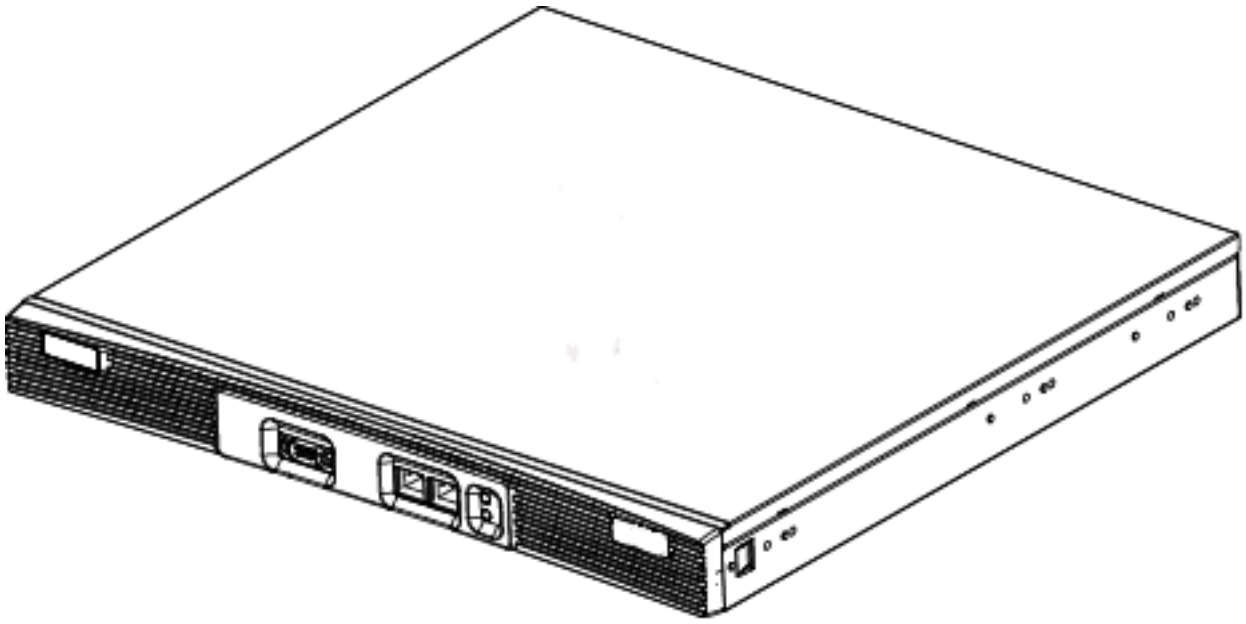
MOTOROLA

WS5100 Series Switch

System Reference Guide



Contents

Chapter 4. Network Setup

Chapter 5. Switch Services

Chapter 6. Switch Security

Chapter 7. Switch Management

Chapter 8. Diagnostics

About This Guide

Introduction

This guide provides information about using the WS5100 Series Switch.

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

Documentation Set

The documentation set for the WS5100 Series Switch is partitioned into the following guides to provide information for specific user needs.

- **WS5100 Installation Guide** - describes the basic setup and configuration required to transition to more advanced configuration of the switch.
- **WS5100 CLI Reference** - describes the *Command Line Interface* (CLI) and *Management Information Base* (MIB) commands used to configure the WS5100 Series Switch.
- **WS5100 Migration Guide** - provides upgrade instructions and new feature descriptions for legacy users of the WS5100 Series Switch.
- **WS5100 Troubleshooting Guide**- describes workarounds to known conditions the user may encounter.
- **RF Management Software Users Guide** - describes how to use Motorola RFMS to set up and monitor your WS5100 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.

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.

1

Overview

The switch provides a centralized management solution for wireless networking components across the wired network infrastructure. The switch connects to legacy access ports through a Layer 2 switch/hub. The switch connects to non-legacy access ports through a Layer 3 interface.

The switch functions as the center of the wireless network. The access ports function as radio antennas for data traffic management and routing. All of the system configuration and intelligence for the wireless network resides in the switch.

The switch uses access ports to bridge data from associated wireless devices to the wireless switch. The wireless switch applies appropriate policies to the data packets before routing them to their destination. Data packets destined for devices on the wired network are processed by the switch, where appropriate policies are applied before they are encapsulated and sent to their destination.

Access port configuration is managed by the switch through the *Graphical User Interface* (GUI), SNMP or the *Command Line Interface* (CLI). The switch streamlines the management of a large wireless system and allows for *Quality of Service* (QoS), virtual WLANs and packet forwarding implementations.

1.1 Hardware Overview

The wireless switch is a rack-mountable device that manages all inbound and outbound traffic on the wireless network. It provides 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. It collects management "intelligence" from individual access points and moves the collected information into the centralized switch. Then, it replaces access points with "dumb" radio antennas called access ports.

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. Depending on the model, an AP can support as many as 16 WLANs.

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 WS5100 Series Switch include:

Width	48.1 cm / 18.93 in. (with mounting brackets) 42.9 cm / 16.89 in. (without mounting brackets)
Height	4.39 cm / 1.73 in.
Depth	40.46 cm / 15.93 in.
Weight	6.25 kg / 13.75 lbs.
Max Power Consumption	100 VAC, 50/60 Hz, 3A 240 VAC, 50/60 Hz, 1.5A
Operating Temperature	10°C - 35°C / 50°F - 95°F
Operating Humidity	5% - 85% without condensation

1.1.1.1 Power Cord Specifications

A power cord is not supplied with the device. Use only a correctly rated power cord certified for the country of operation.

1.1.1.2 Power Protection

To best protect the switch from unexpected power surges or other power-related problems, ensure the system installation meets the following power protection 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.

1.1.1.3 Cabling Requirements

Two Category 6 Ethernet cables (not supplied) are required to connect the switch to the LAN and the WLAN. The cables are used with the two Ethernet ports on the front panel of the switch.

The console cable that comes with the switch is used to connect the switch to a computer running a serial terminal emulator program to access the switch's *Command Line Interface* (CLI) for initial configuration. Initial configuration steps are described in the *WS5100 Series Switch Installation Guide*.

1.1.2 System Status LED Codes

A WS5100 has two LEDs on the front panel (adjacent to the RJ45 ports). The System Status LEDs display three colors—blue, amber, or red —and three "lit" states—solid, blinking, or off.

1.1.2.1 Start Up

Event	*Top LED*	*Bottom LED*
Power off	Off	Off
Power On Self Test (POST) running	All colors in rotation	All colors in rotation
POST succeeded	Blue solid	Blue solid

1.1.2.2 Primary

Event	*Top LED*	*Bottom LED*
Active *(Continually Adopting Access Ports)*	Blue blinking	Blue solid
No License to Adopt	Amber blinking	Amber blinking

1.1.2.3 Standby

Event	*Top LED*	*Bottom LED*
Active *(Failed Over and Adopting Ports)*	Blue blinking	Blue blinking
Active *(Not Failed Over)*	Blue blinking	Amber solid

1.1.2.4 Error Codes

Event	*Top LED*	*Bottom LED*
POST failed (critical error)	Red blinking	Red blinking
Software initialization failed	Amber solid	Off
Country code not configured. ***Note:*** *During first time setup, the LEDs will remain in this state until the country code is configured.*	Amber solid	Amber blinking
No access ports have been adopted	Blue blinking	Amber blinking

1.1.3 10/100/1000 Port Status LED Codes

A WS5100 Series Switch has two LED indicators for its RJ-45 ports:

- Upper left (amber/green) for link rate
- Upper right (green) for link activity

The following table provides additional information about the status of the 10/100/1000 Port Status LEDs.

LED	*State*	*Meaning*
Upper left	Off	10 Mbps link rate
	Green steady	100 Mbps link rate
	Amber steady	1 Gigabit link rate
Upper right	Off	The port isn't linked
	Green steady	The port is linked
	Green blinking	The port is linked and active

1.2 Software Overview

The switch includes a robust set of features.This section provides an overview of the software and features. The features are listed and described in the following sections:

- *Infrastructure Features*
- *Wireless Switching*
- *Wired Switching*
- *Management Features*
- *Security Features*
- *Access Port Support*

NOTE: The *Motorola RF Management Software* is also 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

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

The switch platform has sufficient non-volatile memory to store multiple firmware images. The switch stores an active and a passive firmware image. The switch supports staged upgrade operations.

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 48.
- You can install/remove AP licenses in batches of 6 APs at a time.
- The Radius server and VPN capability is not a part of the licenses feature.

1.2.1.3 Configuration Management

The system supports redundant storage of configuration files to protect against corruption during a write operation and ensures at any given time a valid configuration file exists. If a configuration file has failed to completely execute, it is rolled back and the pre-write file is used.

Text Based Configuration

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

1.2.1.4 Diagnostics

The following diagnostics are available for the switch:

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. The in-service-diagnostics continuously monitor any available physical characteristics (as detailed below) and issues log messages when either 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 unit is in operation. The 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 (for example, check the time critical processes were started), 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 allows service personnel to capture incoming and outgoing packets in a buffer.

The switch also maintains various statistics for RF activity, Ethernet ports 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 Process Monitor constantly checks to ensure processes under its control are up and running. Each monitored process sends the Process Monitor 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 functionality, up to 12 switches can be configured in a redundancy group (and thereby provide group monitoring). In the event of a switch failure, a switch within the cluster takes control. Therefore, the switch supported network is always up and running even if a switch fails or is removed for maintenance or software upgrade. Switch redundancy provides minimal traffic disruption in the event of a switch failure or intermediate network failure.

The following redundancy features are supported:

- Up to 12 switch redundancy members supported per 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. Each redundancy group can support two or more primary members, each responsible for group load sharing.
- Members within the same redundancy group can be deployed across different subnets and maintain their interdependence as redundancy group members.
- Each member of the redundancy group supports AP load balancing by default.
- Members of the redundancy group support license aggregation. 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) 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 group support, see *Configuring Switch Redundancy on page 5-25*.

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 environment. 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 additionally hold 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 5-16*.

1.2.1.11 Password Recovery

The switch has a provision enabling the switch to restore its factory default configuration if your password is lost. In doing so however the current configuration is erased and can be restored assuming if has been exported to a secure location. For information on password recovery, see *Switch Password Recovery on page 2-3*.

1.2.2 Wireless Switching

The switch includes the following wireless switching features:

- *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*

1.2.2.1 Physical Layer Features

802.11a

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

  The purpose of DFS is:

  - Detect interference from other systems and avoid co-channeling with those systems, most notably radar systems.
  - Provide uniform loading of the spectrum 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. The TPC functionality is enabled automatically for every AP that operates on the channel.

802.11bg

- Dual mode b/g protection – The 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. Of these rates, 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.

1.2.2.2 Rate Limiting

Rate limiting controls the maximum rate sent or received on a network. Rate limiting enables the proper allocation of bandwidth, based on the source MAC address, destination MAC address, source IP address,

destination IP address and/or TCP/UDP port number. Rate limiting allows the definition of two rates: a guaranteed minimum bandwidth and a second burst size. Rate limiting is performed as part of the flow control process (WISP protocol) between access ports and the switch.

1.2.2.3 Proxy-ARP

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 switch). Thus, the MU is not woken to send ARP replies (increasing battery life and conserving wireless bandwidth).

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

1.2.2.4 HotSpot / IP Redirect

A hotspot is a Web page that 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 / IP Redirect feature allows the switch to function as a single on-site switch supporting WLAN hotspots. The Hotspot feature re-directs user traffic (for a hotspot enabled WLAN) to a Web page that requires them to authenticate before granting access to the WLAN. The IP-Redirection requires no special software on the client but its does require the client be set to receive its IP configuration through DHCP. The following is a typical sequence of events for hotspot access:

1. A visitor with a laptop requires hotspot access at a site.
2. A user ID/ Password and the hotspot ESSID are 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. The DHCP service can be provided by an external DHCP server or provided by the internal DHCP server located on the switch.
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, connection time remaining and an I Agree button.
10. The user accepts by clicking the I Agree button and is granted access to the Internet. (or other network services).

To redirect user traffic from a default home page to a login page, the switch uses destination network address translation (destination NAT is similar to the source NAT/ PAT but the destination IP address and port get modified instead of the source as in traditional NAT). More 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. Therefore, acting like a proxy between the user and the Web site they are trying to access.

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 for it would be impractical to authenticate visitors using 802.1x authentications. Motorola also recommends reviewing the *WS5100 Migration Guide* (available

on the Motorola Web site) for a use case on hotspot deployment. For information on configuring a hotspot, see *Configuring Hotspots on page 4-29*.

1.2.2.5 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 SSID configured differently in their Radius server.
- User 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 in Radius Server.

1.2.2.6 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 4-53*

1.2.2.7 Self Healing

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

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

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

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, the AP scans all channels at a configurable rate and forwards received beacons the switch. The switch uses the received 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 and their signal strength. This enables you to verify your installation and configure it for self-healing when an AP fails.

Self Healing Actions

This mechanism allows you to assign a self healing action to an AP's neighbors, on a per-AP basis. If AP1 detects AP2 and AP3 as its neighbors, you can assign failure actions to AP2 and AP3 whenever AP1 fails.

You can assign four self healing actions:

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

You can also 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 5-46*.

1.2.2.8 Wireless Capacity

Wireless capacity specifies the maximum numbers of MUs, access ports and wireless networks usable by a given 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:

- Maximum number of WLANs per switch
- Maximum number of access ports per switch
- Maximum number of MUs per switch
- Maximum number of MUs per access port.

Up to 48 access ports are supported by the switch. The actual number of access ports adoptable by a switch is defined on a per platform basis and will typically be lower than 48.

1.2.2.9 AP and MU Load Balancing

Fine tune a network to evenly distribute the data and/or processing across available resources. The following 2 topics explain load balancing:

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

MU Balancing Across Multiple APs

As 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 the roaming decision. 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: Kbps, 2 byte : Kbps and 2 byte : MU Count are sent in beacon to MU.

NOTE: Each switch can support a maximum of 4096 MUs.

AP Balancing Across Multiple Switches

At adoption time, 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: Each switch can support a maximum of 48 access ports. However, port adoption per switch is determined by the number of licenses acquired.

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.

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 4-88*.

1.2.2.10 Wireless Roaming

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

- *L3 Roaming*
- *Fast Roaming*
- *Interswitch Layer 2 Roaming*
- *International Roaming*
- *MU Move Command*
- *Virtual AP*

L3 Roaming

L3 roaming works with switches in the mobility domain to exchange mobility related control information. This includes IP addresses, *Media Access Control* (MAC) address information and the HS-VLAN-id of all MUs in the mobility-domain. A consistent peer configuration results in full-mesh sessions required for L3 roaming to work correctly. Peering sessions use *Transmission Control Protocol* (TCP) as the transport layer protocol to carry mobility update messages. TCP provides the following advantages:

- TCP retransmits lost messages thereby providing reliable connectivity
- TCP ensures ordered message delivery using sequenced numbers.
- TCP has a built-in "keep-alive" mechanism which helps detect loss of connectivity to the peer or peer failure.

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 4-88*.

Fast Roaming

MUs roam from AP to AP as an MU moves throughout a WLAN coverage area. To improve roaming performance, various fast roaming features are implemented:

- *Pairwise Master Key (*PMK) — Caching credentials are in the AP, so the MU does not need to re-authenticate.
- PMK Opportunistic Caching — The MU starts transmitting on another AP in order for both AP's to connect to a common wireless switch.
- Switch to Switch Hand-Off — When an MU roams from a wireless switch in one subnet to a wireless switch in another subnet, the transport layer connections will be preserved as far as possible.
- PMK Pre-Authentication —The MU authenticates itself with the AP before roaming to it.

Interswitch Layer 2 Roaming

An associated MU (connected to a particular wireless switch) can roam to another access port connected to a different wireless switch. Both switches must be on the same L2 domain. Authentication information is not shared between the switches, nor is buffered packets on one switch transferred to the other switch. Pre-authentication between the switch and MU allows faster roaming.

International Roaming

The wireless switch supports international roaming as 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. This command permits an MU to roam between ports connected to the same wireless 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.

Virtual AP

The switch supports multiple *Basic Service Set Identifiers* (BSSIDs). An access port capable of supporting multiple BSSID's generates multiple beacons, one per BSSID. Hence, an AP that supports 4 BSSID's can send 4 beacons. The basic requirement for supporting multiple BSSID's is multiple MAC addresses, since each BSSID is defined by its MAC address.

When multiple BSSID's are enabled, you cannot tell by snooping the air whether any pair of beacons is sent out by the same physical AP or different physical AP. Hence the term "virtual AP's"- each virtual AP behaves exactly like a single-BSSID AP.

