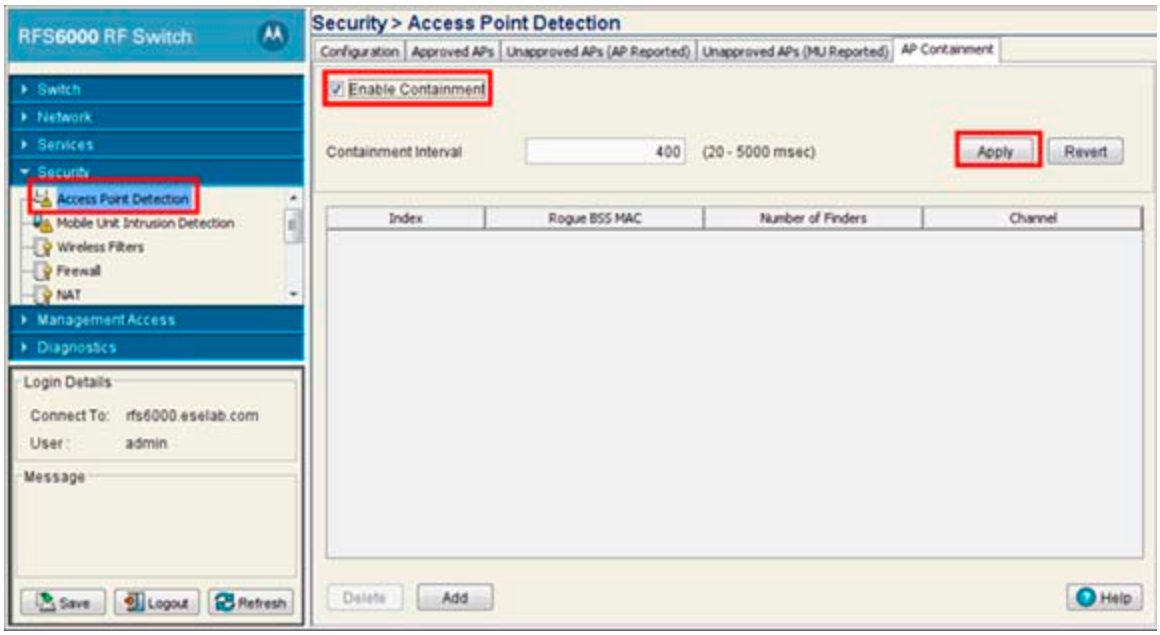
Unauthorized AP containment can be enabled on the RF Switch to provide temporary remediation if an unauthorized AP is placed at the site. Once enabled, the RF Switch provides RF countermeasures against any unauthorized AP MAC addresses added to the containment list.



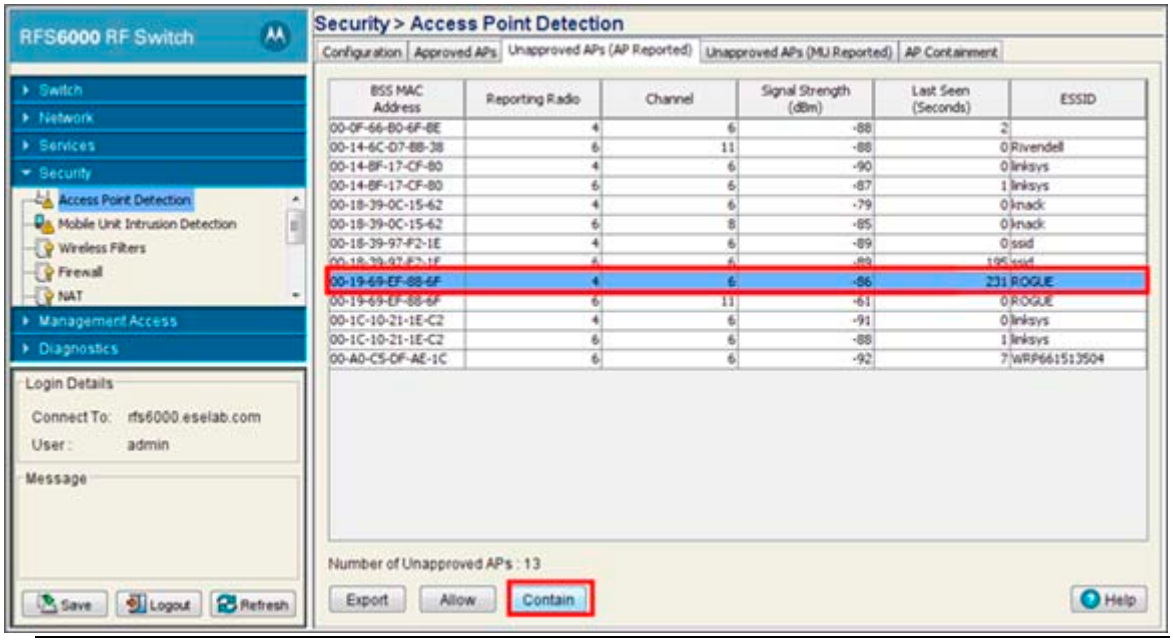
Switch Web UI Configuration

The following configuration example demonstrates how to globally enable unauthorized AP containment and contain an unauthorized AP:

1. From the switch menu tree select **Security** > **Access Point Detection.**
2. Select the **AP Containment** tab.



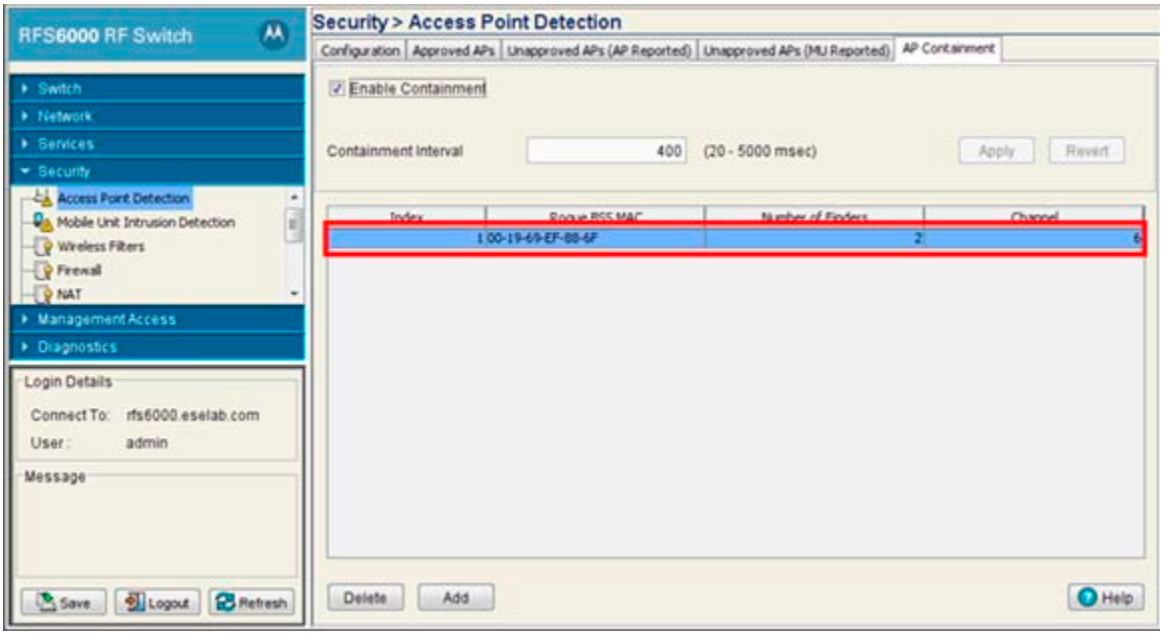
3. Select the **Enable Containment** checkbox. Select **Apply.**
4. Select the **Unapproved APs (AP Reported)** tab.



CAUTION: Care should be taken when using unauthorized AP containment to ensure containment is not being performed on authorized neighboring APs.

5. To contain an unauthorized AP, select an entry from the Unapproved APs list and click **Contain**.

   This adds the MAC address of the unauthorized AP to the AP Containment list.
6. Select the **AP Containment** tab.



The unauthorized AP is listed in the containment list. You can manually add additional unauthorized AP MAC addresses to the containment list or remove unauthorized APs as needed.

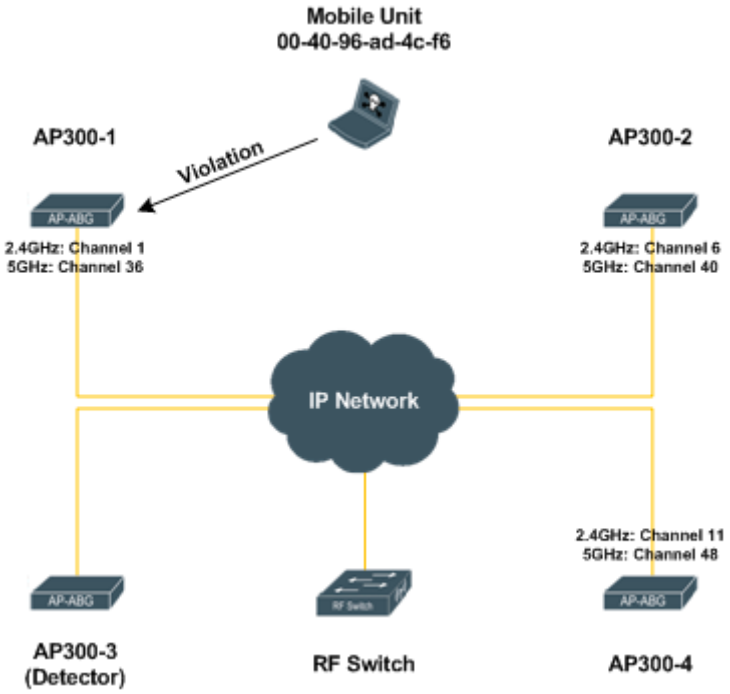
7. Select **Save** (from the lower left-hand corner) to apply the changes.

D.7.6.5 Mobile Unit Intrusion Detection

Mobile unit (MU) intrusion detection can enabled on the RF Switch to provide proactive protection against active intrusion attempts. The switch can detect numerous intrusion violations and can alert administrators of intrusion attempts and attacks. The switch can mitigate by automatically blacklisting MUs triggering the violation.

The following configurations will be performed as part of this MU intrusion detection example:

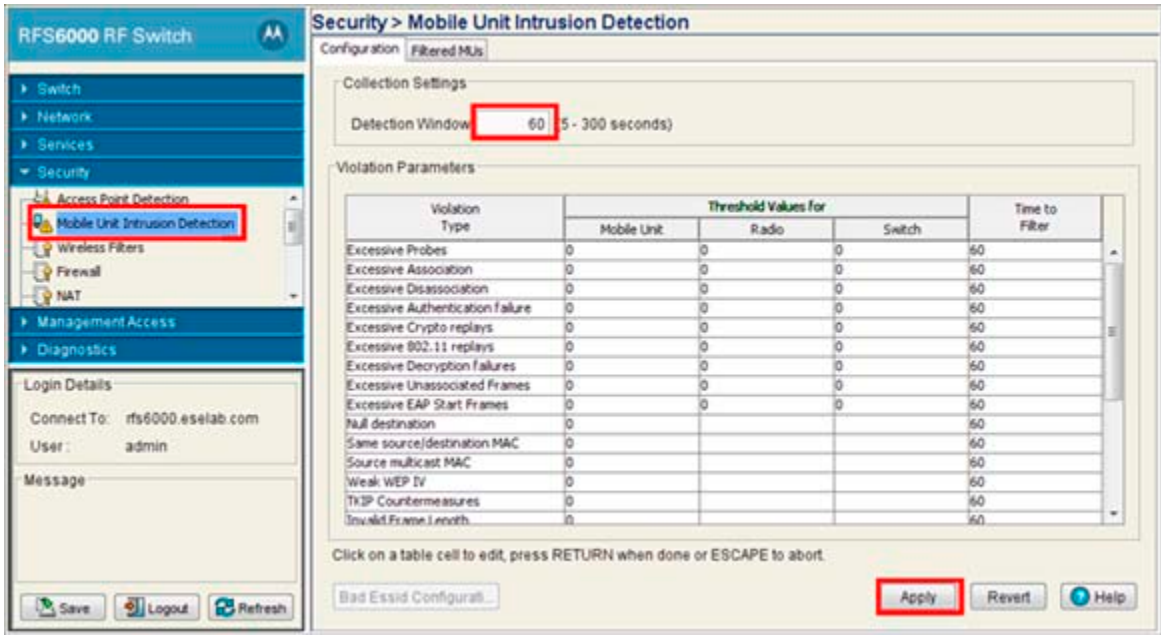
- The global detection window will be increased from 10 seconds to 60 seconds.
- An excessive authentication failure intrusion violation will be configured with a threshold of 10 attempts. If 10 authentication failures occur within a 60 second window, an alarm is generated and mitigation performed.
- The Time to Filter for the excessive authentication failure intrusion violation will be set to 300 seconds. If an MU triggers the intrusion violation, the MUs MAC address is filtered for 5 minutes.



Switch Web UI Configuration

The following configuration example demonstrates how to enable mobile unit intrusion detection for excessive authentication failures:

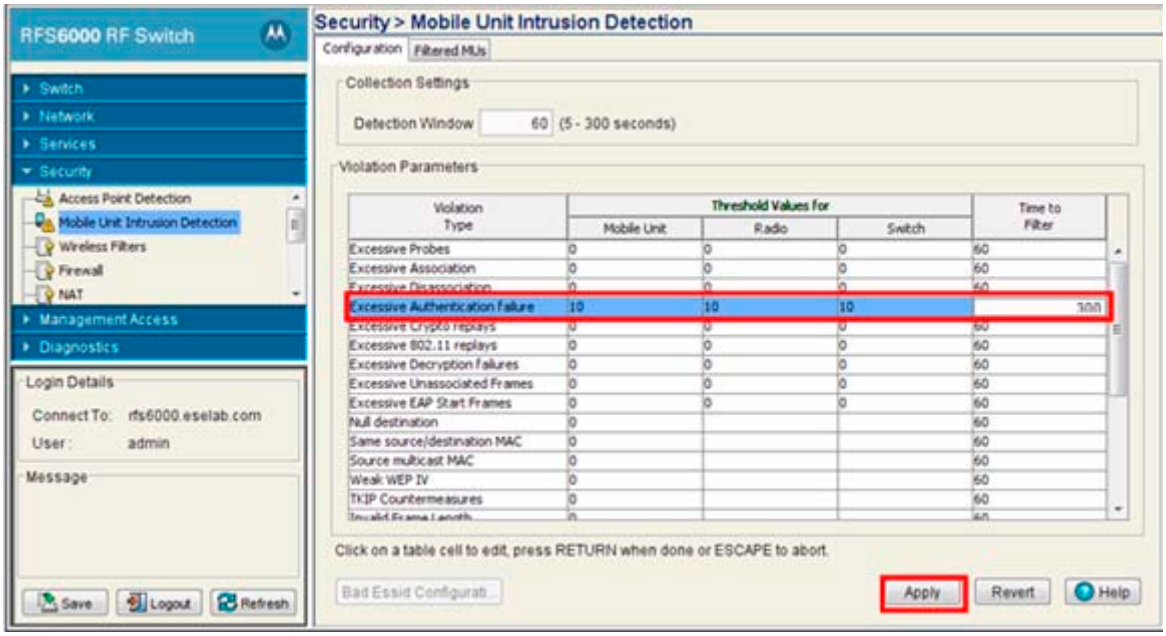
1. From the switch menu tree select **Security** > **Mobile Unit Intrusion Detection.**
2. Select the **Configuration** tab.



3. In the **Detection Window** field, specify the detection window interval (in seconds) the RF Switch uses to scan for violations.

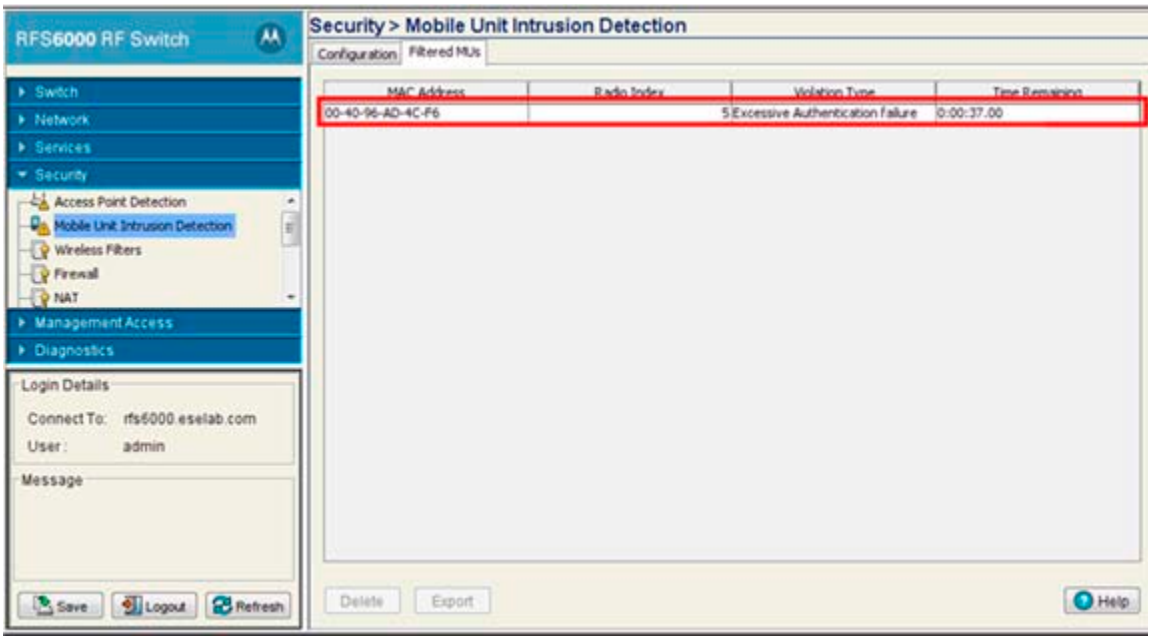
   In this example, a 60 second detection window is defined. Click **Apply**.

4. Within the **Violation Parameters** table, locate **Excessive Authentication failure** then enter a threshold value in the Mobile Unit, Radio and Switch fields.



5. Additionally, in the **Time to Filter** field enter a value (in seconds) the MU will be blacklisted for when violations occur. In this example, the Mobile, Radio and Switch threshold is set to 10. Click **Apply.**

6. Select the **Filtered MUs** tab.

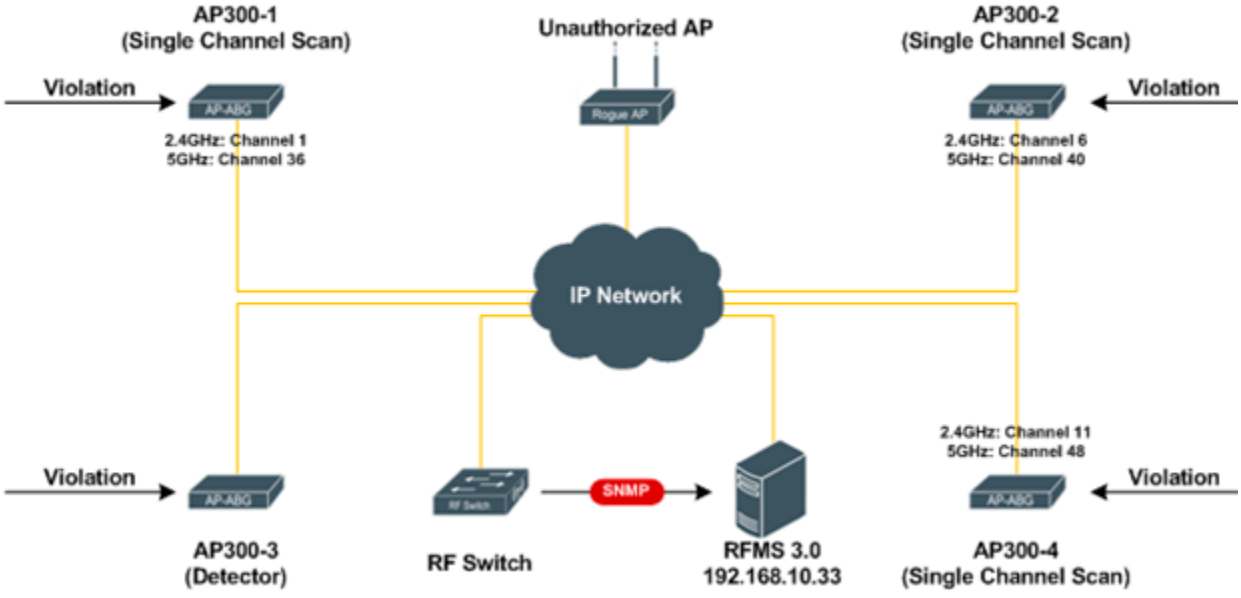


Any MUs violating an event are listed in the table.

7. Select **Save** (from the lower left-hand corner) to apply the changes.

D.7.6.6 SNMP Traps

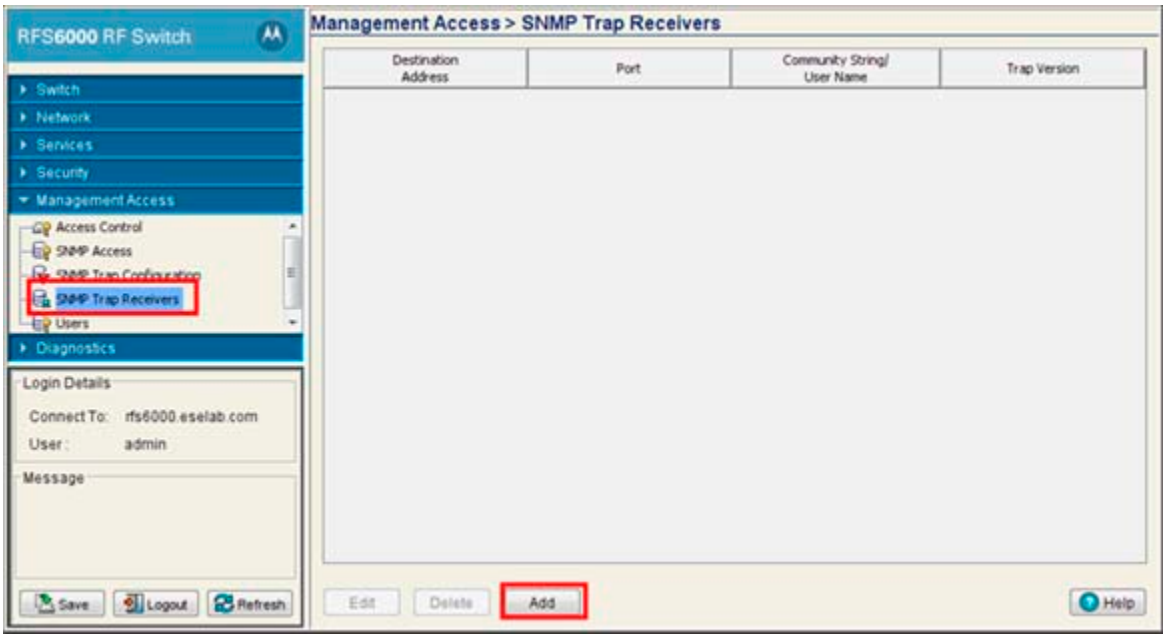
To alert users of unauthorized APs and intrusion events, an RFMS server should defined on the RF Switch as an SNMP trap receiver, and the detection of unauthorized APs and intrusion detection traps should be enabled. When the RF Switch detects an unauthorized AP, or a intrusion detection violation, the switch forwards an SNMP trap to the RFMS server.



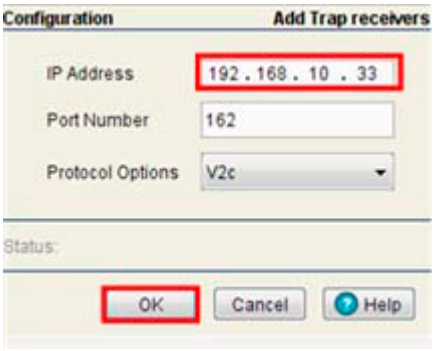
Switch Web UI Configuration

The following configuration example demonstrates how to enable SNMP traps to an RFMS server for unauthorized AP and MU intrusion detection violations:

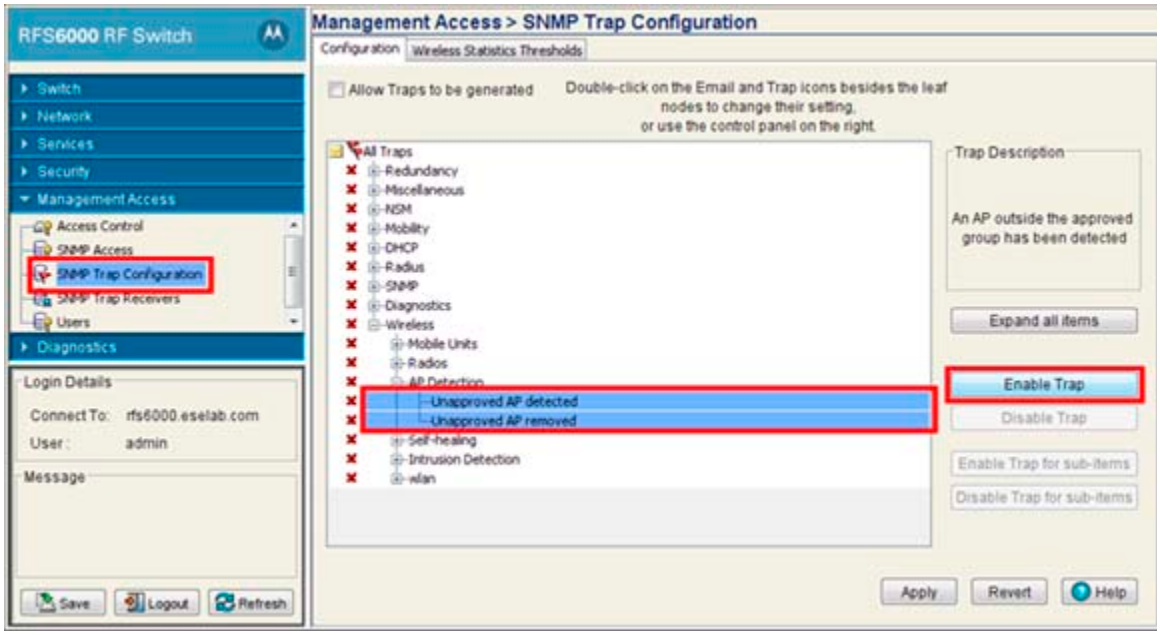
1. From the switch menu tree select **Management Access** > **SNMP Trap Receivers.**
2. Select **Add**.