Each BSSID supports 1 *Extended Service Set Identifier* (ESSID). Sixteen ESSIDs per switch are supported.

1.2.2.11 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.

1.2.2.12 QoS

QoS provides the user a data traffic prioritization scheme. A QoS configuration scheme is useful in the case of congestion from excessive traffic or different data rates and link speeds.

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 total bandwidth is shared by different users and applications.

The objective of QoS is to ensure each WLAN configured 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 types:

802.11e QoS

802.11e enables real-time audio and video streams to be assigned a higher priority over regular data. 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. 802.1p uses the *Generic Attributes Registration Protocol* (GARP) and the *GARP VLAN Registration Protocol* (GVRP). GARP allows MUs to request membership within a multicast domain, and GVRP lets them register to a VLAN.

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, the VoIP conversation (a real-time session), receives priority, maintaining a high level of voice quality. The voice QoS used by the switch ensures:

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

Data QoS

The switch supports the following for data QoS techniques:

- Egress Prioritization by WLAN
- Egress Prioritization by ACL

DCSCP to AC Mapping

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

1.2.2.13 Wireless Layer 2 Switching

The switch supports the following layer 2 wireless switching techniques:

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

1.2.2.14 Automatic Channel Selection

Automatic channel selection works 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.

1.2.2.15 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, then 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, where a trigger frame is defined as a data frame (e.g. an uplink voice frame) associated with an uplink

flow having 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

1.2.3 Wired Switching

The switch includes the following wired switching features:

- *DHCP Servers*
- *DDNS*
- *GRE Tunneling*
- *VLAN Enhancements*
- *Interface Management*
- *Multiple WLAN Support*

1.2.3.1 DHCP Servers

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses, and discover information about the network to which they are attached. Configure address pools for each subnet, and whenever a DHCP client in that subnet requests an IP address, the DHCP server assigns an IP address from the address pool configured for that subnet.

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 DDNS

Dynamic DNS (DDNS) is a method of keeping 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.

1.2.3.3 GRE Tunneling

GRE tunnelling extends a WLAN across a Layer 3 network using standards based GRE tunneling technology.

- GRE tunnels need to be explicitly provisioned on the switch as well as the tunnel termination device present at the other end of the Layer 3 network.
- One or more WLANS on the switch are then mapped to the GRE tunnel interface. The configuration is very similar to mapping WLANs to VLANs.
- All IP packets received from MUs on the WLAN are encapsulated in GRE and sent across the Layer 3 network. The tunnel termination device at the other end decapsulates the GRE header and routes the inner IP packet to its original destination.

- When packets are received on the GRE tunnel interface by the switch, the switch decapsulates the GRE header and forwards the IP packet to the MU based on the destination IP address. The MAC address of the MU is obtained from the MU table.

1.2.3.4 VLAN Enhancements

The switch has incorporated the following VLAN enhancements:

- Physical port (L2) is now operated in Trunk Mode or Access Mode.
- A VLAN now allows an AP to receive and send only untagged packets. All tagged packets received by the AP are discarded. The untagged traffic received is internally placed in an “access vlan”.
- A trunk port can now receive, both tagged and untagged packets. Only one native VLAN per trunk port is supported. All untagged traffic received on is placed into 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 permits a physical interface to Auto Negotiate, Full Duplex or Half Duplex. The switch also allows:

- Manual bandwidth configuration of a physical interface to 10/100/1000Mbps. This is only permitted if duplex is not set to Auto-Negotiate.
- Manual configuration of administrative shutdown of a physical interface.

1.2.3.6 Multiple WLAN Support

A WS5100 switch supports 32 WLANS.

1.2.4 Management Features

The switch includes the following management features:

- Secure browser-based management console
- *Command Line Interface* (CLI) accessible via the serial port or through a *Secure Shell* (SSH) application
- CLI Service mode enables the capture of system status information that can be sent to Motorola personnel for use in problem resolution
- Support for *Simple Network Management Protocol* (SNMP) version 3 as well as SNMP version 2
- TFTP upload and download of access port firmware and configuration files
- Graphing of wireless statistics
- Dashboard summary of system state in the Web UI
- Multi switch management via MSP application
- Heat Map support for RF deployment
- Secure Guest Access
- Switch Discovery enabling users to discover each Motorola switch on the specified network.

1.2.5 Security Features

The 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 Allow*
- *MU to MU Disallow*
- *Switch-to-Wired*
- *802.1x Authentication*
- *IEEE 802.1AB LLDP*
- *WIPS*
- *Rogue AP Detection*

The switch includes the following wired security features:

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

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 4-40* or *Configuring WEP 128 / KeyGuard on page 4-41*.

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 4-43*.

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 4-43*.

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 MIC. KeyGuard is proprietary to Motorola MUs only. For information on configuring KeyGuard for a WLAN, see *Configuring WEP 128 / KeyGuard on page 4-41*.

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 4-22* to WLAN MU authentication.

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 Kerboros on page 4-27*.

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 purpose. For information on configuring 802.1x EAP for a WLAN, see *Configuring 802.1x EAP on page 4-26*.

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 allowed to be completed before the Radius lookup begins. For information on configuring 802.1x EAP for a WLAN, see *Configuring Dynamic MAC ACL on page 4-36*.

1.2.5.3 Secure Beacon

All the 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 Allow

MU to MU allow enables frames from one MU (where the destination MAC is that of another MU) to be switched to the second MU.

1.2.5.5 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.

1.2.5.6 Switch-to-Wired

The MU frames are switched out to the wired network (out of the switch). Another upstream device decides whether the frame should be sent back to the second MU, and if so it sends the frame back to the switch, and it is switched out just like any other frame on the wire. This allows a drop/allow decision to be made by a device other than the wireless switch.

1.2.5.7 802.1x 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.

- The default username is ***admin***
- The default password is ***symbol***

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*, 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
- At 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.

1.2.5.8 IEEE 802.1AB LLDP

The access port implements a *Link Layer Discovery Protocol* (LLDP) agent and operates in Transmit- mode only (it only transmits the information about the capabilities and the current status of the local system).

The following modes are not supported:

- Receive-only mode — The LLDP agent can only receive information about the capabilities and the current status of the remote systems
- Transmit and receive mode — The LLDP agent can transmit the local system capabilities and status information as well as receive remote system's capabilities and status information.

The LLDP agent uses a high frequency (sending LLDP advertisements every 1 second) only until the AP receives Hello Response i.e. after the AP sees Hello Response, no LLDPDUs are transmitted by the access port. After AP has been adopted, the LLDP advertisements are sent at lower frequency (sending LLDP advertisements every 30 seconds).

On reset (all resets including power-up), an access port sends a LLDP advertisement every time it sends the "Hello" message. This is in addition to 802.1x EAPOL messages.

NOTE: LLDPDUs are transmitted untagged.

LLDP is always enabled and cannot be disabled.

1.2.5.9 WIPS

The Motorola *Wireless Intrusion Protection System* (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 (with WISPe support) to an Intrusion Detection Sensor, the conversion requires approximately 60 seconds.

1.2.5.10 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*

NOTE: The *Motorola RF Management Software* is a recommended utility 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 WISP 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 will be a non-disruptive and none of the MU will be 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. You can configure how frequently this needs to be performed.

RF scan by Access Port on all channels

This process uses Auto Channel Select (called Detector AP assist) to scan for Rogue APs on all available channels. It functions as follows:

- The switch sends a WISP 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

The process of detecting a Rogue AP is disruptive, as connected MUs loose association. MUs need to reconnect once the access port resets.

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

The switch allows you to 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 1-22*.

Rogue AP Report

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

1.2.5.11 ACLs

ACLs control access to the network through a set of rules. Each rule specifies an action taken when a packet matches the given 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

ACLs are identified by either a number or a name (the exception being MAC extended ACLs which take only name as their identifier). Numbers are predefined for IP Standard and Extended ACLs, whereas a name can be any valid alphanumeric string not exceeding 64 characters. With numbered ACLs, the rule parameters have to be specified on the same command line along with the ACL identifier. For named ACLs, rules are configured within a separate CLI context. For information on creating an ACL, see *Configuring ACLs on page 6-16*.

1.2.5.12 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 6-62*.

1.2.5.13 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 everything in 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)

1.2.5.14 NAT

NAT (Network Address Translation) is supported for non-IPSec packets which are 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 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 will be used when hosts on a private network are trying to access a host on a public network. Destination NAT IP address can be used for public hosts to talk to a host on the private network.

1.2.5.15 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 6-74*.

1.2.6 Access Port Support

Access ports work on any VLAN with connectivity to the wireless switch. The switch supports the following access ports:

- AP100 (supports 802.11b)
- AP300 (supports 802.11a/b/g)
- Access points converted to access ports, including:
    - AP-4131

2

Switch Web UI Access and Image Upgrades

The content of this chapter is segregated amongst the following:

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 User ID **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 2-3*.

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

If the switch Web UI password is lost, you cannot get passed 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 switch using a password recovery username and password:

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:

   ```
   WS5100 login: cli
   ```

2. Enter a password recovery username of **restore** and password recovery password of **restoreDefaultPassword**.

   ```
   User Access Verification


   Username: restore
   Password: restoreDefaultPasword


   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. For information on importing switch configuration files, see *Transferring a Config File on page 3-19*.

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.

Additionally, legacy users running either the 1.4.x or 2.x version switch firmware may want to upgrade to the new 3.x baseline to take complete advantage of the new diverse feature set available to them. This chapter describes the method to upgrade from either the 1.4.x or 2.x baseline to the new 3.x baseline.

CAUTION: Motorola recommends caution when upgrading your WS5100 switch image to the 3.x baseline (from the 1.4.x and 2.x baselines), as portions of your configuration will be lost and unrecoverable. Ensure that you have exported your switch configuration to a secure location before upgrading your switch. The upgrade.log file will contain a list of issues found in the conversion of the configuration file to the new format.

CAUTION: If using a 1.4.x or 2.x admin user password shorter than 8 characters (such as the default Motorola password), the password will be converted to the 3.x baseline admin password of "password" upon a successful update to the 3.x baseline. Ensure your existing 1.4.x or 2.x admin password is longer than 8 characters before updating, or leave as is and use "superuser" to login into an updated 3.x baseline.

CAUTION: After upgrading the switch baseline from 1.4.x or 2.x to the 3.x baseline, applet caching can produce unpredictable results and contents. After the upgrade, ensure your browser is restarted. Otherwise, the credibility of the upgrade can come into question.

CAUTION: The 3.x version WS5100 switch uses 3 unique (default) SNMPv3 user names and passwords for MD5 authentication and DES privacy. If upgrading your configuration from a 1.4.x or 2.x baseline, you will need to change your SNMPv3 usernames and passwords to ensure SNMPv3 interoperation.

The unique SNMPv3 usernames and passwords include:

- username = snmpoperator/password = operator
- username = snmpmanager/password = symboladmin
- username = snmptrap/password = symboladmin

2.3.1 Upgrading the Switch Image from 1.4.x or 2.x to Version 3.x

To upgrade a switch running either a 1.4.x or 2.x version to the latest 3.x version switch firmware:

1. Execute the PreUpgradeScript utility (or use the CLI) to ensure there is enough space on your system to perform the upgrade. The PreUpgradeScript utility should be in the same directory as the upgrade files.
2. Install the **Cfgupgrade1.x-setup** utility on a Windows desktop system by double clicking the Cfgupgrade 1.x-setup file.

   Follow the prompts displayed by the installer to install Cfgupgrade 1.x-setup.

   A **WS5100 Configuration Upgrade** icon gets created within the Program Files folder. The icon can be optionally created on your Windows desktop as well.

3. From the WS5100 running either 1.4.x or 2.x, create a configuration and save it on the switch.

   WS5100# save <file name> <.cfg>

   This is the configuration that will be upgraded to the new 3.x baseline.

NOTE: Motorola recommends saving a copy of the switch configurartion to a secure location before the upgrade. If an error occurs with the upgrade a viable configuration will be needed to restore on the switch.

4. Copy the configuration file <.cfg> from the legacy WS5100 to the Windows system where the conversion utility resides.

   Use ftp or tftp to transfer the file.

5. Click on the **WS5100 configuration Upgrade** icon (from the Windows system).

6. Select the config file copied on to the windows system and run it.

   A folder having the same name as the config file is created. The folder contains the converted startup-config file (in the new upgraded format) along with other log files.

7. Copy the startup-config file back to the WS5100 running using either tftp or ftp.

8. Download or copy the image file <`WS5100-3.0.2.0-XX.v1`> or <`WS5100-3.0.2.0-XX.v2`> to the WS5100 running the legacy switch firmware.

NOTE: If upgrading a 1.4.x version WS5100 to the new 3.x baseline, be sure you are using the <`WS5100-3.0.2.0-XX.v1`> image file. If upgrading a 2.x version WS5100 to the new 3.x baseline, be sure you are using the <`WS5100-3.0.2.0-XX.v2`> image file.

9. On the WS5100, type:

   ```
   WS5100#service
   WS5100#password "password"
   exec
   ```

   Upon reboot, the switch runs the 3.x image using startup-config as the running configuration.

10. Repeat the instructions above for additional switch upgrades, ensuring <`WS5100-3.0.2.0-XX.v1`> is used for 1.4.x version upgrades, and <`WS5100-3.0.2.0-XX.v2`> is used for 2.x version upgrades.

2.4 Auto Installation

The switch auto Install function works via the DHCP server. This 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 the static case (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, derive it from the file name. If it can not be derived from the filename, the system will attempt to load something other than what it is currently running.

Configuration files are tracked by their MD5 checksum. If a file is renamed, it will still have the same md5 sum. Once a file has been loaded it will not be reloaded, even if the local configuration information is changed.

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):

```
WS5100(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:

```
WS5100>en
WS5100#conf t
WS5100(config)#autoinstall image
WS5100(config)#autoinstall config
WS5100(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 set 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.

```
WS5100(config)#autoinstall config url ftp://ftp:ftp@192.9.200.1/ws5100/
config
WS5100(config)#autoinstall cluster-config url ftp://ftp:ftp@192.9.200.1/
ws5100/cluster-config
WS5100(config)#autoinstall image url ftp://ftp:ftp@147.11.1.11/ws5100/
images/WS5100.img
WS5100(config)#autoinstall image version 3.0.2.0-XXXXX
WS5100(config)#autoinstall config
WS5100(config)#autoinstall cluster-config
WS5100(config)#autoinstall image
WS5100(config)#show autoinstall
feature    enabled      URL
config       yes        ftp://ftp:ftp@192.9.200.1/ws5100/config
cluster cfg  yes        ftp://ftp:ftp@192.9.200.1/ws5100/cluster-config
image        yes        ftp://ftp:ftp@147.11.1.11/ws5100/images/WS5100.img
expected image version  3.0.2.0-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 Downgrading the Switch Image

If for some reason you want to downgrade your WS5100 back down to a 1.4.x or 2.x version firmware image, use one of the two following image files:

- WS5100-1.4.3.0-012R.img
- WS5100-2.1.0.0-029R.img

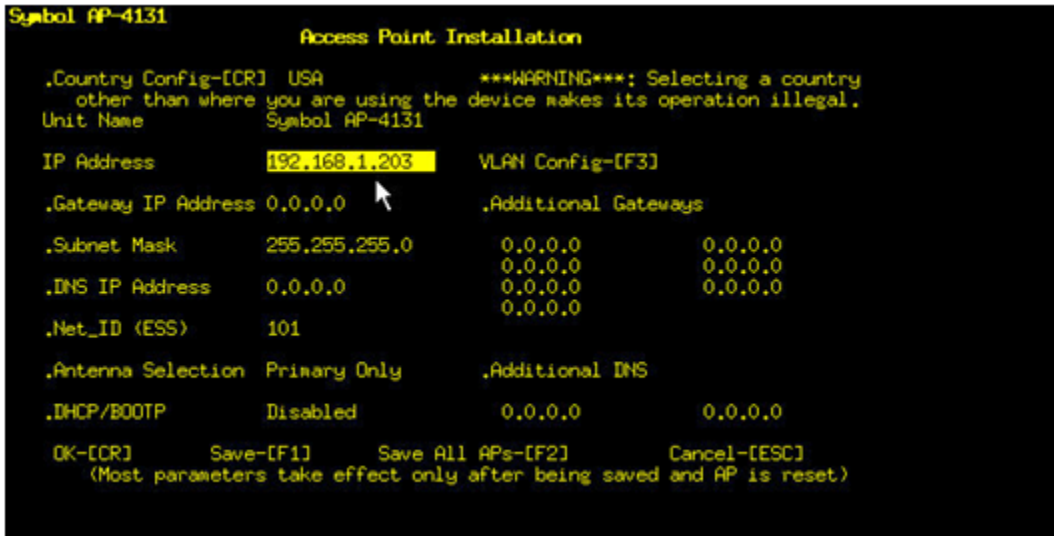
2.6 AP-4131 Access Point to Access Port Conversion

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.