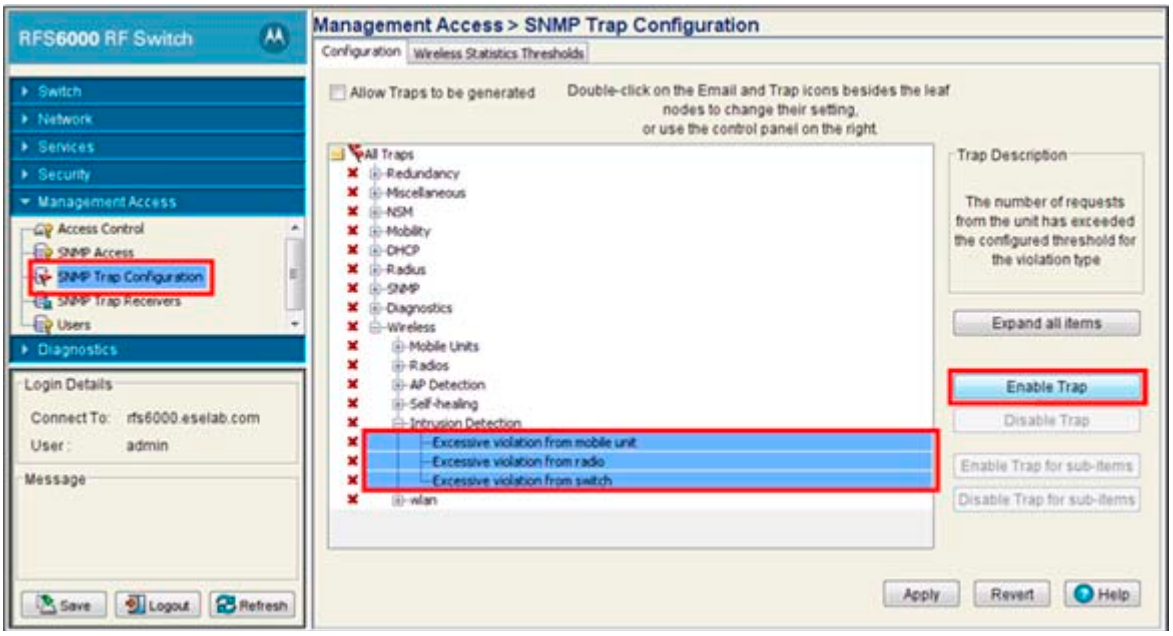
3. Go to **Management Access** > **SNMP Traps**.



4. Enter the **IP Address** of the RFMS server.
5. Under **Protocol Options**, select the SNMP version. Click **OK**.
6. From the menu tree select **Management Access** > **SNMP Trap Configuration**.
7. Select the **Configuration** tab.



8. In the All Traps tree, locate **Wireless** > **AP Detection,** then select the **Unapproved AP detected** and **Unapproved AP removed** traps. Select **Enable Trap**.
9. Click **Apply**.
10. From the menu tree select **Management Access** > **SNMP Trap Configuration.**
11. Select the **Configuration** tab.

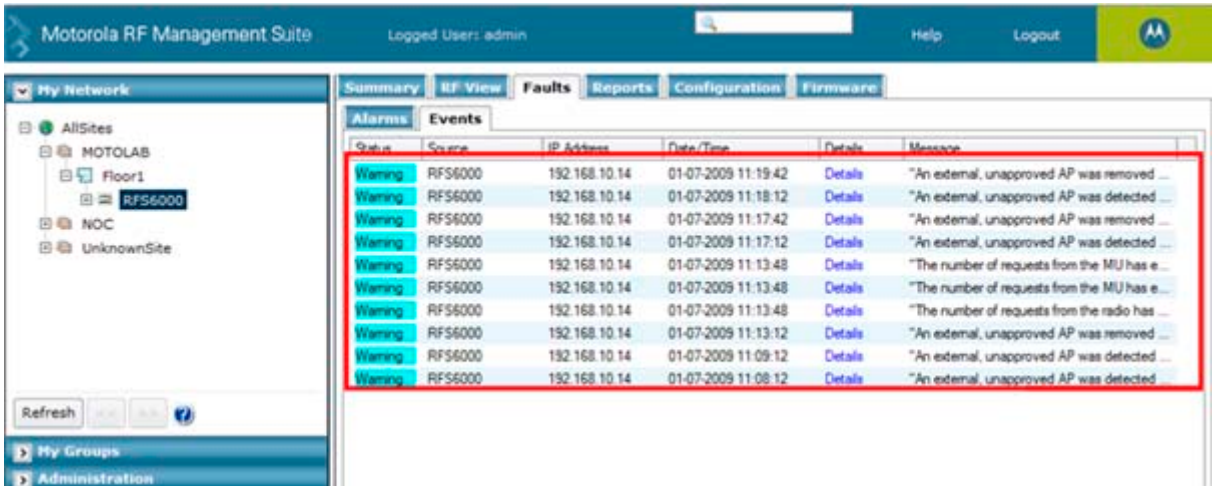


12. In the All Traps tree, locate **Wireless** > **Intrusion Detection,** then select the **Excessive violation from mobile unit**, **Excessive violation from radio** and **Excessive violation from switch** traps. Select **Enable Trap**.
13. Click **Apply.**

14.From within the Configuration tab, select the **Allow Traps to be generated** option then click **Apply**.

15.Select **Save** (from the lower left-hand corner) to apply the changes.

SNMP traps for unauthorized APs and MU intrusion detection violations are forwarded to RFMS.



D.7.6.7 RF Switch Running Configuration

The following is the running configuration on the RFS6000 switch used to create this Wireless IDS tutorial:

```
RFS6000# show running-config

!
! configuration of RFS6000 version 3.3.0.0-029R
!
version 1.2
!
!
aaa authentication login default local none
service prompt crash-info
!
username "admin" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc."
"WLAN Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server community public  ro
snmp-server community private  rw
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
```

```
snmp-server sysname RFS6000
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
snmp-server host 192.168.10.33 v2c
snmp-server enable traps
snmp-server enable traps wireless ap-detection
externalAPDetected
snmp-server enable traps wireless ap-detection externalAPRemoved
snmp-server enable traps wireless ids muExcessiveEvents
snmp-server enable traps wireless ids radioExcessiveEvents
snmp-server enable traps wireless ids switchExcessiveEvents
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
timezone America/New_York
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d04677
7fbed80f433b68ea
!
wireless
 secure-wispe-default-secret 0 new-pre-shared-key
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
```

```
wlan 1 dot11i preauthentication
wlan 2 enable
wlan 2 description MOTO-GUEST
wlan 2 ssid MOTO-GUEST
wlan 2 vlan 70
wlan 2 authentication-type hotspot
wlan 2 hotspot webpage-location advanced
wlan 2 radius server primary 192.168.10.14
wlan 2 radius server primary radius-key 0 ESELAB
wlan 2 radius accounting server primary 192.168.10.14
wlan 2 radius accounting server primary radius-key 0 ESELAB
wlan 3 enable
wlan 3 description MOTO-VOICE
wlan 3 ssid MOTO-VOICE
wlan 3 vlan 80
wlan 3 encryption-type tkip
wlan 3 dot11i phrase 0 motovoicetest
wlan 3 dot11i preauthentication
radio add 1 00-15-70-78-F5-23 11a ap300
radio 1 description AP300-1-A
radio 1 bss 1 1
radio 1 channel-power indoor 36 15
radio 1 on-channel-scan
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
```

```
 radio 4 bss 3 3
 radio 4 channel-power indoor 6 18
 radio 4 on-channel-scan
 radio 4 short-preamble
 radio 4 adoption-pref-id 200
 radio add 5 00-15-70-B2-FD-D0 11a ap300
 radio 5 description AP300-3-A
 radio 5 bss 1 1
 radio 5 channel-power indoor 44 15
 radio 5 detector
 radio 5 adoption-pref-id 100
 radio add 6 00-15-70-B2-FD-D0 11bg ap300
 radio 6 description AP300-3-BG
 radio 6 bss 1 1
 radio 6 bss 2 2
 radio 6 bss 3 3
 radio 6 channel-power indoor 11 18
 radio 6 detector
 radio 6 short-preamble
 radio 6 adoption-pref-id 100
 radio add 7 00-15-70-D5-DA-CE 11a ap300
 radio 7 description AP300-4-A
 radio 7 bss 1 1
 radio 7 channel-power indoor 48 17
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 bss 1 1
 radio 8 bss 2 2
 radio 8 bss 3 3
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 no ap-ip default-ap switch-ip
 ap-detection enable
 ids detect-window 60
 ids ex-ops authentication-fails threshold mu 10
 ids ex-ops authentication-fails threshold radio 10
 ids ex-ops authentication-fails threshold switch 10
 ids ex-ops authentication-fails filter-ageout 300
 ap-containment enable
 ap-containment add 00-19-69-EF-88-6F
!
```

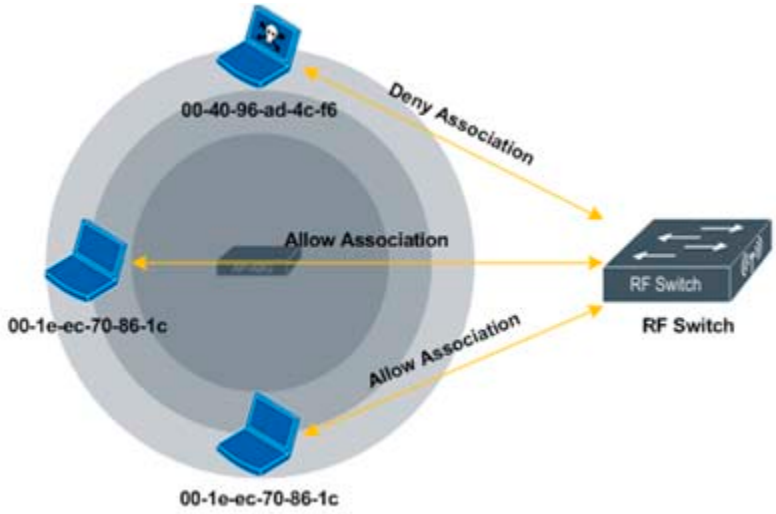
```
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
!
radius-server local
 authentication eap-auth-type all
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
switchport access vlan 10
```

```
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
interface vlan1
 no ip address
 shutdown
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
!
interface vlan70
 description GUEST
 ip address 192.168.70.14/24
!
!
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
end
```

D.8 Wireless Filters

Wireless filters can be applied to specific WLANs to grant or deny access to MUs based on individual or ranges of MAC addresses. Wireless filters may be applied to one or more WLANs and are used to grant or deny access to MUs during association.

Wireless filters can be used for multiple applications including blacklisting malicious devices as well as providing an additional layer of security less secure WLANs by restricting access to specific devices. Wireless filters may be applied to the RF Switch using the CLI and Web UI or from an Motorola AirDefense Enterprise server when a threat is detected.



Wireless filters can be used for multiple applications including blacklisting malicious devices as well as providing an additional layer of security for less secure WLANs by restricting access to specific devices. Wireless filters can be applied to the RF Switch using the CLI or switch Web UI or from an AirDefense Enterprise server.

Wireless filters are only used to allow or deny MUs from associating with a WLAN, and are not intended to filter layer 2 traffic passing through the switch. To restrict or limit traffic at layer 2, MAC firewall rules can be created to permit or deny traffic based on specific (or wildcard) source or destination MAC addresses.