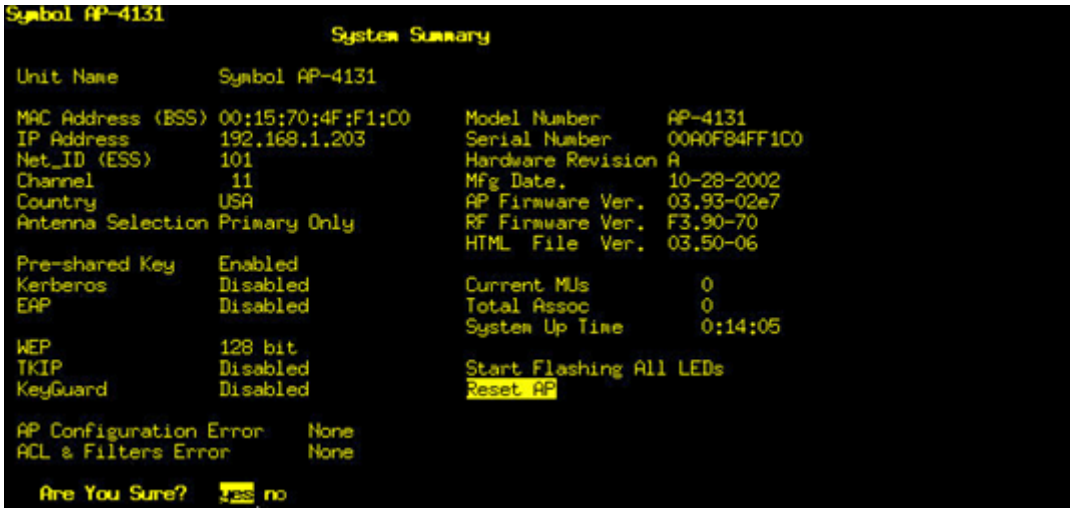
To convert an AP-4131 access point

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**.

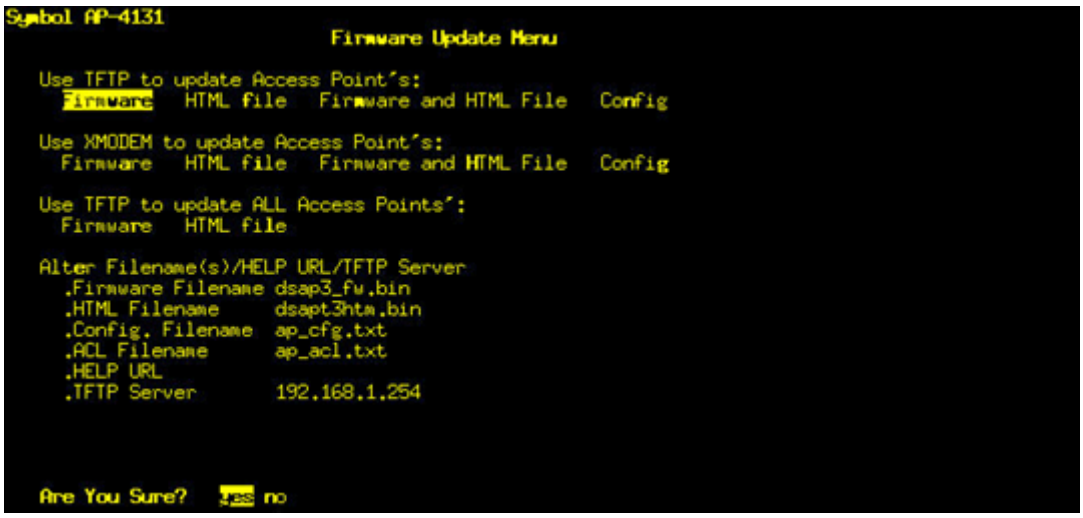
3. Select the **AP Installation** main menu item.
4. From the **IP Address** field, enter a new IP address (if required) and select **Save-[F1]** to save the change. If the IP address was changed, you will need to reset the AP for the change to be implemented.



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 WS5100. 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:

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 Web UI.

3.1 Viewing the Switch Interface

The **Switch** screen provides high-level system, switch name and address information accessible from one location. The values within the screen can be defined in numerous locations throughout the applet.

NOTE: The *Motorola RF Management Software* is also 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 in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Motorola Web site.

It consists of the following two tabs:

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).

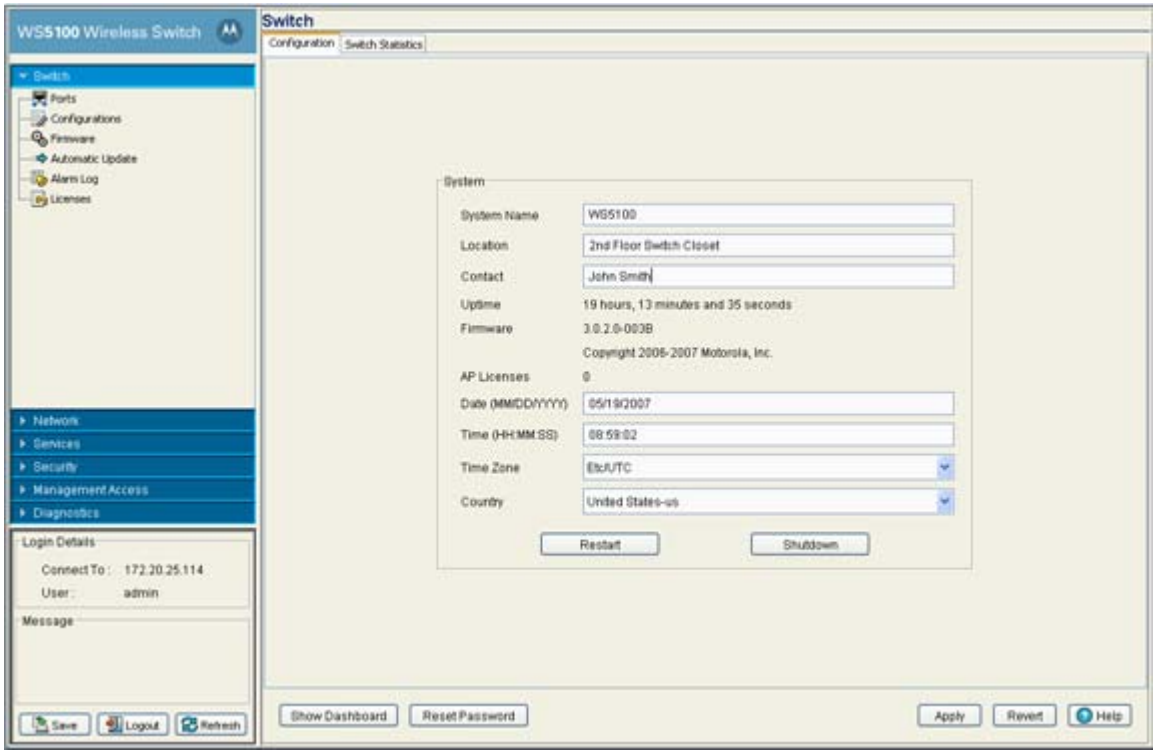
3.1.1 Viewing the Switch Configuration

The system prompts you to enter the correct country code after the first login. A warning message may display stating that an incorrect country setting will lead to the illegal use of the switch. Hence, 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** field correctly.

The **Configuration** screen displays high-level system settings for system name, location and contact information.

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

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



3. The system prompts the user for the correct **Country** code after the first login.

   A warning message could display stating that an incorrect country setting will lead to an illegal use of the switch. 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 field correctly.

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

System Name	Displays the designated read-only system name. Select a system name serving as a reminder of the user base the switch supports (engineering, retail, etc.).
Location	The **Location** is used to define the location of the switch. The Location parameter acts as a reminder of where the switch can be found. Use the System Name field as a specific identifier of the switch's location. Use the System Name and Location fields together to optionally define the switch name by the radio coverage type it supports and specific physical location. For example, "second floor engineering."
Contact	Displays the **Contact** value for contact information for system administration and troubleshooting.
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.
AP Licenses	Displays the number of access port licenses currently available for the switch. In other words, the maximum number of access ports the switch is licensed to adopt.
Date (MM/DD/YYYY)	Displays the day, month and year currently used with the switch.
Time	Displays the time of day used by the switch.
Time Zone	Use the Time Zone drop-down menu to specify the time zone used to with the switch. Adjusting the time zone will in turn, cause an adjustment to the time displayed in the Time field.
Country	Use the drop-down menu to specify the correct country of operation. Selecting the country incorrectly could render your switch as operating illegally.

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.

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

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

6. Click the **Shutdown** button to halt (stop) the switch.
7. Click the **Show Dashboard** button to display a screen with indicators of switch health and status. For more information, see *Viewing Dashboard Details on page 3-4*.

8. Click the **Reset Password** button to display a screen to reset you password to a new value.

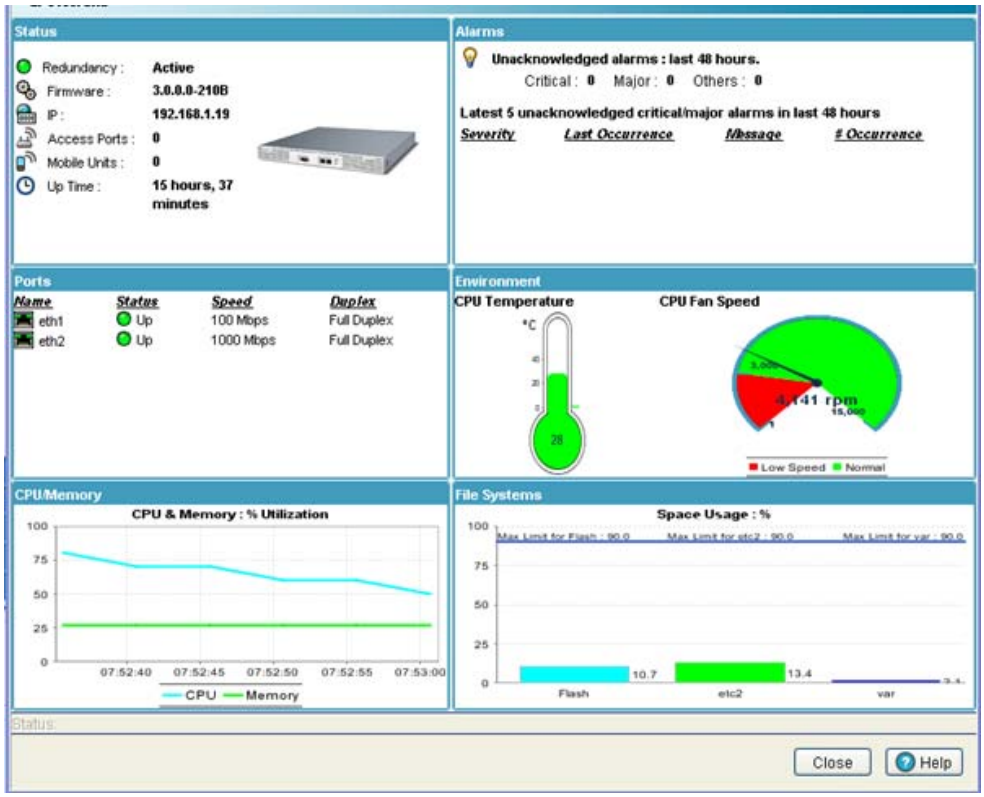
Enter the new password within the **Password** and **Confirm Password** fields and click **OK**.

9. Click the **Apply** button to save the updates (to Time Zone or Country).
10. Click the **Revert** button to undo any changes.

3.1.1.1 Viewing Dashboard Details

The switch dashboard represents a high-level (graphical) overview of central switch processes. When initially logging into the switch, it 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.



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

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

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

Displays the status of the switch. The status can be either Active or Inactive.

- Active — Is denoted with a green dot.
- Standby— Is denoted with a red dot.

Displays the current Firmware value of the current software running on the wireless switch.

Displays the Management IP Address of the switch.

Displays the status of the Ethernet Port 1 and Ethernet Port 2. The status of the port can be either:

- Up — Port in use.
- Down — Port not in use.

Displays the total number of access ports adopted by the switch.

Displays the total number of MUs associated with the switch.

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 legend.
   - Major — Denoted by a yellow legend.
   - Others — Denoted by a blue legend.

   It also displays details of the 5 most recent unacknowledged critical/major alarms raised during the past 48 hours in a tabular format. 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, duplex, POE Status of each physical port on the front panel. It displays the following details in a tabular format:

Name	Displays the name of the port, either—Ethernet1 or Ethernet 2
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.

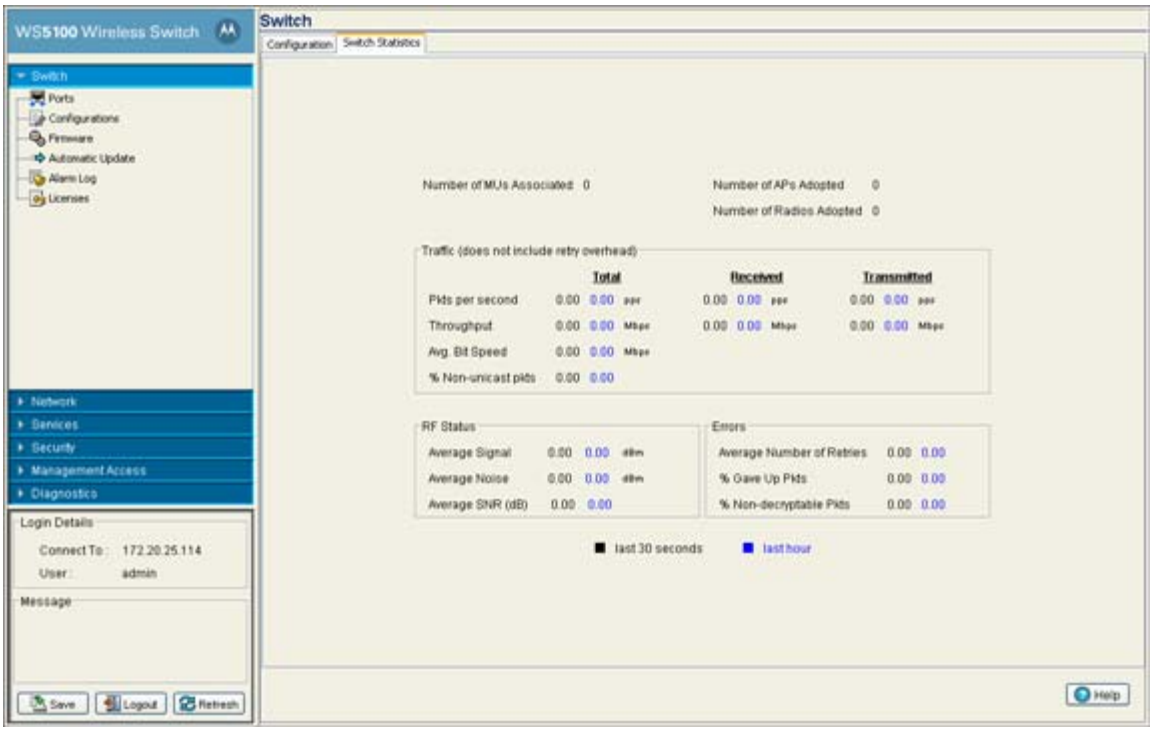
3. The **Environment** section displays the CPU temperature and switch fan speed. It displays the valid threshold range set by the user.
4. The **CPU/Memory** section displays the free memory available with the RAM.
5. The **File Systems** section displays the free file system available with:
6. Root file system usage (/flash)
    a. RAM file system usage (/var)
    b. etc2 file system usage (/etc2)

3.1.2 Viewing Switch Statistics

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

To display the main 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 **Switch Statistics** area for 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** section for read-only network traffic information 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. The throughput value can help identify network bandwidth and utilization issues negatively impacting performance.
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.

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

Avg Signal	Displays the average signal strength for MUs associated with the switch over the last 30 seconds and 1 hour. The higher the signal, the closer the MU.
Avg 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.
Avg SNR	Displays the average *Signal to Noise Ratio* (SNR) for all MUs associated with the switch. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

6. Refer to the **Errors** section for the following 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.
% 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.
% 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.