D.8.1 Configuring a Wireless Filter

The following sections outline the configuration steps required to enable wireless filters on a switch:

- *Wireless Filters that Deny*
- *Wireless Filters that Allow*

  To view the running configuration on the RFS6000 switch used to create this wireless filter tutorial, refer to *RF Switch Running Configuration on page D-120*.

D.8.1.1 Requirements

The following requirements must be met prior to attempting the wireless filter configuration described in this section:

- One (or more) RF Switches are installed and operational on the network
- One (or more) Access Ports configured and adopted by the RF Switch

- One (or more) WLAN profiles are configured and assigned to adopted radios
- A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration and verify secure management operations
- One (or more) wireless workstations are available to test and verify the wireless filters

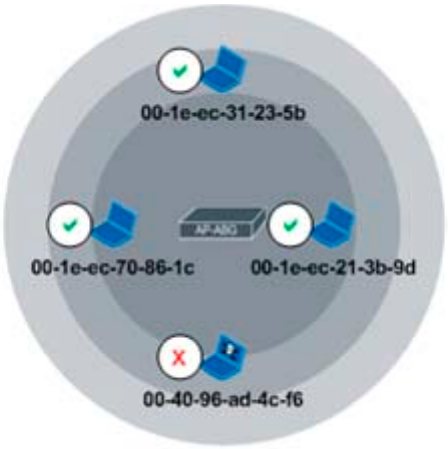
D.8.1.2 Components

The information in this section is based on the following Motorola hardware and software versions:

- 1 RFS6000 model switch
- 5 AP300 model Access Ports

D.8.1.3 Wireless Filters that Deny

Wireless filters can be used to block devices. A common scenario is to block (blacklist) associations from a suspicious or malicious device. Administrators can create up to 1000 wireless filter entries on the RF Switch which can deny access to individual MAC addresses or range of MAC addresses as required. All MAC addresses not matched by the wireless filter list can associate to the WLAN.

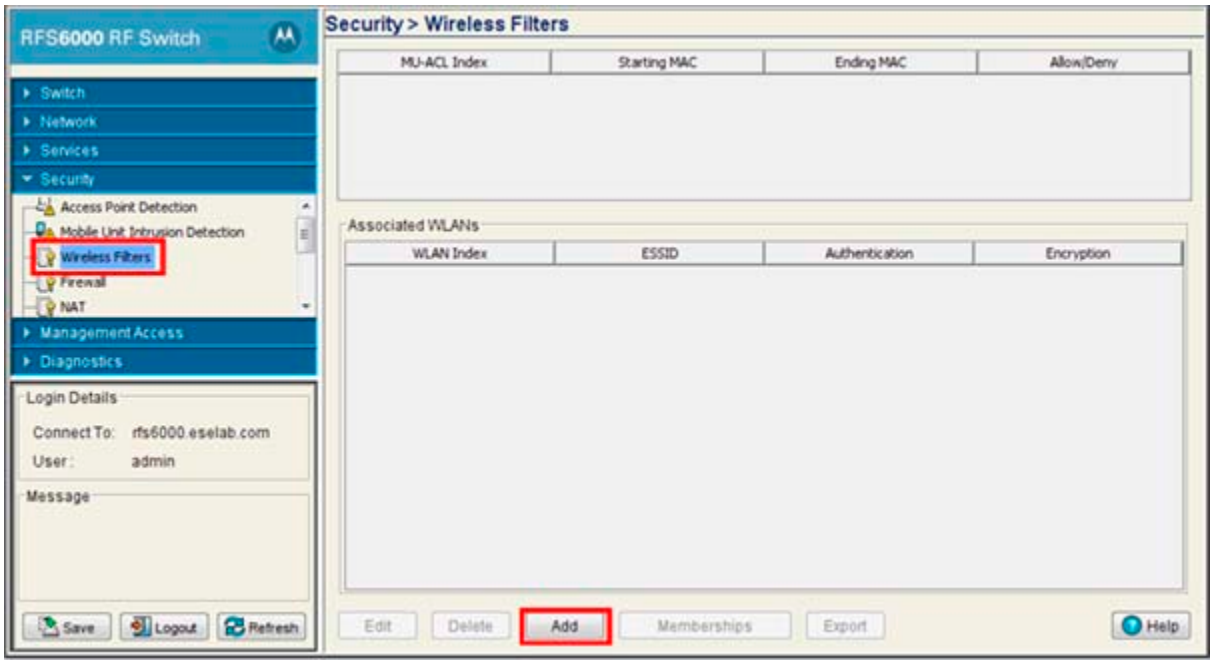


ACL Index	*Start MAC*	*End MAC*	*Allow / Deny*	*WLAN*
1	00-40-96-ad-4c-f6	00-40-96-ad-4c-f6	Deny	MOTO-GUEST

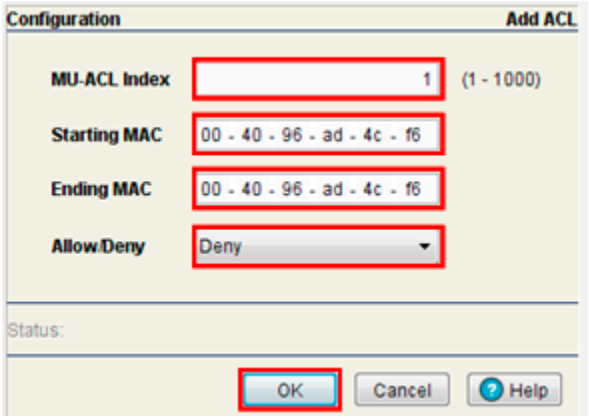
As illustrated in the figure above, wireless filtering is deployed on a guest WLAN (named MOTO-GUEST) to block a device with the MAC address 00-40-96-ad-4c-f6. A wireless filter has been created on the RF Switch with a Start MAC and End MAC set to a specific device address. If the device attempts to associate with the MOTO-GUEST SSID, the RF Switch denies the association attempt and a logs an entry for the association attempt.

To blacklist a single client MAC address on a WLAN using the switch Web UI:

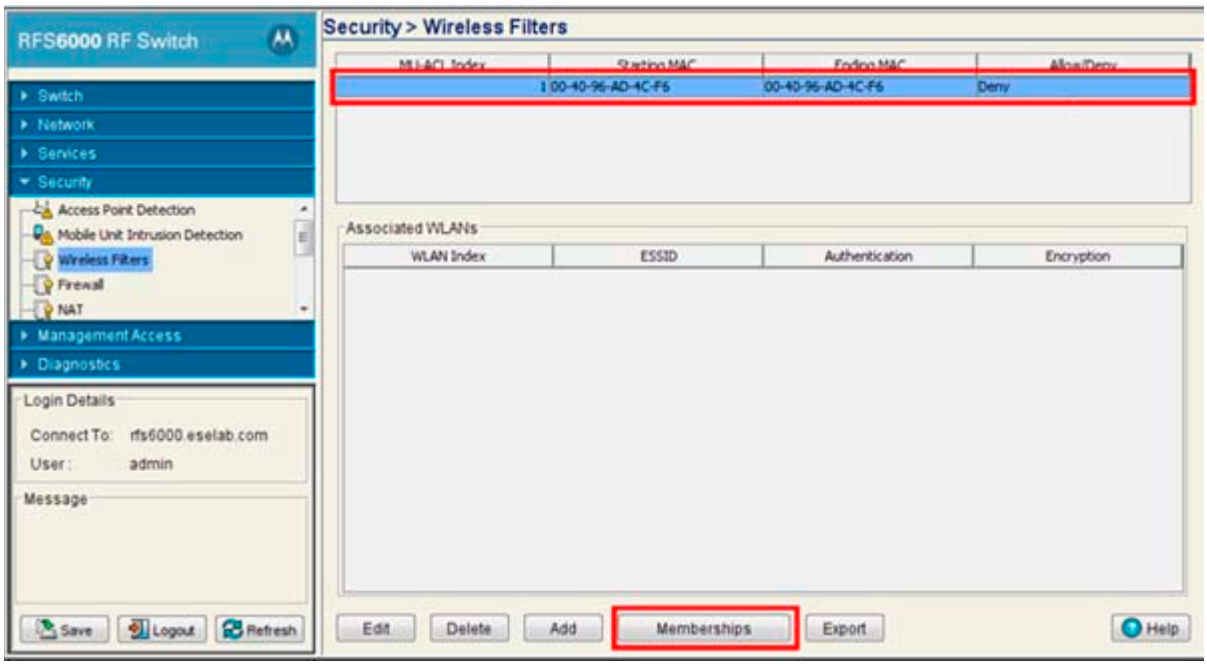
1. From the menu tree select **Security** > **Wireless Filters**.



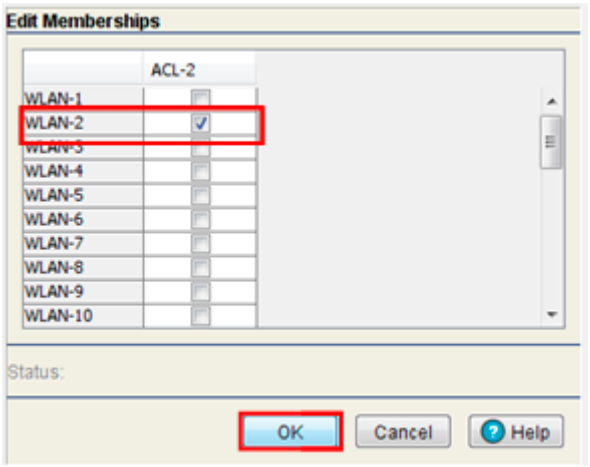
2. Select **Add**.



3. Enter 1 in the **MU-ACL Index** field.
4. In the **Starting MAC** and **Ending MAC** fields enter the MAC address of the client to block.
5. Set the **Allow/Deny** option to **Deny**. Click **OK**.



6. Highlight the MU-ACL created in steps 3-5 and select **Memberships**.



7. Check the WLAN index number(s) to associate the MAC-ACL with.

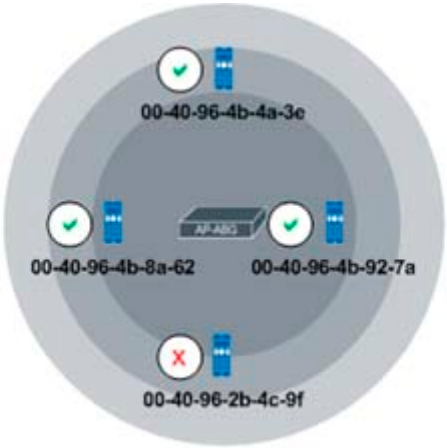
   In this example the MAC-ACL is associated with MOTO-GUEST WLAN-2. Click **OK**.

8. Select **Save** (from the lower left-hand corner) to apply the changes.

D.8.1.4 Wireless Filters that Allow

Wireless filters can also be used to allow access to a specific group of devices such as mobile handhelds or VoIP handsets while blocking associations to other devices. Since most enterprises typically deploy mobile devices from a common vendor, the vendors OUI can be leveraged in a wireless filter to restrict access to a range of vendor devices. Since no implicit deny is provided, an additional wireless filter must be created after the allow filter to block access from all other vendor devices.