3.2 Viewing Switch Port Information

The **Port** screen displays the configuration, runtime status and statistics of the Ethernet Port 1 and Ethernet port 2. It consists of the following tabs:

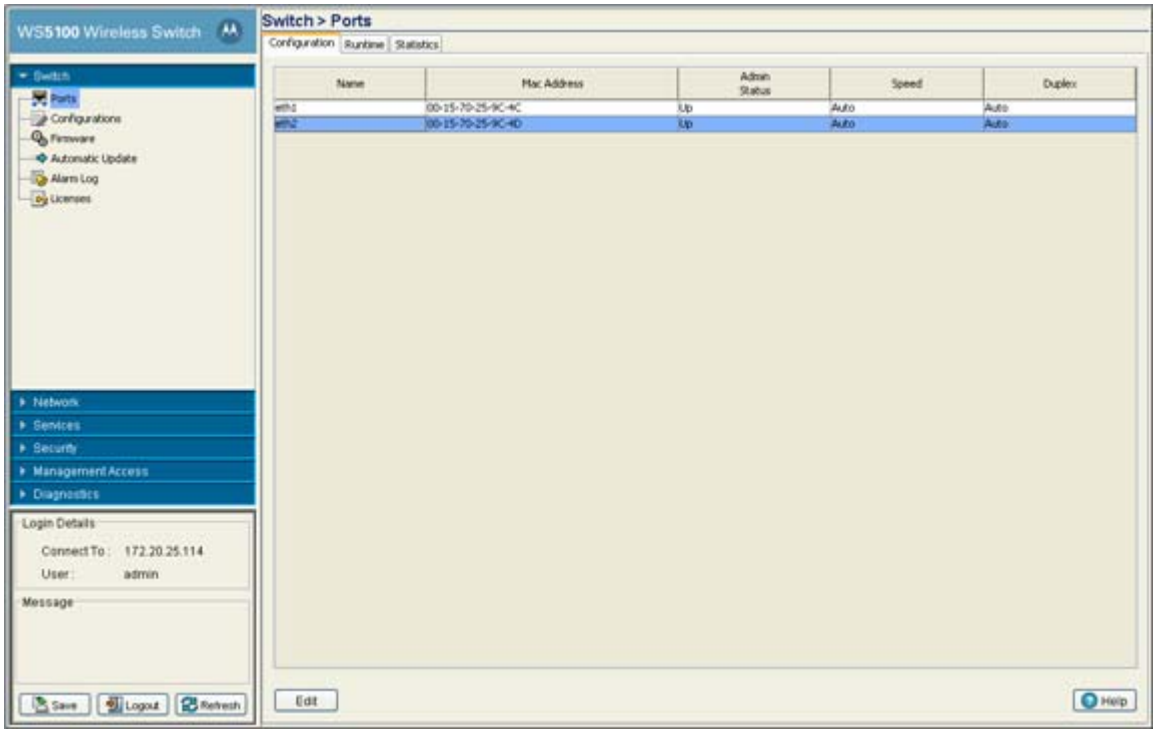
- Configuration
- Runtime
- Statistics

3.2.1 Viewing the Port Configuration

The **Configuration** screen displays the current configuration for the switch ports. This screen has a Filter option, which can be either displayed or hidden. Use this information to determine whether an existing port configuration can be used as is or requires modification to be valid 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. By default, eth1 and eth2 are available.
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.

3. Select a port and click the **Edit** button to modify the port configuration. For additional information, see *Editing the Port Configuration on page 3-9*.

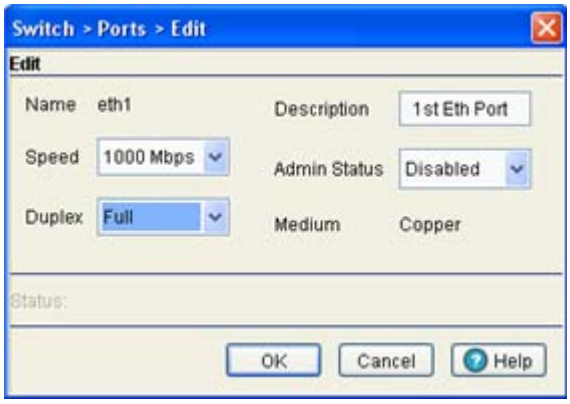
3.2.1.1 Editing the Port Configuration

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 the modification 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 this pop-up.
4. Use the **Edit** screen to modify the following port configurations for the selected port.



Name	If necessary, modify the read-only name assigned to the port.
Speed	Select the speed at which the port can receive and transmit the data. You can select from either of the following ranges: • 10 Mbps • 100 Mbps • 1000 Mbps • Auto
Duplex	Modify the duplex status of the switch by selecting one of the following options: • Half • Full • Auto
Description	Enter a brief description for the port.
Admin Status	Either Enable (activate) or Disable (inactivate) the admin status of the port.

Read-only details about the port's cabling connection also display within the Edit screen. This information should be used to help assess what configuration should be set for this port.

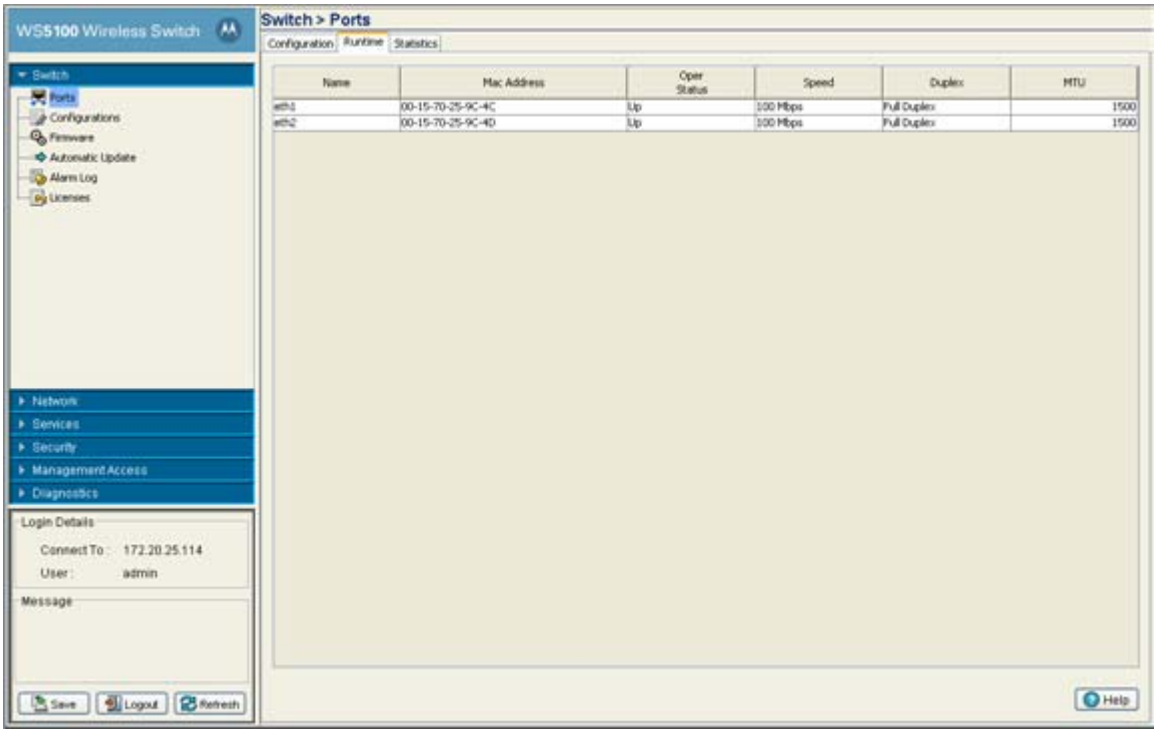
5. Click the **OK** button to commit the changes made to the port configurations.
6. Click **Cancel** to disregard any changes and revert back to the last saved configuration.

3.2.2 Viewing the Ports Runtime Status

The Configuration screen displays the read-only runtime configuration for uplink and downlink ports. This screen has a Filter option (which can be either displayed or hidden).

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 ports 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 operational 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 or full duplex.
MTU	Displays the MTU setting configured on the port. MTU stands for maximum transmission unit. The MTU value represents the largest packet size that can be sent over a link. The MTU is determined by the underlying network, but must be taken into account at the IP level. IP packets (which can be up to 64K bytes each) must be packaged into lower-level packets of the appropriate size for the underlying network(s) and re-assembled on the other end. 10/100 Ethernet ports have a maximum MTU setting of 1500.

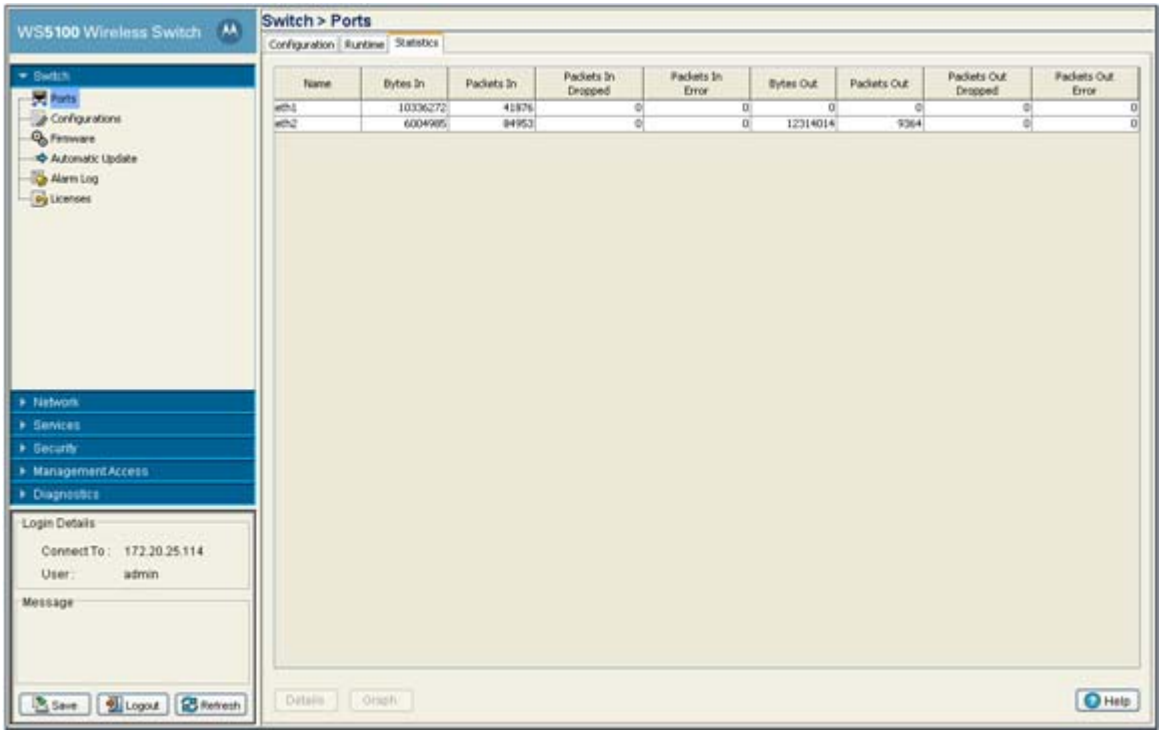
3.2.3 Viewing the Ports Statistics

The **Statistics** screen displays read-only statistics for uplink and downlink ports. Use this information to assess if configuration changes are required to improve network performance. This screen has a Filter option, which can be either displayed or hidden.

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

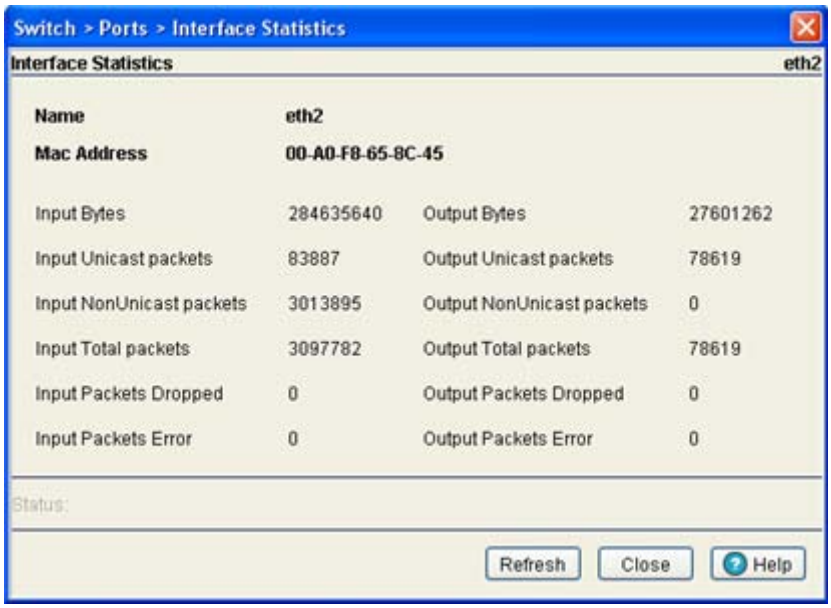
Name	Defines the port name (as either uplink or downlink).
Bytes In	Displays the total number of bytes received by the port.
Packets In	Displays the total number of packets received by the port.
Packets In Dropped	Displays the number of packets dropped by the port. If the number appears excessive, a different port could be required.
Packets In Error	Displays the number of erroneous packets received by the port. If the number appears excessive, a different port could be required.
Bytes Out	Displays the total number of bytes transmitted by the port.
Packets Out	Displays the total number of packets transmitted (sent) by the port. A low value could be an indication of a network problem.
Packets Out Dropped	Displays the total number of transmitted packets dropped. A high value may be an indication of network 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 on page 3-13*.
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 on page 3-14*.

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 the 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 in the interface.
Input Unicast Packets	Displays the number of unicast packets (packets directed towards the interface) received in 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 received 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 received 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 the 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 at the interface. Output Packet Errors are the sum of all the output packet errors, malformed packets and misaligned packets received on an interface.

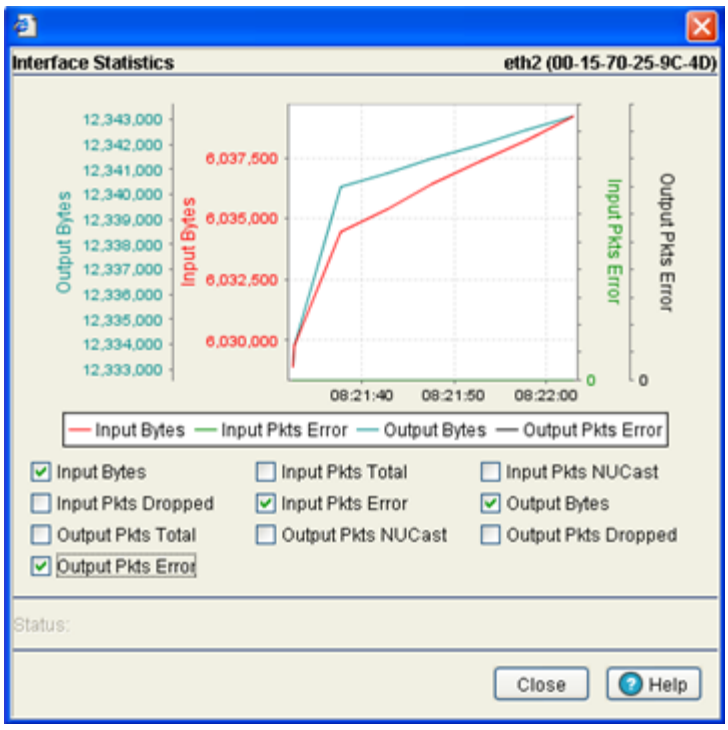
4. The **Status** is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click on the **Refresh** button to refresh the port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

3.2.3.2 Viewing the Port Statistics Graph

The Web UI 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 statistics for 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. Select any of the above parameters by selecting the checkbox associated with it.