NOTE: A current list of vendor assigned OUIs can be downloaded directly from the IEEE web site: *http://standards.ieee.org/regauth/oui/iab.txt.*



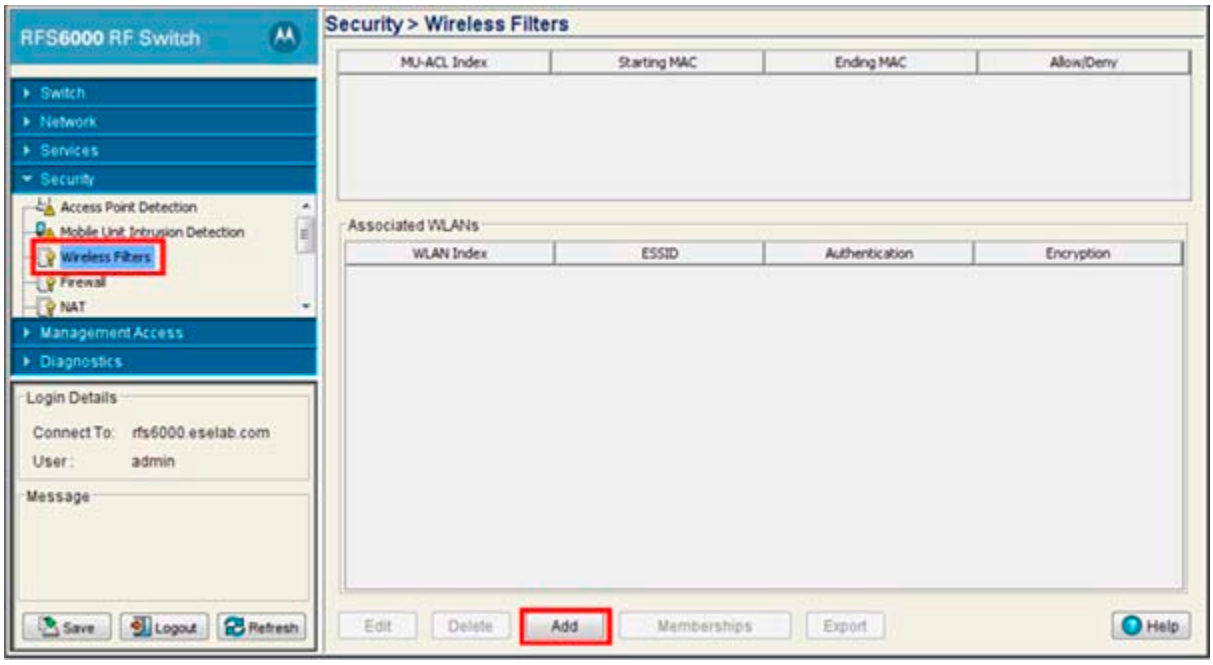
ACL Index	*Start MAC*	*End MAC*	*Allow / Deny*	*WLAN*
1	00-40-96-4b-00-00	00-40-96-4b-ff-ff	Allow	MOTO-VOICE
2	00-00-00-00-00-01	ff-ff-ff-ff-ff-f2	Deny	MOTO-VOICE

As illustrated in the figure above, wireless filtering is deployed on a voice WLAN named MOTO-VOICE to only allow select SpectraLink VoIP handsets to associate with the WLAN. The first wireless filter has been created on the RF Switch allowing a range of MAC addresses (00-40-96-4b-00-00 through 00-40-96-4b-ff-ff) to associate with the WLAN. A second *catch all* wireless filter has been created denying access to all MAC addresses from 00-00-00-00-00-01 through ff-ff-ff-ff-ff-fe.

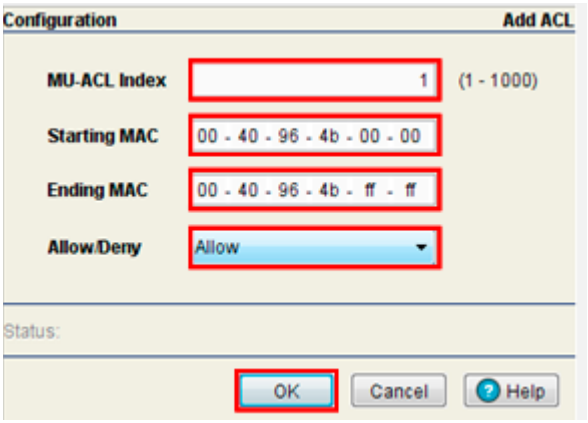
In this example, a device with a MAC address that matches the range in the allow list is allowed to associate with the WLAN. Devices which do not match the allowed list will be denied association from the RF Switch and a log entry for the association attempt is made.

To allow a range of MAC addresses on a WLAN:

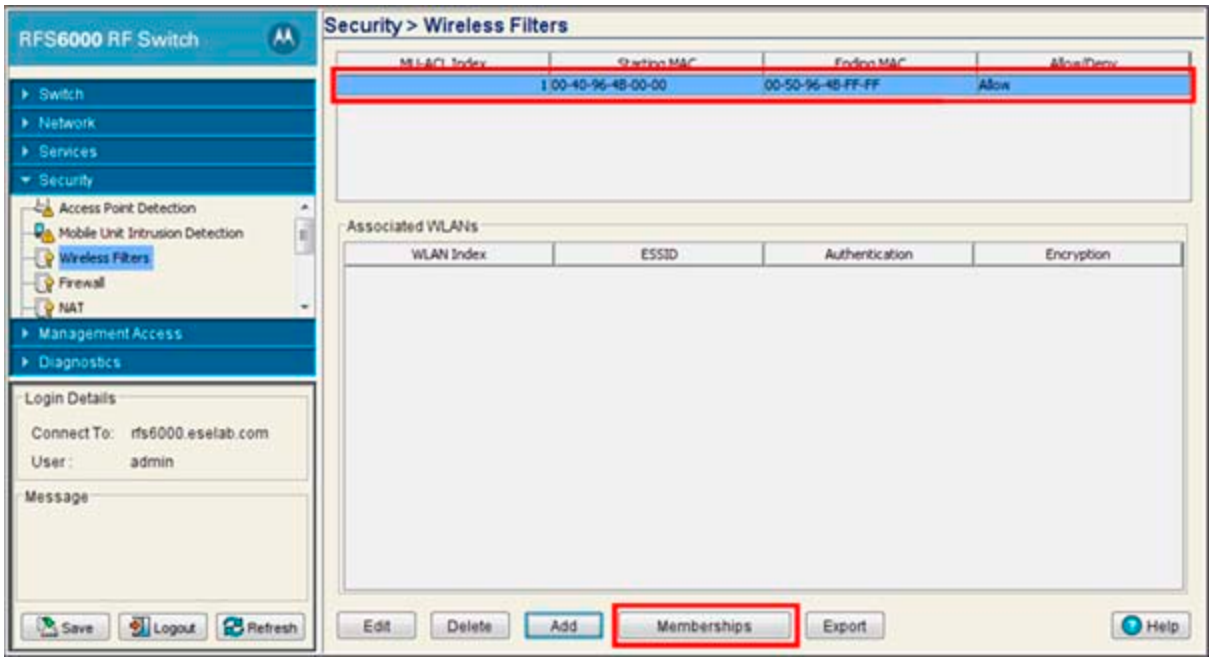
1. From the menu tree select **Security** > **Wireless Filters**.



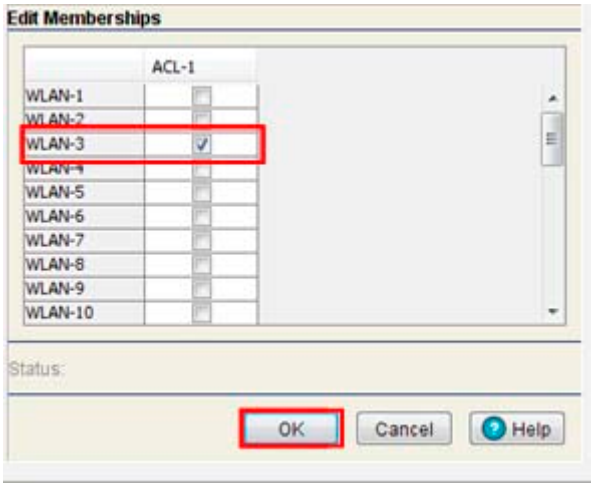
2. Select **Add**.



3. Enter 1 in the **MU-ACL Index** field.
4. In the **Starting MAC** field enter the first MAC address in the range. In the **Ending MAC** field enter the last MAC address in the range.
5. Set the **Allow/Deny** option to **Allow**. Click **OK**.



6. Highlight the MU-ACL created in steps 3-5 and select **Memberships**.



7. Check the WLAN index number(s) to associate the MAC-ACL with.

   In this example the MAC-ACL has been associated with MOTO-VOICE WLAN-3. Click **OK**.

8. Select **Save** (from the lower left-hand corner) to apply the changes.

D.8.1.5 RF Switch Running Configuration

The following is the running configuration on the RFS6000 switch used to create this wireless filter tutorial:

```
RFS6000# show running-config
!
! configuration of RFS6000 version 3.3.0.0-029R
!
version 1.2
```

```
!
!
aaa authentication login default local none
service prompt crash-info
!
username "admin" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1
b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc."
"WLAN Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
```

```
ip ssh
ip telnet
no service pm sys-restart
timezone America/New_York
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d04677
7fbed80f433b68ea
!
wireless
 secure-wispe-default-secret 0 new-pre-shared-key
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type tkip
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 radius accounting server primary 192.168.10.5
 wlan 1 radius accounting server primary radius-key 0 ESELAB
 wlan 1 dot11i preauthentication
 wlan 2 enable
 wlan 2 description MOTO-GUEST
 wlan 2 ssid MOTO-GUEST
 wlan 2 vlan 70
 wlan 2 authentication-type hotspot
 wlan 2 hotspot webpage-location advanced
 wlan 2 radius server primary 192.168.10.14
 wlan 2 radius server primary radius-key 0 ESELAB
 wlan 2 radius accounting server primary 192.168.10.14
 wlan 2 radius accounting server primary radius-key 0 ESELAB
 wlan 3 enable
 wlan 3 description MOTO-VOICE
 wlan 3 ssid MOTO-VOICE
 wlan 3 vlan 80
 wlan 3 encryption-type tkip
 wlan 3 dot11i phrase 0 motovoicetest
 wlan 3 dot11i preauthentication
 radio add 1 00-15-70-78-F5-23 11a ap300
```

```
radio 1 description AP300-1-A
radio 1 bss 1 1
radio 1 channel-power indoor 36 15
radio 1 on-channel-scan
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
radio 5 description AP300-3-A
radio 5 bss 1 1
radio 5 channel-power indoor 44 15
radio 5 on-channel-scan
radio 5 adoption-pref-id 100
radio add 6 00-15-70-B2-FD-D0 11bg ap300
radio 6 description AP300-3-BG
radio 6 bss 1 1
radio 6 bss 2 2
radio 6 bss 3 3
radio 6 channel-power indoor 11 18
radio 6 on-channel-scan
radio 6 short-preamble
```

```
 radio 6 adoption-pref-id 100
 radio add 7 00-15-70-D5-DA-CE 11a ap300
 radio 7 description AP300-4-A
 radio 7 channel-power indoor 48 17
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 radio add 9 00-15-70-D5-DA-FB 11a ap300
 radio 9 description AP300-5-A
 radio 9 channel-power indoor 149 20
 radio 9 on-channel-scan
 radio add 10 00-15-70-D5-DA-FB 11bg ap300
 radio 10 description AP300-5-BG
 radio 10 channel-power indoor 6 4
 radio 10 on-channel-scan
 no ap-ip default-ap switch-ip
 mac-auth-local 1 deny 00-40-96-AD-4C-F6  00-40-96-AD-4C-F6 2
 mac-auth-local 2 allow 00-40-96-4B-00-00  00-40-96-4B-FF-FF 3
 ap-detection enable
!
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
!
radius-server local
 authentication eap-auth-type all
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
```

```
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
switchport access vlan 10
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
interface vlan1
 no ip address
 shutdown
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
```

```
!
interface vlan70
 description GUEST
 ip address 192.168.70.14/24
!
!
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
end
```

D.9 802.11i Support

The IEEE 802.11i standard (ratified in 2004) provides enhanced security for WLANs. 802.11i supersedes the initial 802.11 *Wired Equivalent Privacy* (WEP) security specification, which was shown to have severe security weaknesses. The 802.11i standard improves WLAN security by implementing the *Temporal Key Integrity Protocol* (TKIP) and *Advanced Encryption Standard* (AES) for encryption and data integrity. 802.11i amends the original 802.11 standard by mandating authentication using either 802.1X authentication or pre-shared keys.

The Wi-Fi Alliance organization created the *Wi-Fi* brand. The Wi-Fi Alliance promotes and certifies WLAN product inter-operability and promotes them as the global WLAN standard across all market segments. The Wi-Fi Alliance has instituted a test suite that defines how member products are tested to certify they are interoperable with other Wi-Fi certified products.

During the 802.11i standard ratification, the Wi-Fi alliance introduced *Wi-Fi Protected Access* (WPA) as an intermediate solution to address WEP vulnerabilities. WPA uses TKIP for encryption and dynamic encryption key generation. WPA was also designed to be supported on existing WLAN infrastructures without hardware upgrades.

Wi-Fi Protected Access 2 (WPA2) is the next generation of Wi-Fi security, based on the final 802.11i standard supporting AES. The new AES encryption mechanism introduced in 802.11i generally requires a hardware upgrade from earlier versions of WLAN clients and APs, however all current shipping Motorola RF Switches and Access Ports / Access Points support WPA2.

D.9.1 Applications

802.11i with AES should be considered for new WLAN applications, as it represents the strongest encryption scheme available today for data privacy. 802.11i with AES encryption is supported by all new WLAN client devices including workstations, handhelds and voice handsets.

For legacy deployments, which include devices that cannot support AES, Motorola recommends TKIP with 802.1x or pre-shared-keys be utilized. TKIP is supported by most (but not all) legacy devices via a software update provided by the device manufacturer.

For legacy devices that cannot support AES or TKIP, dynamic WEP or VPN should be considered. Static WEP should only be considered when no other encryption options are available and should be augmented with firewalls to reduce the attack footprint.

D.9.2 Restrictions

WPA/802.11i provides support for pre-shared-keys as an alternative to 802.1x. A pre-shared-key is typically entered as an 8 - 63 character passphrase on the WLAN infrastructure. The client must know the pre-shared key before being permitted access to the WLAN.

WPA and 802.11i pre-shared-key implementations are potentially suspect to dictionary attacks when short, or weak, passphrases are used. This vulnerability is not the fault of WPA/802.11i, and can be thwarted by implementing strong passphrases utilizing 20 or more random alphanumerical and special characters. Random passphrase generators are available on the Web and can generate strong random passphrases of varying complexity.

Attacks can also be thwarted by implementing MU intrusion detection on the RF Switch, which alert administrators of excessive authentication failures and provides automatic mitigation against attacking devices.

Finally, as a general best practices it's also recommended to frequently refresh passphrases. The frequency of the refresh should depend on each specific environment, as passphrases will also need to be updated on the client devices.

D.9.3 Configuring 802.11i Support

The following sections outline the steps required to configure 802.11i with 802.1X and pre-shared keys on a RF Switch:

- *802.11i with 802.1x Authentication*
- *802.11i with Pre-Shared Key Authentication*

To review the running configuration deployed on the RF Switch used to create this tutorial, see *RF Switch Running Configuration on page D-135*.

D.9.3.1 Requirements

The following requirements must be met prior to attempting this configuration:

- One (or more) RF Switches be installed and operational on the network
- One (or more) Access Ports be configured and adopted by the RF Switch
- A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform the Web UI configuration
- One (or more) wireless workstations be available to verify 802.11i 802.1X and PSK operation

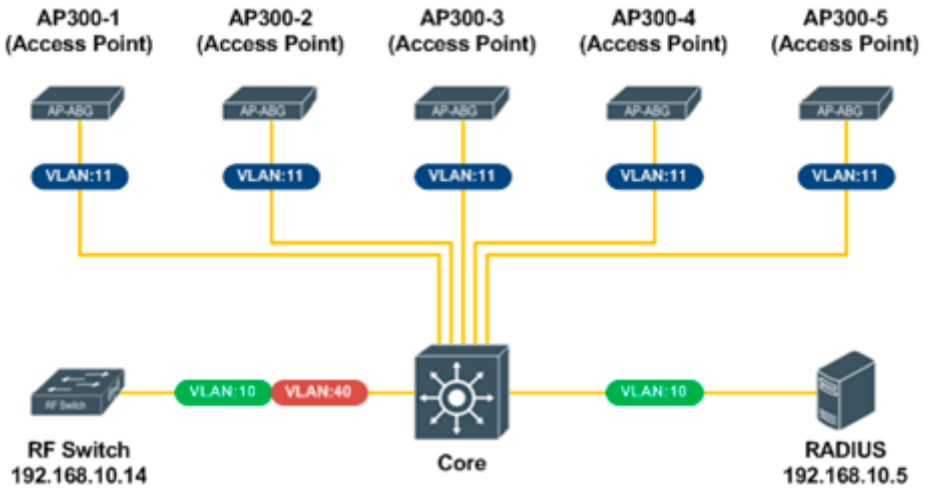
D.9.3.2 Components

The information in this section is based on the following Motorola hardware and software versions:

- 1 RFS6000 model switch
- 5 AP300 model Access Ports

D.9.3.3 802.11i with 802.1x Authentication

As depicted in the illustration below, five AP300s have been deployed at a site supported by a single RF Switch. A WLAN named MOTO-DATA has been created to provide secure 802.11i 802.1X authenticated access for Enterprise data users. Authentication is provided using an external Microsoft IAS Radius server configured with a remote access policy for PEAP authentication. Since this site is small, all authenticated data users are statically mapped to data VLAN 40. However, dynamic VLAN assignments can be enabled at a later date if required.

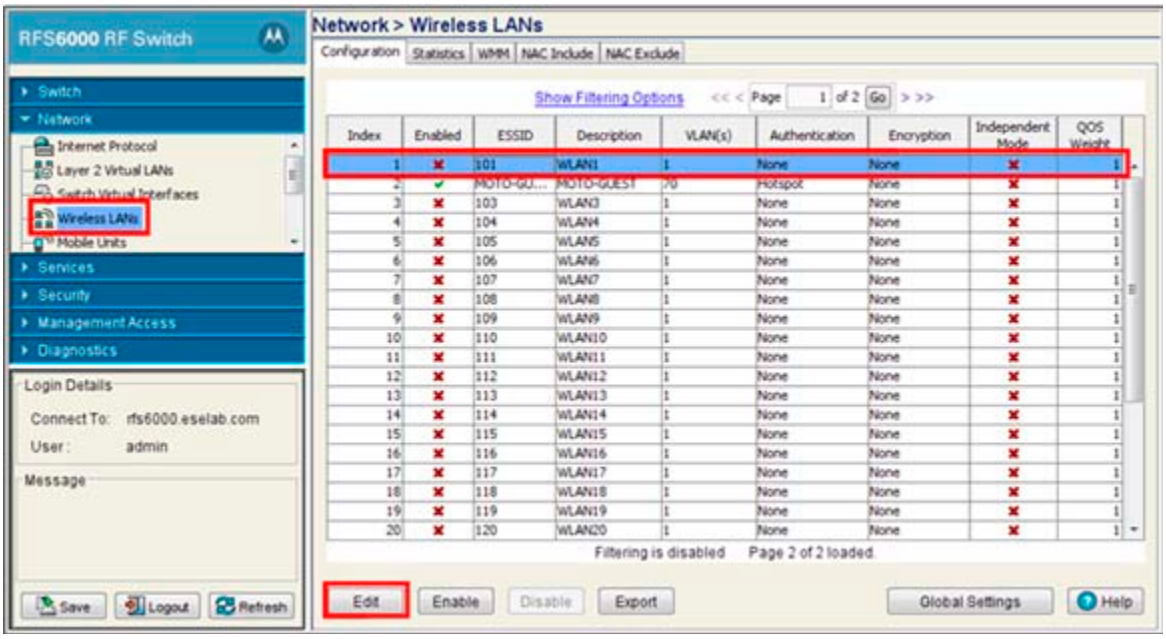


WLAN	*ESSID*	*VLAN(s)*	*Authentication*	*Encryption*
1	MOTO-DATA	40	802.1x	CCMP

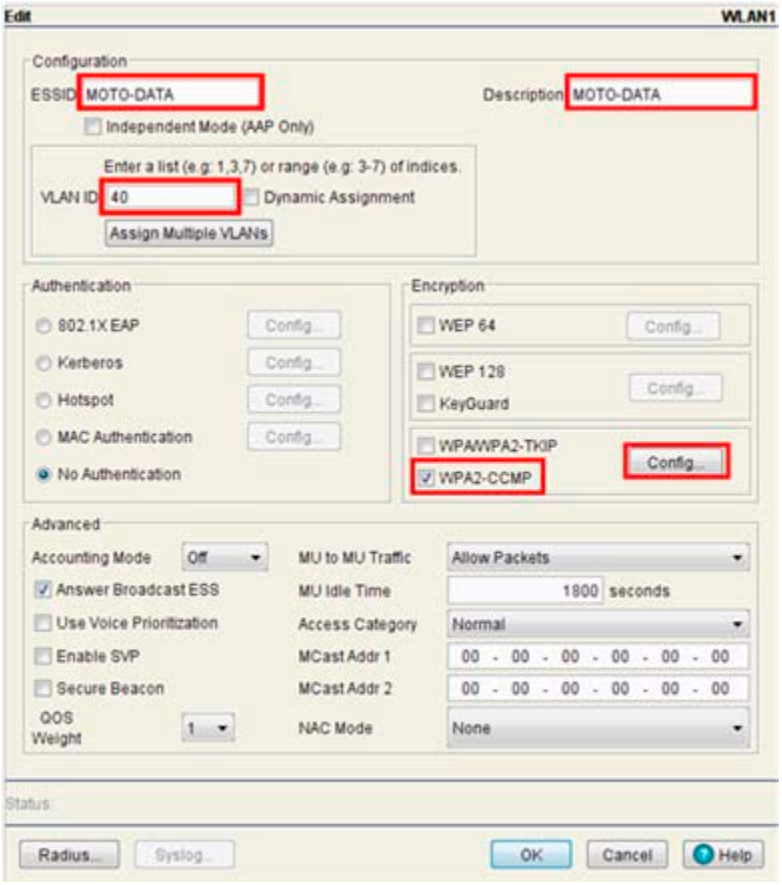
Switch Web UI Configuration

To configure 802.11i with 802.1X on a RF Switch:

1. From the menu tree select **Network** > **Wireless LANs**.
2. Select the **Configuration** tab.



3. Highlight an unused WLAN in the table and select **Edit**.

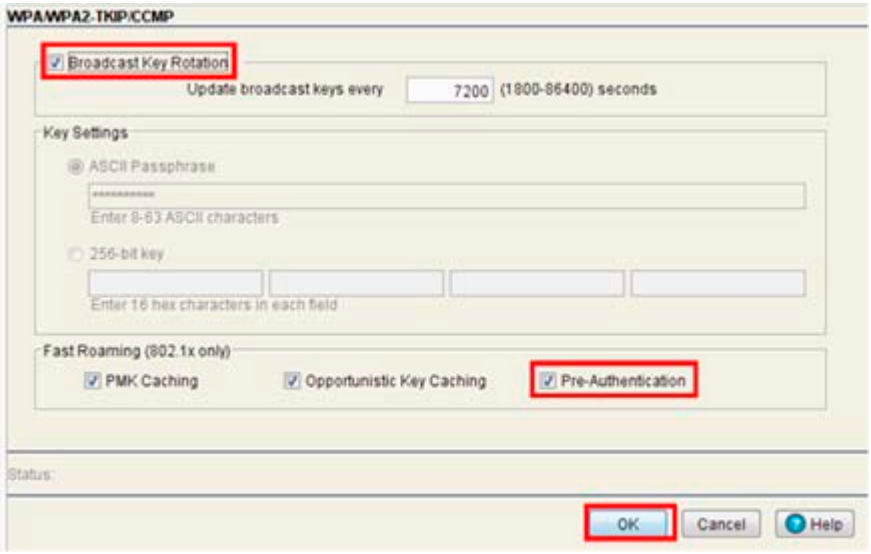


4. Enter an **ESSID** and **Description**.

5. Specify one or more **VLAN IDs**.

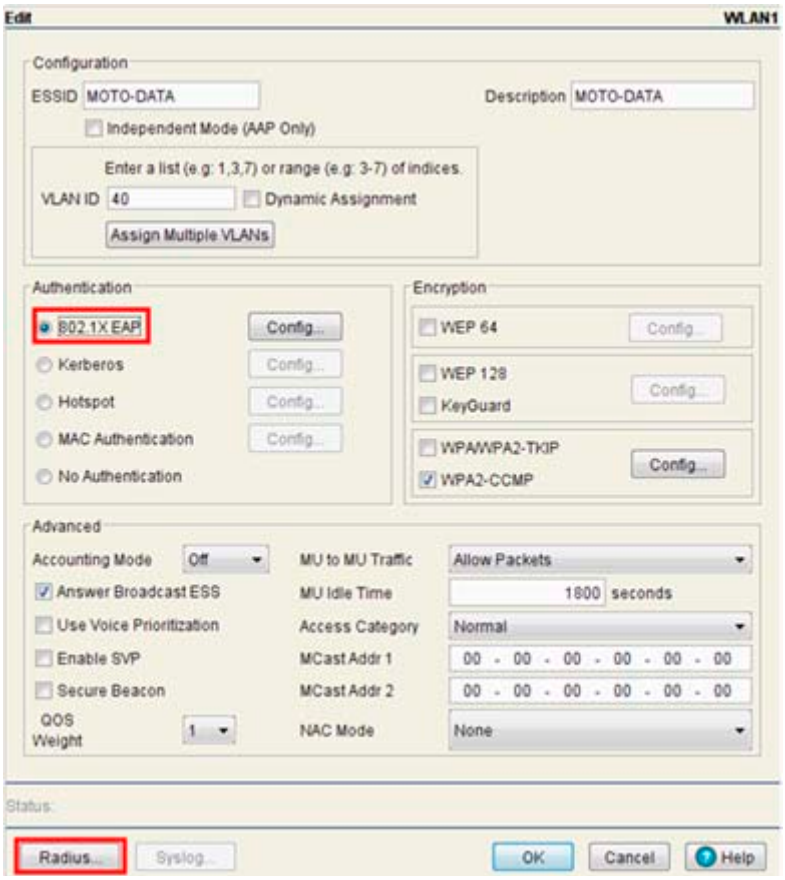
   Optionally enable **Dynamic Assignment** to enable dynamic VLAN assignments from a Radius server.