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

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

3.3 Viewing Switch Configurations

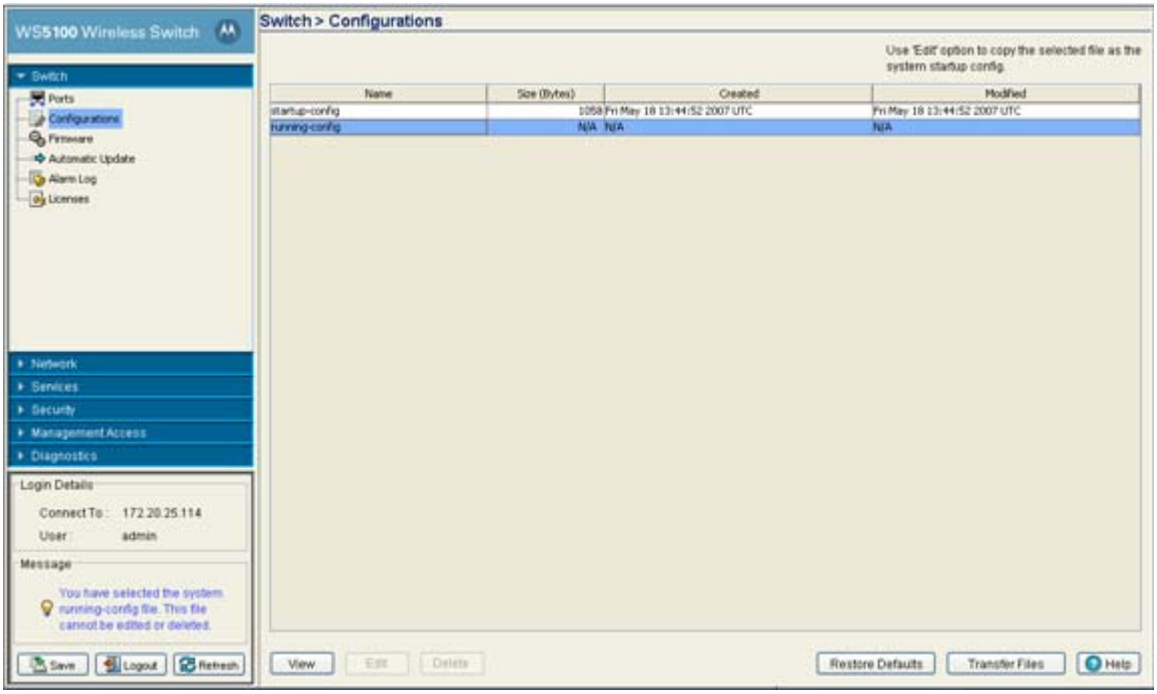
Use the **Configurations** screen to review the configuration files available to the switch. The details of each file can be viewed individually. Optionally, you can edit the file to modify its name or use the file as the startup configuration. A file can be deleted from the list of available configurations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

NOTE: If you would like 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 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 a tabular format. Each file can be edited, viewed or deleted.

Name	Displays a list of existing configuration files that can used with the switch.
Size (Bytes)	Displays the size (in bytes) of each available switch 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.

2. To view the entire 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 on page 3-17*.
3. To modify a configuration file name and/or use it as the configuration at startup, select a row (other than the start-up-config or running config) from the table and click the **Edit** button. For more information, see *Editing a Config File on page 3-18*.

NOTE: Selecting either the startup-config or running-config does not enable the Edit button. A different configuration file must be available to enable the Edit button 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 name 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 file and revert the settings back to their factory default, click the **Restore Defaults** button.

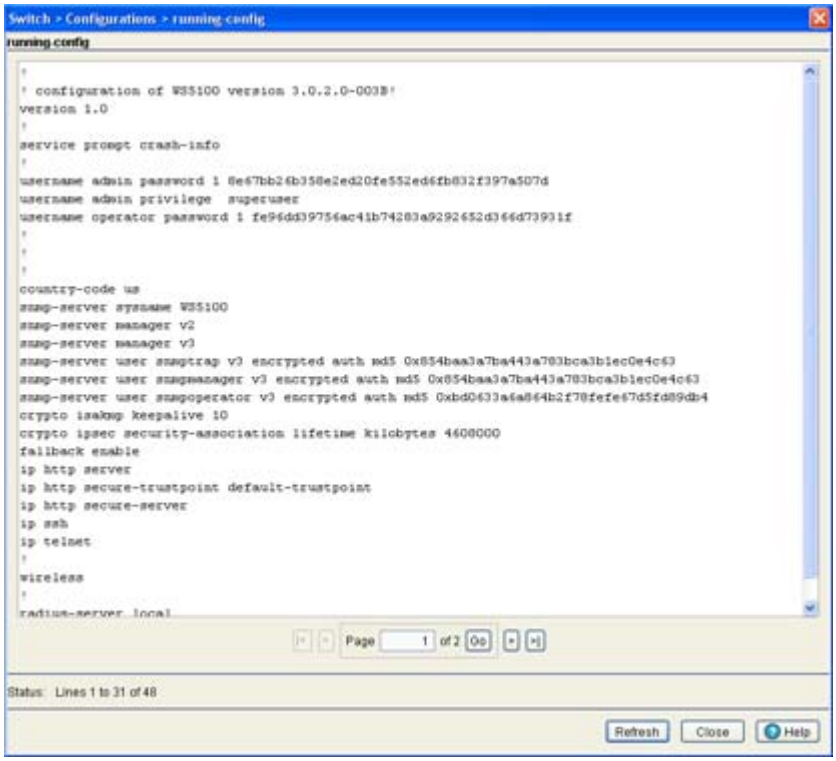
NOTE: After setting the switch to revert to factory default settings, the system must be rebooted before the factory default settings will take effect. When this occurs, the switch IP address may change.

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 on page 3-19*.

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 from the View screen 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.



3. The **Main** screen displays the contents of the configuration file.

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

4. The **Page** parameter displays the portion of the configuration file currently displayed 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.

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

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

3.3.2 Editing a Config File

Configuration files display in the **Name** field within the Configuration tab. If necessary, change the name of the file to meet the needs of the revised configuration.

To edit the contents of a configuration file:

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

2. Select a configuration file from those displayed within the configuration screen and click the **Edit** button.

3. Select the **Copy this file as the system startup config** checkbox to use this configuration file as the switch configuration on the next boot. Ensure this file meets the switch's initial (startup) configuration requirements before selecting this option.
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.
6. Click **Cancel** to close the dialog without committing updates to the running configuration

3.3.3 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	Use the **Using** drop down-menu to configure whether the log file transfer is conducted using FTP or TFTP.
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 the appropriate **Path** name to the target directory on the local system disk or server. The Target options are different depending on the target selected.

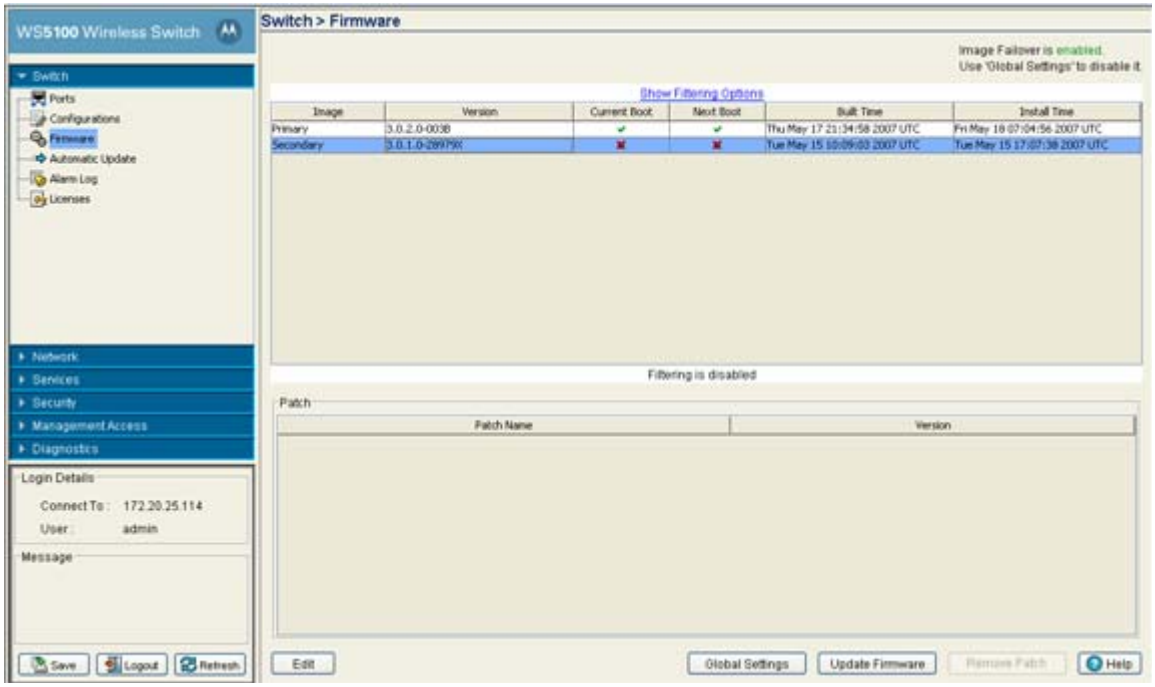
3. Refer to the **Target** field to specify the details of the target file.

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

4. 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.
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 **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 two software versions. Information about 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 name for each firmware version 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.

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 to go with it. 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 that will be used when the switch is booted the next time. For more information, see *Editing the Switch Firmware on page 3-21*.
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 Failover Image on page 3-22*.
6. Click on the **Update Firmware** button to update the firmware file loaded onto the switch. For more information, see *Updating the Switch Firmware on page 3-23*.

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.

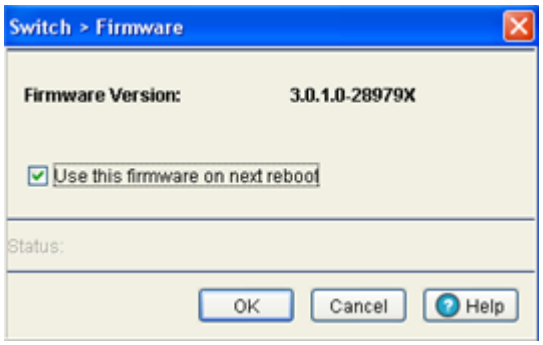
3.4.1 Editing the Switch Firmware

The Edit screen enables the user to select a firmware version 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 the file initiated 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 Failover Image

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*.

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 that is specified for the firmware update.
   b. Use **TFTP** to get the firmware update from a *Trivial File Transfer Protocol* (TFTP) server.
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 will also be restarted regardless of its state before the reboot.

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

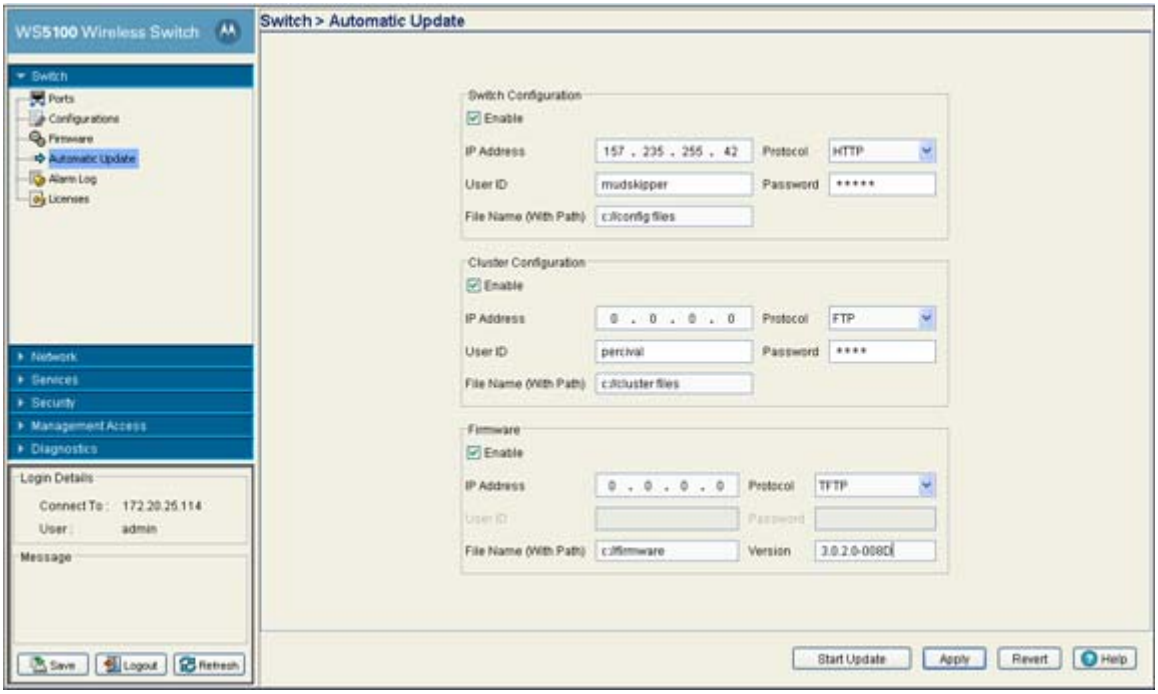
12. Refer to the **Status** field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the switch.
13. Click **Cancel** to close the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

3.5 Configuring Automatic Updates

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

3. Refer to the **Cluster 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 will be 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.

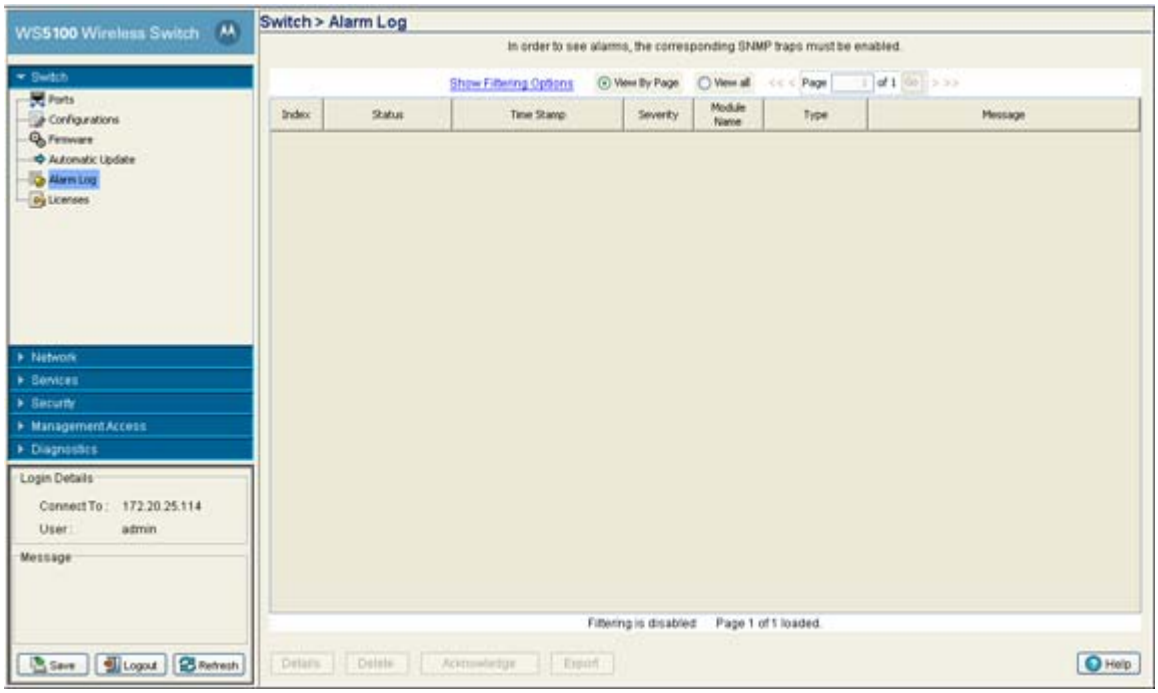
5. Click the **Apply** button to save the changes to the configuration.
6. Click the **Revert** button to revert back to the last saved configuration.

3.6 Viewing the Switch Alarm Log

Use the **Alarm Log** screen as an initial snapshot for alarm log information. Use this screen to expand alarms for greater detail, delete alarms, acknowledge alarms or export alarm data to a user-specified location.

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 as required to view alarm log data by page or the by 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 display alarm logs in pages. 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 the alarm from other alarms 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 with 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 detailed 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 the solution and possible causes. For more information, see *Viewing Alarm Log Details on page 3-27*.
6. Select the alarm(s) from those listed and click the **Delete** button to remove them from the list of alarms.