6. In the **Encryption** field, enable **WPA2-CCMP** then select the **Config** button.

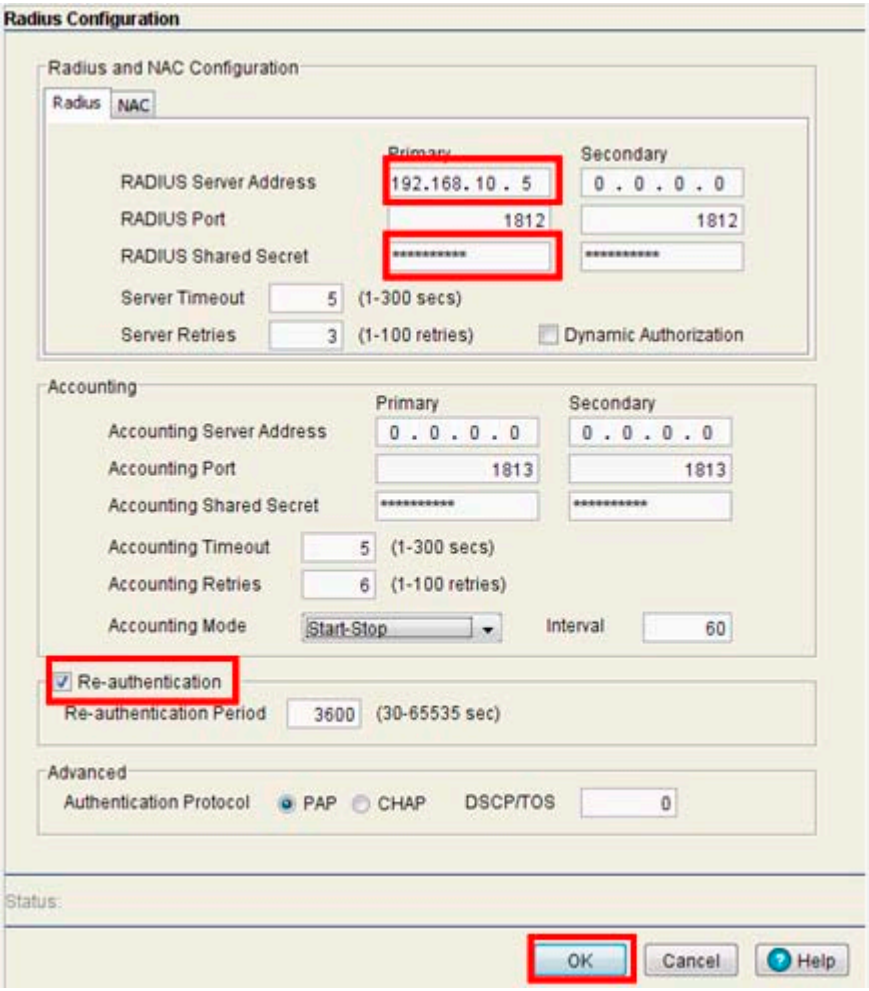


7. Optionally enable the **Broadcast Key Rotation** and **Pre-Authentication** options. Select **OK** to save the updates.

8. Navigate back to the **Network** > **Wireless LANs** > **Edit** screen.

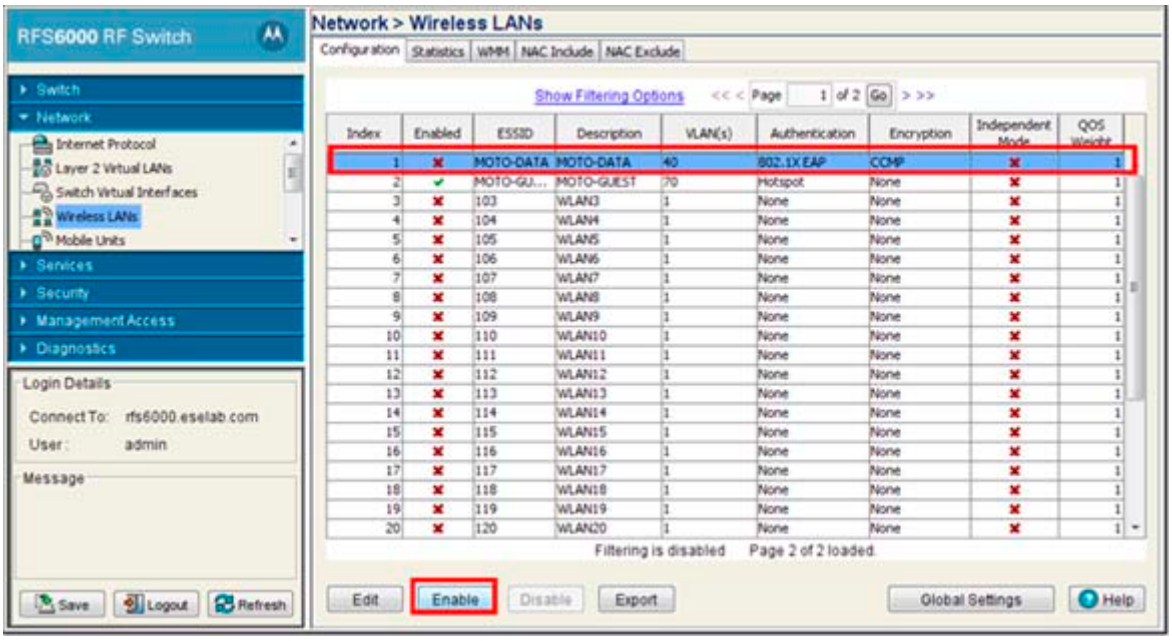


9. Enable the **802.1X EAP Authentication** option and select the **Radius...** button.



10.Enter the **RADIUS Server Address** and **RADIUS Shared Secret**.

11.Select the **Re-authentication** option then select **OK**.



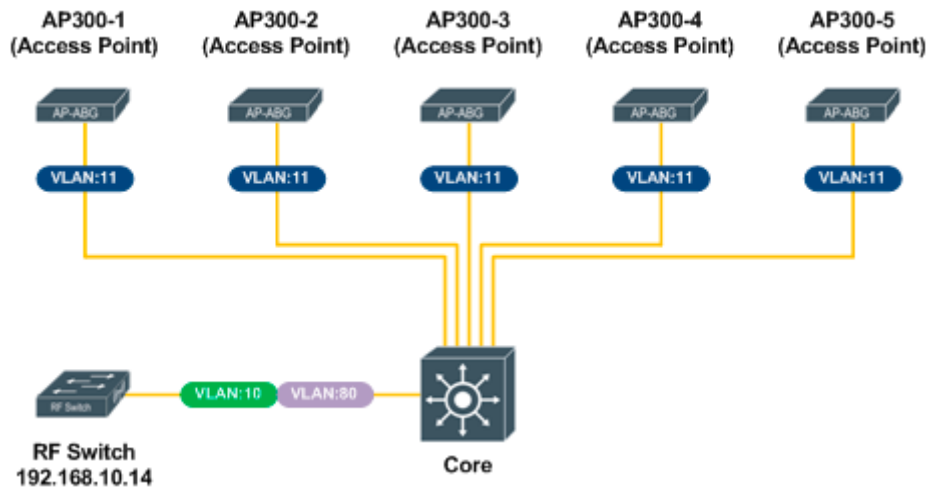
12. From back at the **Network** > **Wireless LANs** > **Configuration** screen, highlight (select) the newly created WLAN and select **Enable**.

    If global WLAN manual mapping is enabled, manually assign the new WLAN to each radio you wish to support. If this global option is disabled, the switch automatically assigns the WLAN to each adopted radio.

13. Select **Save** (from the lower left-hand corner) to apply the changes.

D.9.3.4 802.11i with Pre-Shared Key Authentication

As depicted in illustration below, five AP300s are deployed at a site with a single RF Switch. A WLAN named MOTO-VOICE has been created to provide secure 802.11i pre-shared-key authenticated access for Wi-Fi voice handsets. All authenticated voice handsets are statically mapped to voice VLAN 80.



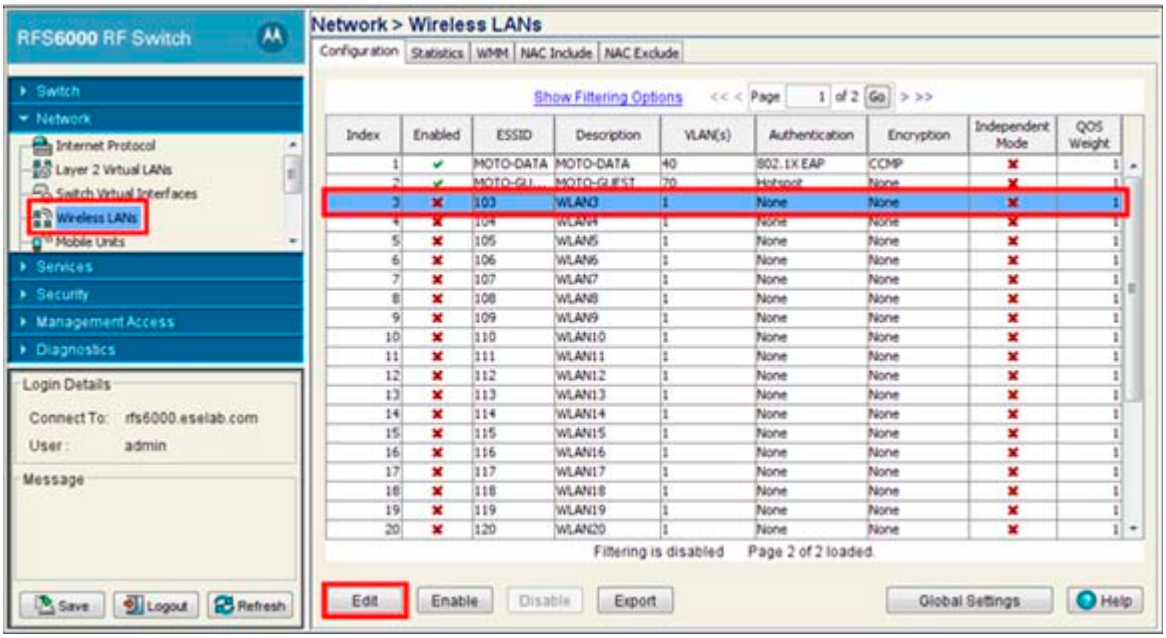
WLAN	*ESSID*	*VLAN(s)*	*Authentication*	*Encryption*
3	MOTO-VOICE	80	Pre-Shared Key	CCMP

NOTE: For optimal security, Motorola recommends selecting an ASCII passphrase of 20 - 63 characters that contains a mix of numerical, alpha numerical, case and special characters.

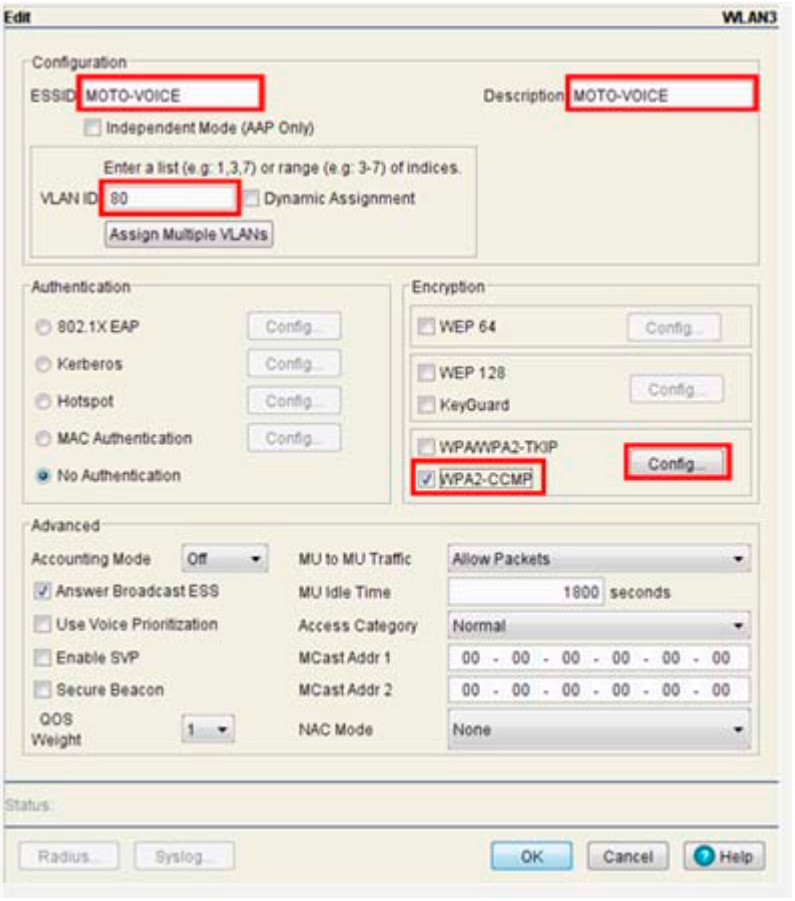
Switch Web UI Configuration

To configure 802.11i with pre-shared keys on a RF Switch:

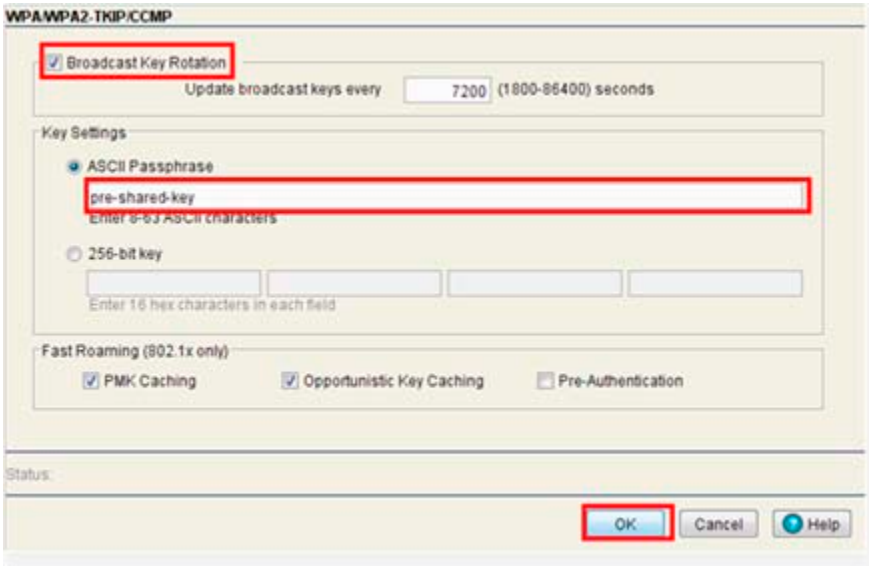
1. From the menu tree select **Network** > **Wireless LANs**.
2. Select the **Configuration** tab.



3. Highlight an unused WLAN and select **Edit**.

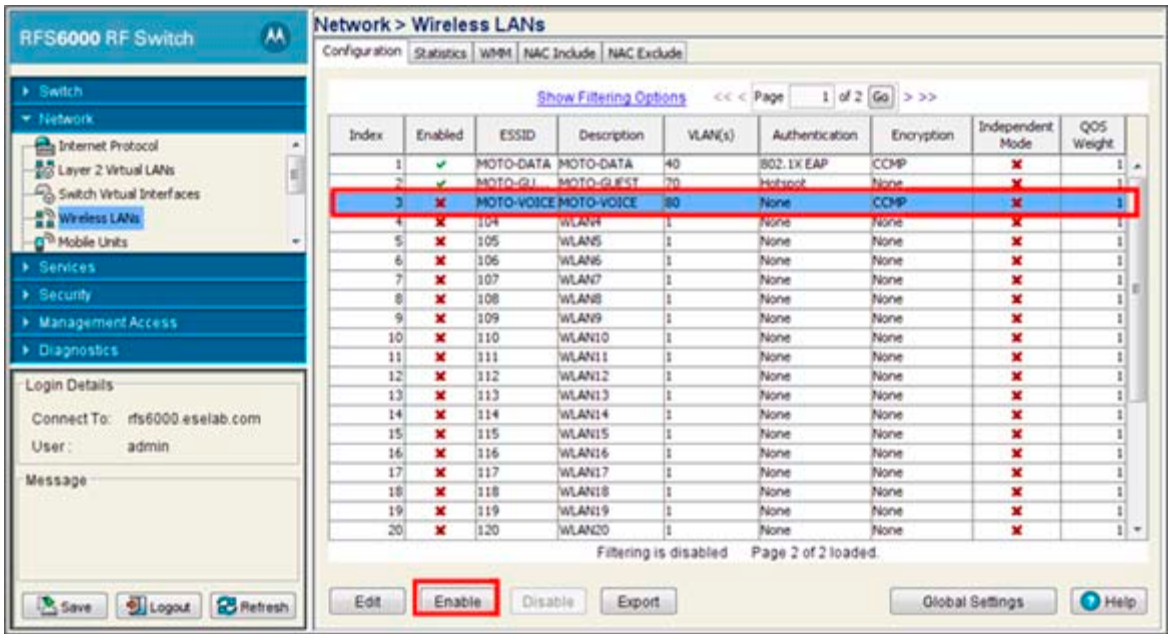


4. Enter an **ESSID** name and **Description.**
5. Specify one or more **VLAN IDs**.
6. In the **Encryption** field enable **WPA2-CCMP** and click the **Config** button.



7. Optionally enable the **Broadcast Key Rotation** option.

8. In the **ASCII Passphrase** field, enter the strong passphrase used for device authentication. Select **OK** to save the updates.



9. From back at the **Network** > **Wireless LANs** > **Configuration** screen, highlight (select) the newly created WLAN and select **Enable**.

   If global WLAN manual mapping is enabled, manually assign the new WLAN to each radio you wish to support. If this global option is disabled, the RF Switch automatically assigns the WLAN to each adopted radio.

10. Select **Save** (from the lower left-hand corner) to apply the changes.

D.9.4 RF Switch Running Configuration

The following shows the running configuration of the RFS6000 switch used to create this tutorial:

```
RFS6000# show running-config
!
! configuration of RFS6000 version 3.3.0.0-029R
!
version 1.2
!
!
aaa authentication login default local none
service prompt crash-info
!
username "admin" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
username "admin" privilege  superuser
username "operator" password 1 b6b6ccabdb85763872c7fbdf436ec2ed86bf931e
!
```

```
!
!
spanning-tree mst configuration
 name My Name
!
crypto pki trustpoint ESELAB
 subject-name "rfs6000" US "TN" "Johnson City" "Motorola Inc." "WLAN
Enterprise Division"
 fqdn "rfs6000.eselab.com"
 ip-address 192.168.10.14
!
management secure
ip domain-name eselab.com
ip name-server 192.168.10.5
no bridge multiple-spanning-tree enable bridge-forward
country-code us
logging buffered 7
logging console 4
logging host 192.168.10.5
snmp-server engineid netsnmp 6b8b456748daa1a5
snmp-server location  Johnson City TN
snmp-server contact kevin.marshall@motorola.com
snmp-server sysname RFS6000
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpmanager v3 encrypted auth md5
0xe3e4b0c4acafa27f6a23ad77d69ac182
snmp-server user snmpoperator v3 encrypted auth md5
0x4fc3ccf48e7c1c7780f936f8cb3fcc64
ip http server
ip http secure-trustpoint ESELAB
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
timezone America/New_York
service radius
license AP
fc781051ebf9d99ced010a4dab46a63a760c66f54b1c496da322d3cd41d046777fbed8
0f433b68ea
!
```

```
wireless
 secure-wispe-default-secret 0 defaultS
 adoption-pref-id 100
 no adopt-unconf-radio enable
 manual-wlan-mapping enable
 wlan 1 enable
 wlan 1 description MOTO-DATA
 wlan 1 ssid MOTO-DATA
 wlan 1 vlan 40
 wlan 1 encryption-type ccmp
 wlan 1 authentication-type eap
 wlan 1 radius server primary 192.168.10.5
 wlan 1 radius server primary radius-key 0 ESELAB
 wlan 1 radius reauth 3600
 wlan 1 dot11i preauthentication
 wlan 1 dot11i key-rotation enable
 wlan 2 enable
 wlan 2 description MOTO-GUEST
 wlan 2 ssid MOTO-GUEST
 wlan 2 vlan 70
 wlan 2 authentication-type hotspot
 wlan 2 mu-mu-disallow
 wlan 2 secure-beacon
 wlan 2 hotspot webpage-location advanced
 wlan 2 radius server primary 192.168.10.14
 wlan 2 radius server primary radius-key 0 ESELAB
 wlan 2 radius accounting server primary 192.168.10.14
 wlan 2 radius accounting server primary radius-key 0 ESELAB
 wlan 3 enable
 wlan 3 description MOTO-VOICE
 wlan 3 ssid MOTO-VOICE
 wlan 3 vlan 80
 wlan 3 encryption-type ccmp
 wlan 3 dot11i phrase 0 pre-shared-key
 wlan 3 dot11i key-rotation enable
 radio add 1 00-15-70-78-F5-23 11a ap300
 radio 1 description AP300-1-A
 radio 1 bss 1 1
 radio 1 channel-power indoor 36 15
 radio 1 on-channel-scan
```

```
radio 1 adoption-pref-id 100
radio add 2 00-15-70-78-F5-23 11bg ap300
radio 2 description AP300-1-BG
radio 2 bss 1 1
radio 2 bss 2 2
radio 2 bss 3 3
radio 2 channel-power indoor 1 18
radio 2 on-channel-scan
radio 2 short-preamble
radio 2 adoption-pref-id 100
radio add 3 00-15-70-B2-FD-CF 11a ap300
radio 3 description AP300-2-A
radio 3 bss 1 1
radio 3 channel-power indoor 40 15
radio 3 on-channel-scan
radio 3 adoption-pref-id 200
radio add 4 00-15-70-B2-FD-CF 11bg ap300
radio 4 description AP300-2-BG
radio 4 bss 1 1
radio 4 bss 2 2
radio 4 bss 3 3
radio 4 channel-power indoor 6 18
radio 4 on-channel-scan
radio 4 short-preamble
radio 4 adoption-pref-id 200
radio add 5 00-15-70-B2-FD-D0 11a ap300
radio 5 description AP300-3-A
radio 5 bss 1 1
radio 5 channel-power indoor 44 15
radio 5 on-channel-scan
radio 5 adoption-pref-id 100
radio add 6 00-15-70-B2-FD-D0 11bg ap300
radio 6 description AP300-3-BG
radio 6 bss 1 1
radio 6 bss 2 2
radio 6 bss 3 3
radio 6 channel-power indoor 11 18
radio 6 on-channel-scan
radio 6 short-preamble
radio 6 adoption-pref-id 100
```

```
 radio add 7 00-15-70-D5-DA-CE 11a ap300
 radio 7 description AP300-4-A
 radio 7 bss 1 1
 radio 7 channel-power indoor 48 17
 radio 7 on-channel-scan
 radio add 8 00-15-70-D5-DA-CE 11bg ap300
 radio 8 description AP300-4-BG
 radio 8 bss 1 1
 radio 8 bss 2 2
 radio 8 bss 3 3
 radio 8 channel-power indoor 1 4
 radio 8 on-channel-scan
 radio 8 short-preamble
 radio add 9 00-15-70-D5-DA-FB 11a ap300
 radio 9 description AP300-5-A
 radio 9 bss 1 1
 radio 9 channel-power indoor 149 20
 radio 9 on-channel-scan
 radio add 10 00-15-70-D5-DA-FB 11bg ap300
 radio 10 description AP300-5-BG
 radio 10 bss 1 1
 radio 10 bss 2 2
 radio 10 bss 3 3
 radio 10 channel-power indoor 6 4
 radio 10 on-channel-scan
 no ap-ip default-ap switch-ip
 ap-detection enable
!
 smart-rf
  radio 1 radio-mac 00-15-70-7E-27-6C
  radio 2 radio-mac 00-15-70-7E-3F-1C
  radio 3 radio-mac 00-15-70-CD-82-BC
  radio 4 radio-mac 00-15-70-CD-83-84
  radio 5 radio-mac 00-15-70-CD-83-6C
  radio 6 radio-mac 00-15-70-CD-83-24
  radio 7 radio-mac 00-15-70-D0-24-4C
  radio 8 radio-mac 00-15-70-D0-23-EC
  radio 9 radio-mac 00-15-70-D0-25-64
  radio 10 radio-mac 00-15-70-D0-26-54
 !
```

```
!
radius-server local
 authentication eap-auth-type all
 nas 192.168.10.0/24 key 0 ESELAB
!
radius-server local
!
!
interface ge1
 switchport access vlan 10
!
interface ge2
 switchport access vlan 10
!
interface ge3
 switchport access vlan 10
!
interface ge4
 switchport access vlan 10
!
interface ge5
 switchport access vlan 10
!
interface ge6
 switchport access vlan 10
!
interface ge7
 switchport access vlan 10
!
interface ge8
switchport access vlan 10
!
interface me1
 no ip address
!
interface up1
 description Uplink
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk native tagged
```

```
 switchport trunk allowed vlan none
 switchport trunk allowed vlan add 10,12,40,70,80,
!
interface vlan1
 no ip address
 shutdown
!
interface vlan10
 management
 description SERVICES
 ip address 192.168.10.14/24
!
interface vlan70
 description GUEST
 ip address 192.168.70.14/24
!
!
!
rtls
 rfid
 espi
 sole
!
ip route 0.0.0.0/0 192.168.10.1
!
ntp server 192.168.10.5 prefer
line con 0
line vty 0 24
!
end
```

MOTOROLA INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-124690-01 Revision A
May 2009