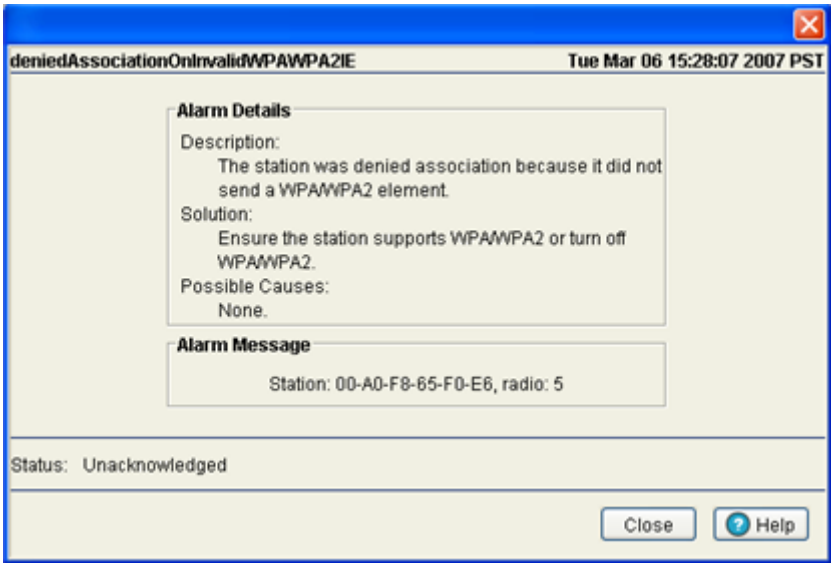
   This is not recommended in instances where the problem is unacknowledged and the criticality has not yet been assessed.
7. Select the unacknowledged alarm(s) from those listed and click the **Acknowledge** button to acknowledge them.
8. Click the **Export** button to export the content of the table to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

3.6.1 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 it.

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 fields within the Details screen for the following information:

Severity	Displays the severity of the event. Use these numeric identifiers to assess the criticality of this specific alarm. The Severity classes include: **Critical**, **Major**, **Warning**, **Informational** and **Normal**.
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.
Possible Causes	Describes the probable causes that could have raised the specific alarm. Determine whether the causes listed can be remedied in order to avoid this alarm from being raised in the future.

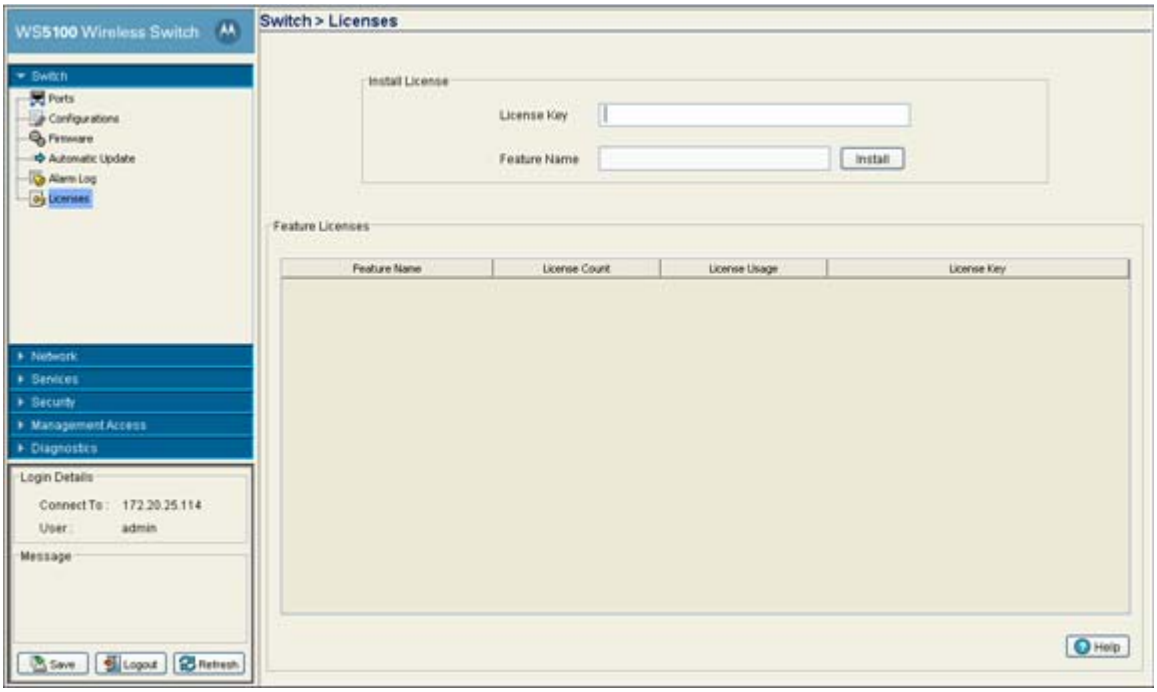
4. Click **OK** to use the changes to the running configuration and close the dialog.

3.7 Viewing Switch Licenses

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

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 provided when you supply the switch MAC address to Motorola customer care.
Feature Name	The name of the feature you wish to install/upgrade using the license.

3. Click the **Install** button to install the selected license.
4. Refer to the **Feature Licenses** table for the following license specific information:

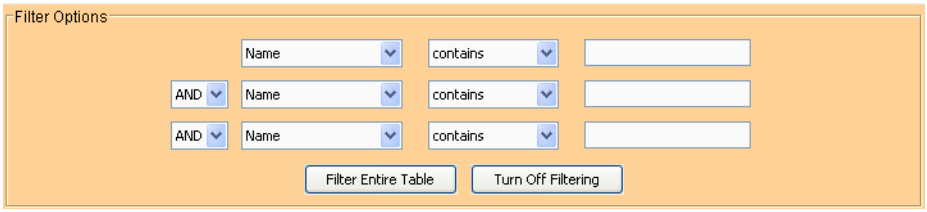
Feature Name	Displays the name of the feature either installed or upgraded on the switch.
License Count	The number of licenses that you have applied while entering the license key.
License Usage	The number of license currently in use. Determine whether this number adequately represents the number of switches you need 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.

3.8 How to use the Filter Option

Use the Filter Option to sort the display details of any 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.
3. The fields in the Filter Option zone are populated with the parameters of the screen in which it appears. Filtering is always conducted for the entire table.
4. 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
5. 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.
6. 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 sections:

- *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 Access Port Status*

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.

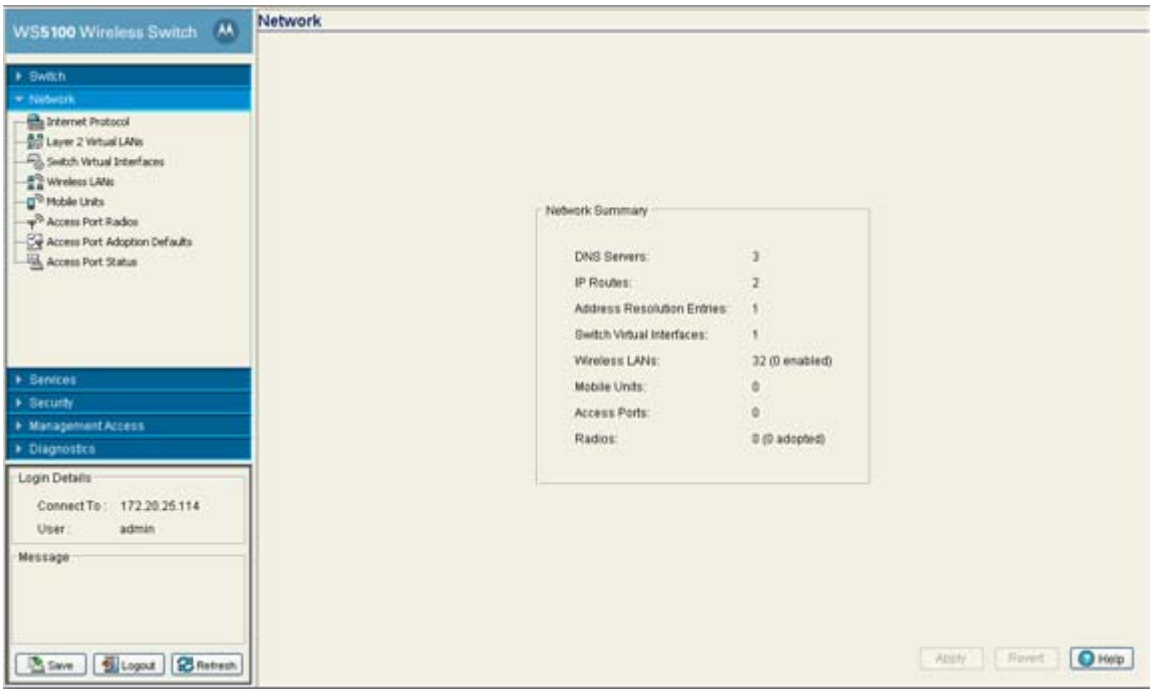
4.1 Displaying the Network Interface

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 what 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 4-3*.
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 4-5*.
Additional Resolution Entries	Displays the number of mappings of layer three (IP) addresses to layer two (MAC) addresses. 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 4-12*.
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 4-20*.
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 4-57*.

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 4-64*.
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 *Viewing Access Port Status on page 4-92*.

4.2 Viewing Network IP Information

Use the **Internet Protocol** screen to view and configure network associated IP details. The Internet Protocol screen consists of the following tabs:

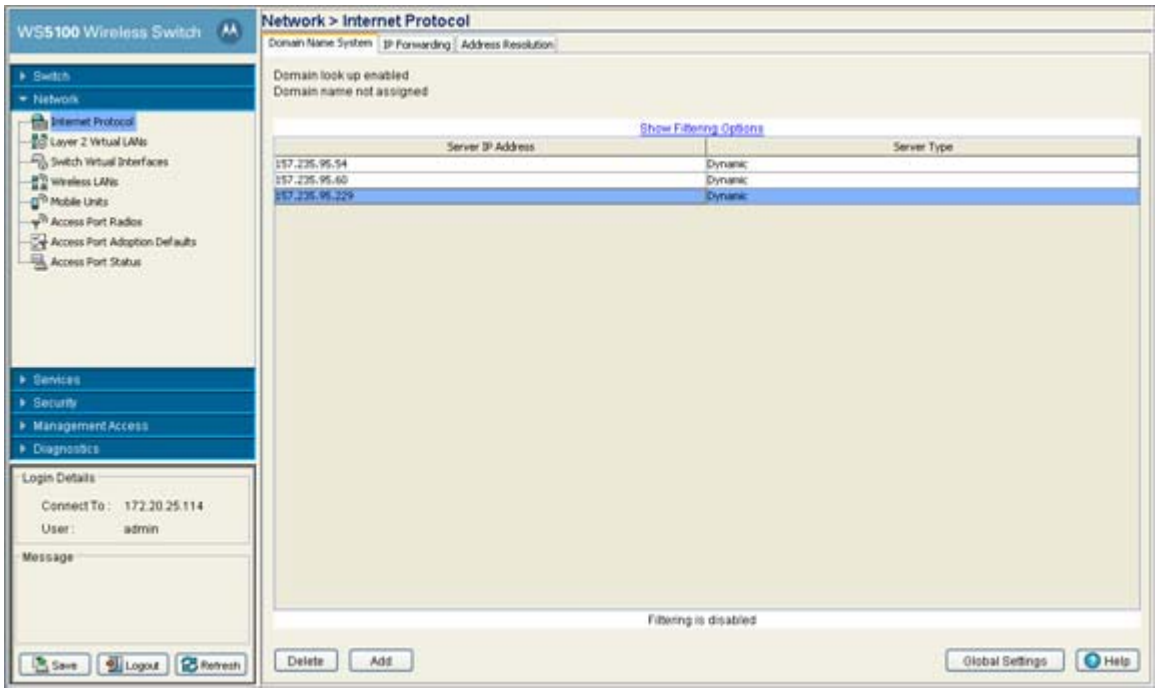
- *Configuring DNS*
- *Configuring IP Forwarding*
- *Viewing Address Resolution*

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.

   Use the Filtering Option 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 which will be displayed on the list. A static DNS IP address can be created by clicking the **Add** button.

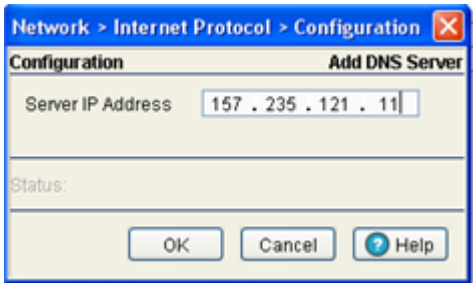
4. Select an IP Address from the table and click the **Delete** button to remove the selected entry from the list.
5. Click the **Add** button to display a screen used to add another domain name server. For more information, see *Adding an IP Address for a DNS Server on page 4-4*.
6. Click the **Global 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 4-4*.

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.



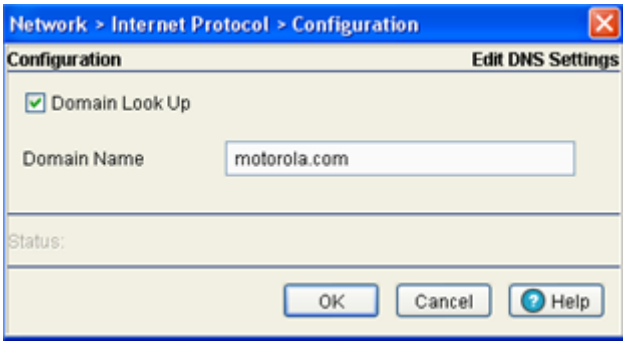
2. Enter the **Server IP Address** to define the IP address of the new static domain name server.
3. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
4. 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 allowing you to edit 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.

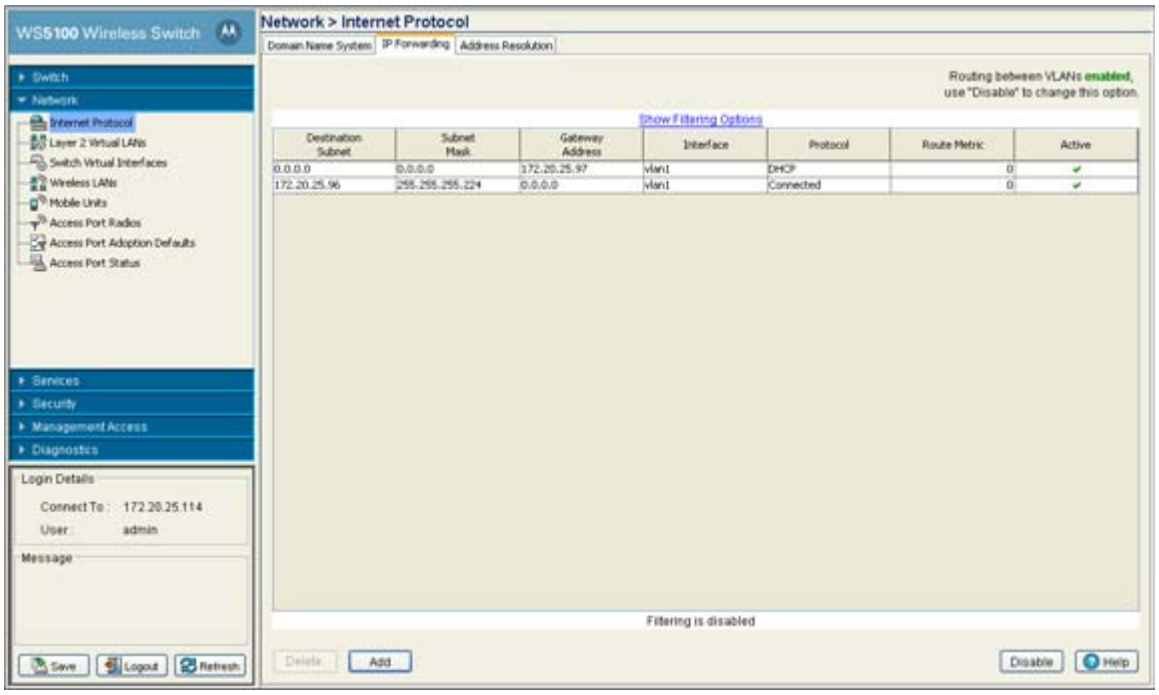
3. Enter a **Domain Name** in the text field. This is the domain the switch is installed in.
4. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
5. Click **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 details:

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.

Route Metric	The **Route Metric** is used for selecting the best available path. If there are multiple routes for a particular destination address, the packets are forwarded on the basis of the route metric. Routes with lower metric value are given higher preference. A routing protocol uses the route metric to determine which routes to include in the routing table when it has two available routes to the same destination from a single routing protocol (static, RIP, OSPF etc). The router includes the route with the smallest metric because it considers this route to be the shortest (and therefore the best). Different routing protocols calculate their metric in different ways. RIP uses hops, OSPF uses bandwidth etc. Sample values: 0, 1, 10, 20… Currently all static and connected routes have a default metric of 0.
Active	When IP Forwarding is enabled for the selected subnet, a green check displays in the Active column.

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.

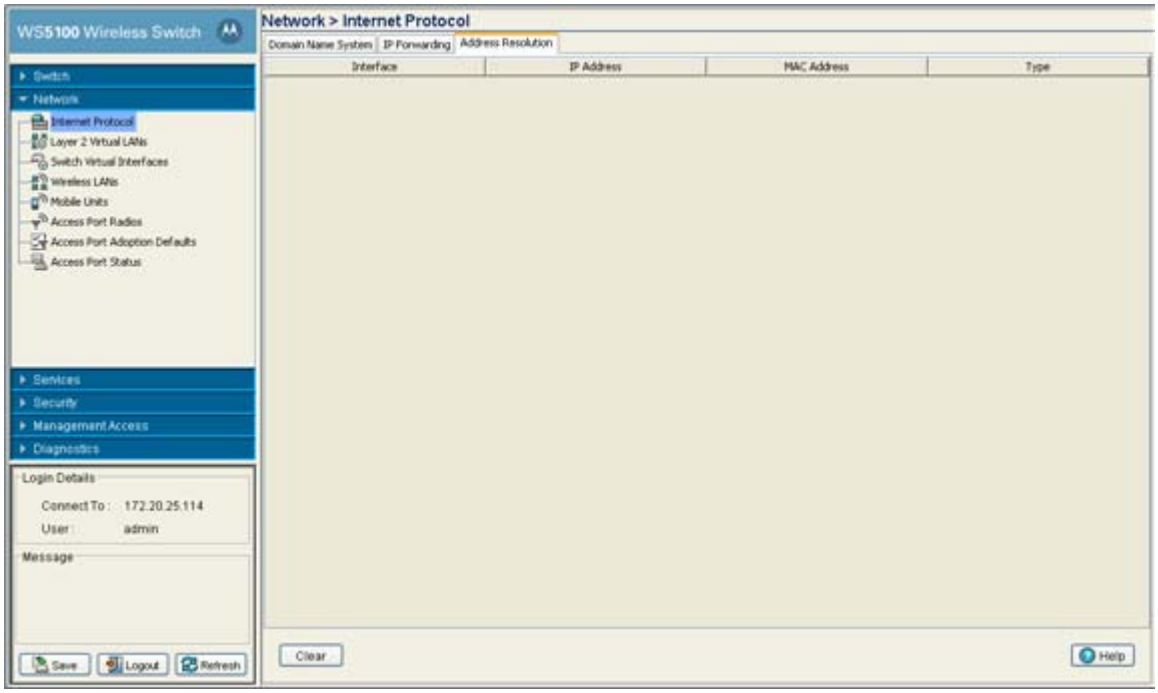
   The Subnet Mask is the IP mask used to divide internet addresses into blocks known as subnets. A value of 255.255.255.0 support 256 IP addresses.
4. In the **Gateway Address** field, enter the IP address of the gateway used to route the packets to the specified destination subnet. Do not set the gateway 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 the details of the tab:

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 on which the IP address was found (typically a VLAN).
IP Address	Displays the IP address being resolved.
MAC Address	Displays the MAC address that correspond to the IP address being resolved.
Type	Defines whether the entry was added statically or created dynamically due to network traffic. Entries are typically static.

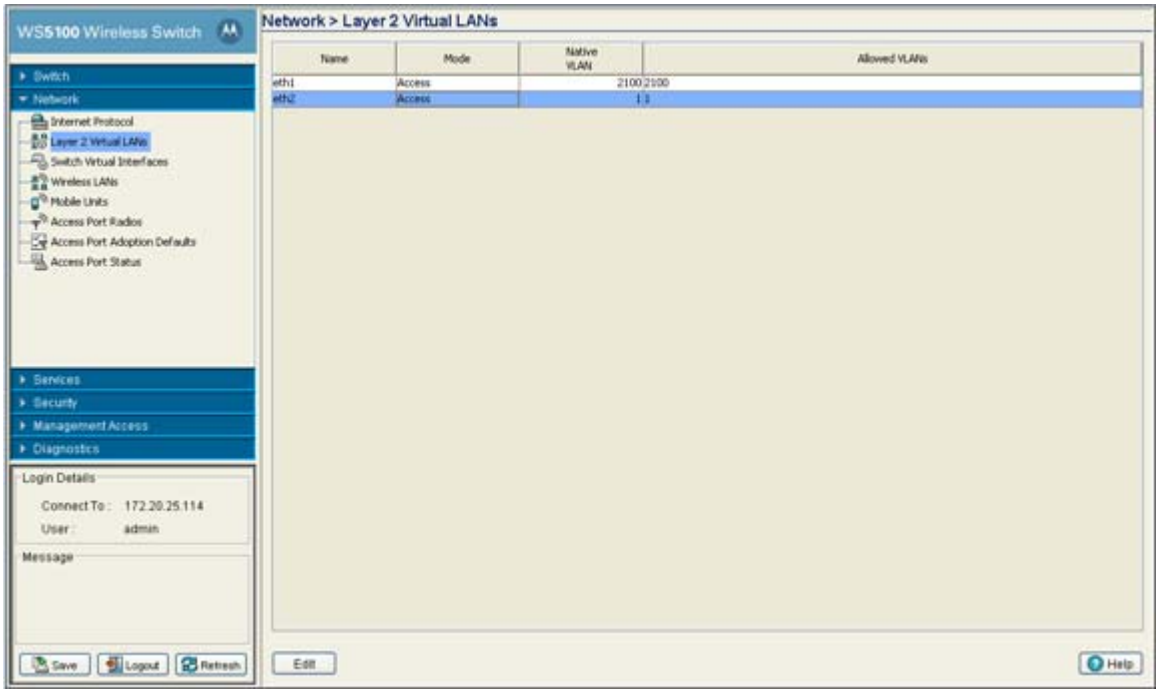
4. Click the **Clear** button to remove the selected AP entry if no longer usable.

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 perform as if they are connected to the same LAN, but they may be connected at various physical connections across the LAN segment. The VLAN can be connected at various physical points but react as if it were connected directly. Therefore, a VLAN is an independent network made up of several devices. One of the biggest advantages of VLANs is that 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.

Use the **Layer 2 Virtual LANs** screen to view and configure VLAN properties. To view Virtual LANs details:

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



The following details display in the table:

Name	Displays the name of the VLAN to which the switch is currently connected. It can be either ethernet 1 or ethernet 2.
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 that you add to the trunk.
Native VLAN	Displays the tag assigned to the native VLAN.
Allowed VLANs	Displays VLAN tags allowed on this interface

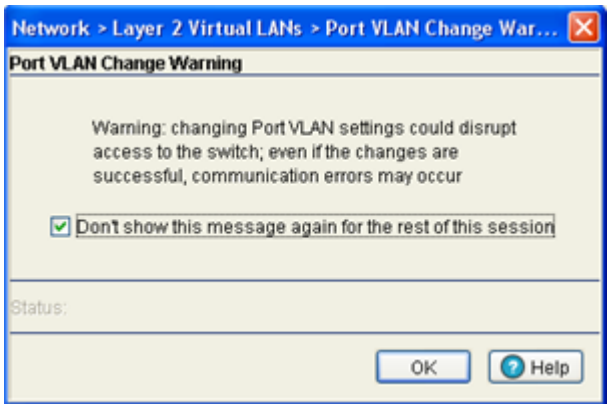
Select a record from the table and click the **Edit** button to modify the record. For more information, see *Editing the Details of an Existing VLAN on page 4-11*.

4.3.1 Editing the Details of an Existing VLAN

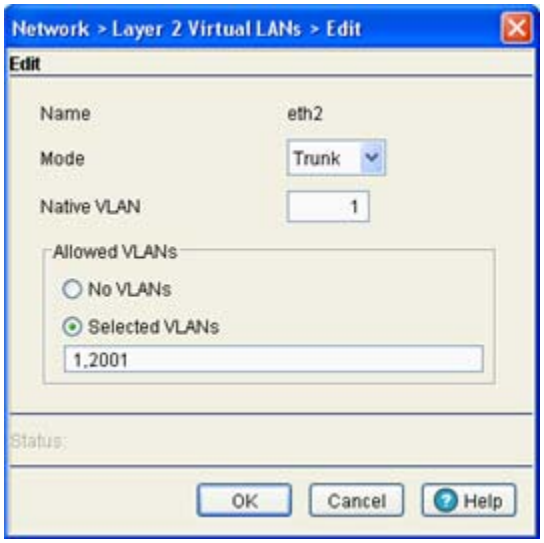
To revise the configuration of an existing VLAN:

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. The Layer 2 Virtual LANs Edit dialog box for the selected ethernet allows you to configure/modify the VLANs.



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 that you 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.

4.4 Configuring Switch Virtual Interfaces

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

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 that 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 properly with the rest of the network.

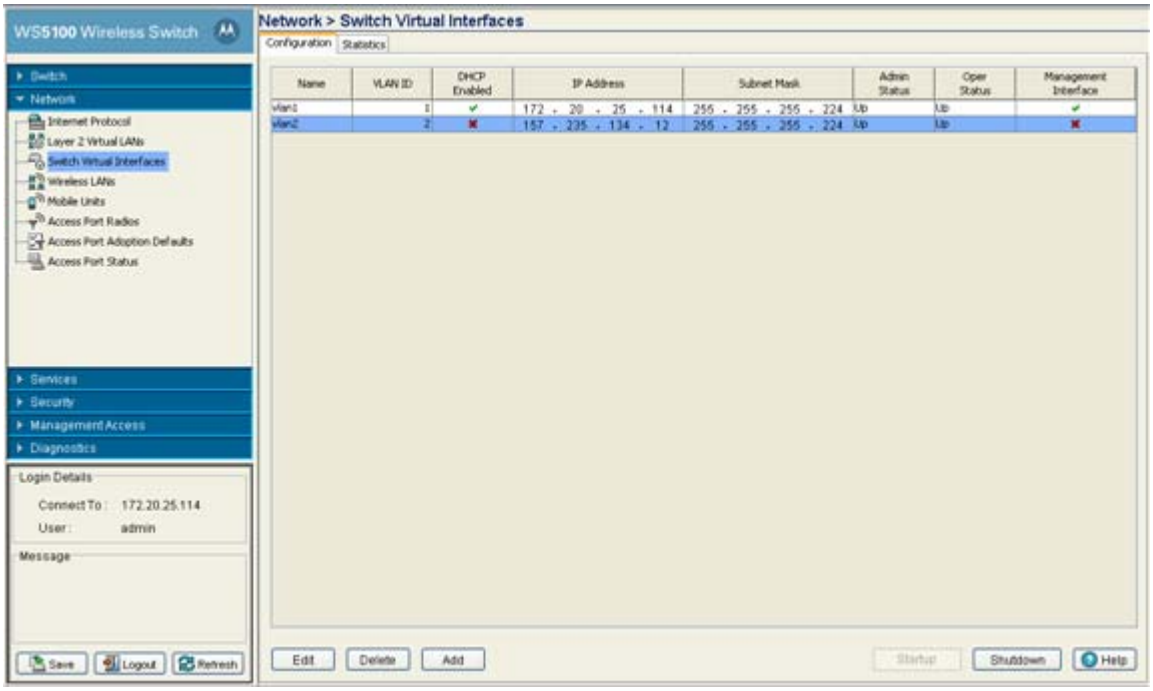
Use the **Switch Virtual Interfaces** screen to view and configure VLAN interfaces. This screen consists of the following tabs:

- *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	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.
IP Address	Displays the IP address for the virtual interface.
Subnet Mask	Displays the subnet mask assigned for this interface.
Oper Status	Displays whether the selected Switch Virtual Interface is currently invoked on the switch (Up) or not (Down).
Management Interface	A green checkmark within this column defines this VLAN as the one currently used by the switch management interface. This designates the interface settings used for global switch settings in case of any conflicts. For example, if multiple SVIs are configured with DHCP enabled on each, the switch could have multiple domain names assigned from the different DHCP servers. This setting does not affect any of the Management Access Interfaces configured using *Configuring Access Control on page 7-2*.

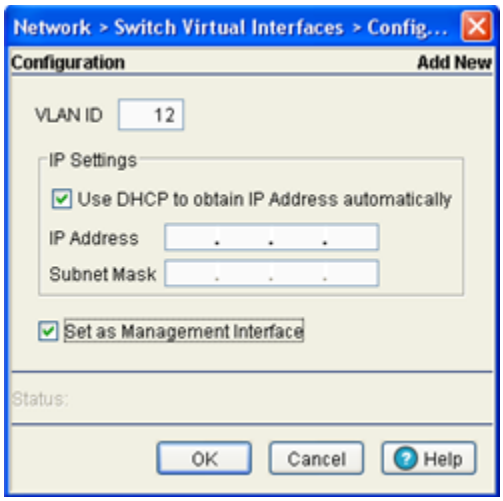
3. Select a record from the table and click the **Edit** button to modify the record. For more information, see *Modifying a Virtual Interface on page 4-14*.
4. Select a record from the table and click the **Delete** button to remove the configuration from the list of switch virtual interfaces.
5. Click the **Add** button to add a new configuration to the switch virtual interface. For more information, see *Adding a Virtual Interface on page 4-14*.

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 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. The IP Setting field consists of the following:
   a. Select **Use DHCP to obtain IP Address automatically to** enable DHCP to provide the IP address for the switch's virtual interface. Selecting this 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.
6. Select the **Set as Management Interface** checkbox to enable any host displayed in this VLAN to configure 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 **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.

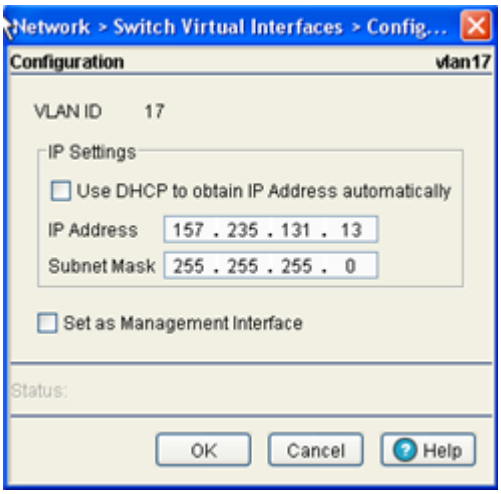
4.4.1.2 Modifying a Virtual Interface

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. Unselect the **Use DHCP to obtain IP Address automatically** checkbox to assign IP addresses manually and do not want DHCP to provide them.
4. Use the **IP Address** field to manually enter the IP address for the virtual interface.
5. Enter the **Subnet Mask** for the IP address.
6. Select the **Set as Management Interface** checkbox to convert the selected VLAN ID as management interface.
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.

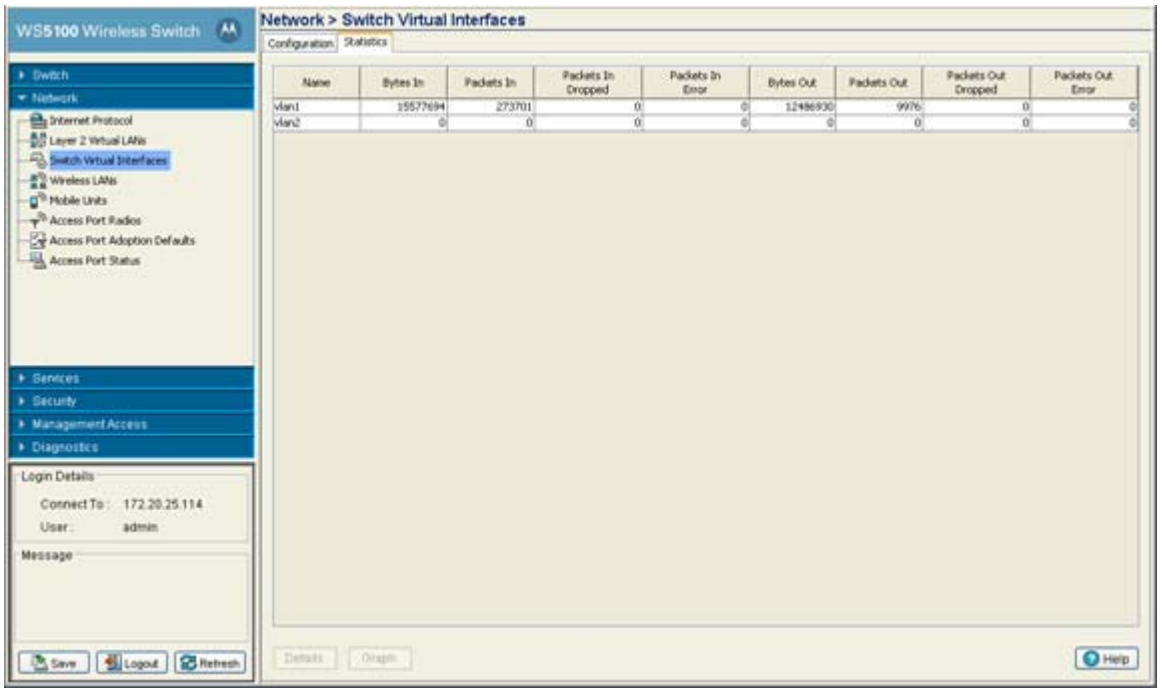
4.4.2 Viewing Virtual Interface Statistics

The **Statistics** screen displays information from the switch software and hardware modules about the packet level statistics and errors at the interface defined.

To view virtual interface statistics:

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

2. Select the **Statistics** tab.



3. Refer to the following details as displayed within the Statistics tab:

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 periodically. To view the current status, click on 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 in the following situations: 1. If the input queue for the hardware device/software module handling the interface definition is saturated/full. 2. Overruns – occurs when the interface receives packets faster than it can transfer them to any buffer.

Packets In Error	Displays the number of error packets coming into the interface.It includes: • 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 CRC value computed by the interface does not match with 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 spec. 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 of the interface.
Packets Out Dropped	Displays the number of dropped packets going out of the interface, due to the 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.

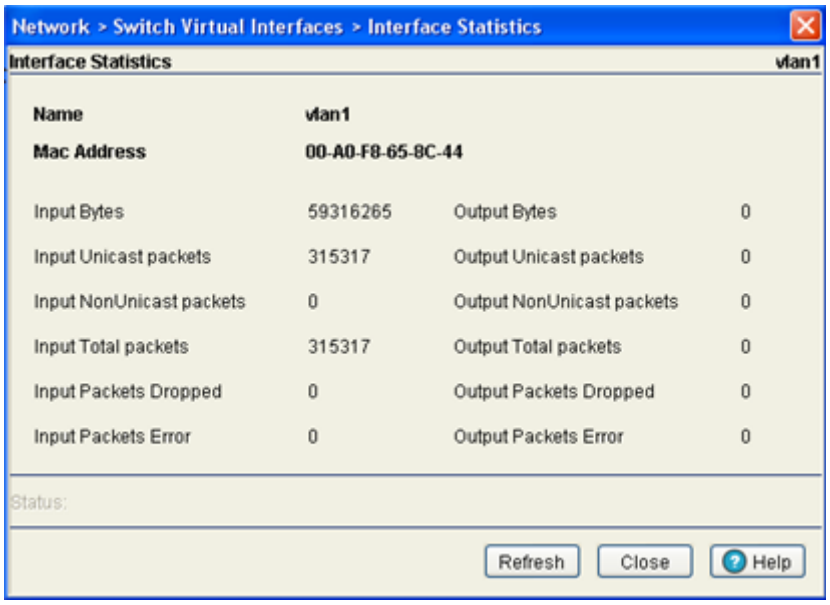
3. Click the **Details** button to view packet level statistics of any user defined interface. For more information, see *Viewing Virtual Interface Statistics on page 4-17*.
4. Click the **Graph** button to view a graphical representation of the switch virtual interface statistics. For more information, see *Viewing the Virtual Interface Statistics Graph on page 4-19*.

4.4.2.1 Viewing Virtual Interface Statistics

To view detailed virtual interface statistics:

1. Select a record from the table displayed in the Statistics screen.

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 in 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 received 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 received 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 the 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 at the interface. 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).

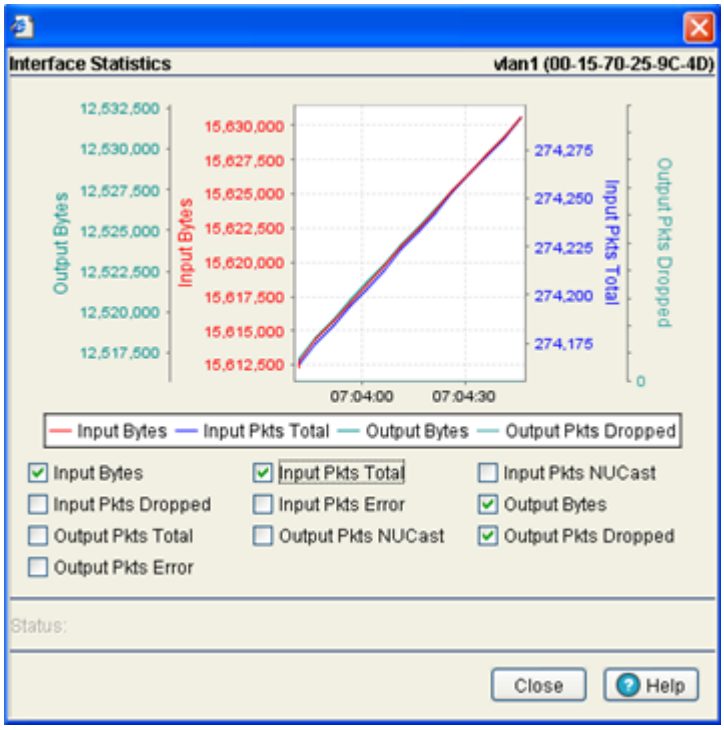
4.4.2.2 Viewing the Virtual Interface Statistics Graph

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.

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: Do not select more than four parameters 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 check the WLANs that are active, their VLAN assignments, updates to a WLANs description and their current authentication and encryption schemes.The Wireless LANs screen consists of the following tabs:

- *Configuring WLANs*
- *Viewing WLAN Statistics*
- *Viewing VLAN/Tunnel Assignments*
- *Configuring WMM*

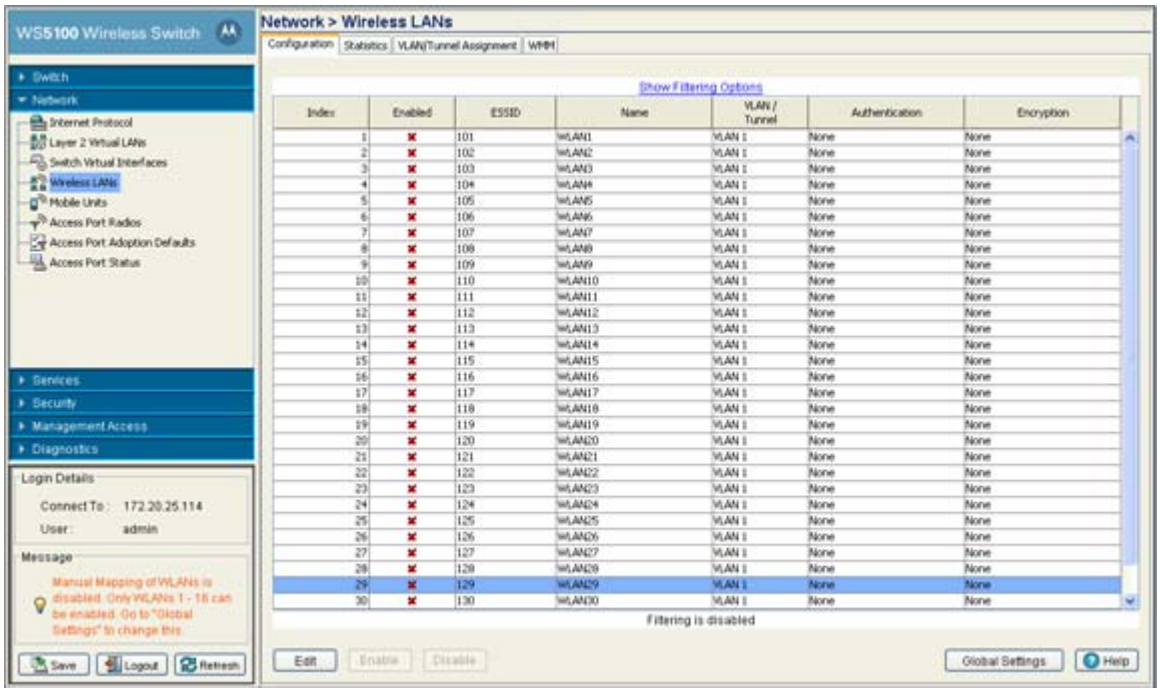
4.5.1 Configuring WLANs

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. the WS5100 supports 32 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 32. 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.
Name	Displays a short description of the associated WLAN. Click the Edit button to modify the value the WLAN description.
VLAN/Tunnel	Displays the name of the VLAN/Tunnel the WLAN is associated with. The VLAN ID is an integer assigned for the corresponding user defined name. The VLAN ID can be between 1 and 4094. The default VLAN ID is 1.
Authentication	Displays the type of authentication in use with the specified WLAN. Click the Edit button to modify the WLAN's current authentication scheme.
Encryption	Displays the type of wireless encryption in use 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.

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. 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. Click the **Global Settings** button to display a screen with WLAN settings applying to the all the WLANs on the system. Checkbox options within the Global Settings screen include:
   - MU Proxy ARP handling - Selected by default.
   - WLAN Prioritization - Selected by default.
   - Shared Key Authentication
   - Manual mapping of WLANs

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 safeguard the transmission of RF packets between WLANs and the MU traffic each supports.

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) or encryption (WEP, KeyGuard, WPA/TKIP or WPA2/CCMP) scheme best suited to the coverage area the policy supports.

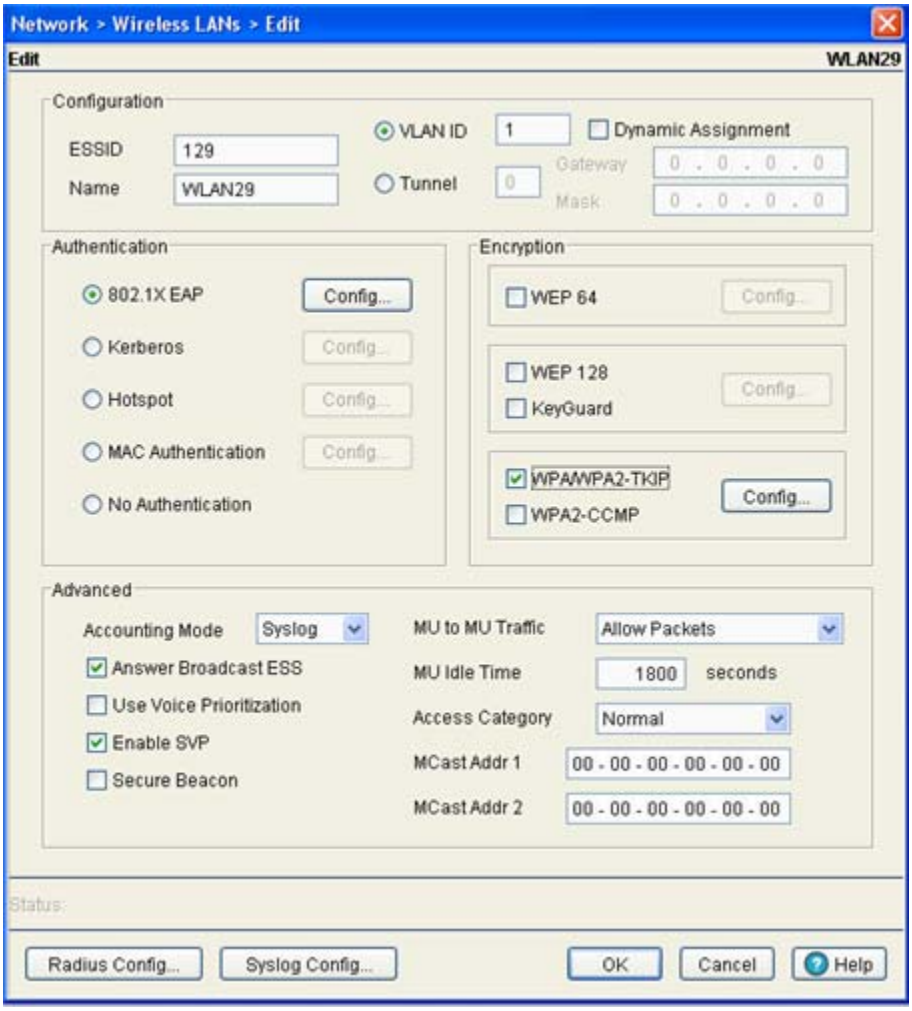
All of the default WLANs are available for modification when the user accesses the Wireless LANs screen. However, the WLAN requires an authentication or encryption scheme be applied before it can begin protecting the data proliferating the switch-managed wireless network.

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 edit 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 Service Set ID associated with each WLAN. If changing the SSID, ensure the value used is unique.
Name	If editing an existing WLAN, ensure its description is updates accordingly to best describe the intended function of the WLAN.

VLAN ID — Select the **VLAN ID** checkbox to change the VLAN designation for this WLAN. By default, all WLANs created are assigned to VLAN 1. Select the **Dynamic Assignment** checkbox for an automatic VLAN assignment for this WLAN. The WS5100 Series Switch cannot route traffic between different VLANs on ETH1 and ETH2. Be cognizant of this limitation when planning to route traffic between different VLANs.

Tunnel — Select the **Tunnel** checkbox to enable a field for entering the tunnel number to be used with this WLAN. The available range is from 1-32. Enter the **Gateway** and **Mask** addresses used with the tunnel. When selected, the **VLAN ID** field is not available. Do not set the gateway address to any VLAN interface used by the switch.

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 4-26*.

Kerberos — A Kerberos server is used to authenticate users. For detailed information on configuring Kerberos for the WLAN, see *Configuring Kerboros on page 4-27*.

Hotspot — A hotspot is used to authenticate users to a designated WLAN for a defined period of time. The attributes of both the hotspot and the Radius Server are required. For more information, see *Configuring Hotspots on page 4-29*.

Dynamic MAC ACL — 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 Dynamic MAC ACL on page 4-36*

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 radio button 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 4-40*.

WEP 128 — Use the WEP 128 radio button 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 4-41*.

KeyGuard — Uses a Motorola MU proprietary encryption mechanism to protect data. For detailed information on configuring KeyGuard for the WLAN, see *Configuring WEP 128 / KeyGuard on page 4-41*.

WPA-WPA2-TKIP	Use the WPA-TKIP radio button 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 4-43*.
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 4-43*.

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 or MAC Authentication 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	Enabling Broadcast ESS allows you to broadcast the WLANs SSID with outgoing data traffic.
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.
Enable SVP	Enabling SVP (*Spectralink Voice Prioritization*) sends packets allowing the switch to identify MU's as voice MU's. Thereafter, any UDP packet sent by these MU's is prioritized ahead of data.
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.
MU to MU Traffic	Allows frames from one MU, where the destination MAC is of another MU, are switch to that 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 • Forward through switch – The frames from the MU are switched out to the wired network (out of the switch). Another upstream device decides whether the frame should be sent back to the second MU, and if so, it sends the frame back to the switch and is switched out just like any other frame on the wire.
MU Idle Time	Set the MUs idle time limit in seconds.

Access Category	Displays the Access Category for the intended AP 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 • Video– Optimized for video traffic • 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 multicast 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.

NOTE: If the WLAN is supporting multimedia applications (video or voice), ensure a valid multicast address is provided. If using a 802.11bg radio, ensure “24” is also selected as an additional Basic data rate. In addition, ensure the “multicast-packet-limit 128 vlan-id" CLI command is properly configured under the “wireless” context.

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.

4.5.1.2 Configuring Authentication Types

Refer to the following to configure the WLAN authentication options available on the WS5100. Refer to the following

- *Configuring 802.1x EAP*
- *Configuring Kerboros*
- *Configuring Hotspots*
  - *Configuring an Internal Hotspot*
  - *Configuring External Hotspot*
  - *Configuring Advanced Hotspot*
- *Configuring Dynamic MAC ACL*

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.

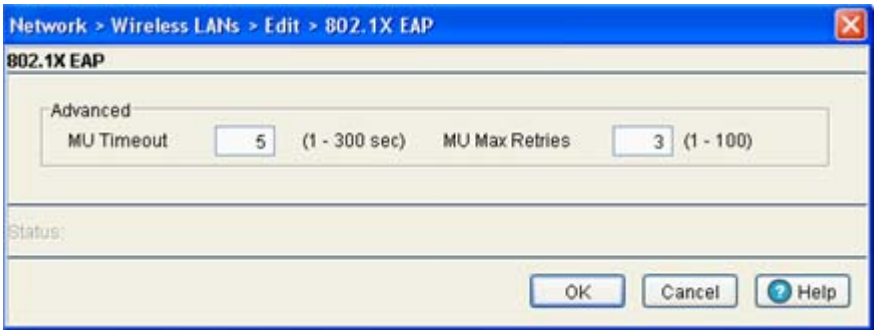
NOTE: As part of the EAP configuration process, ensure a primary and optional secondary Radius server have been properly configured to authenticate the users requesting access to the EAP protected WLAN. For more information on configuring Radius Server support for the EAP 802.1x WLAN, see *Configuring External Radius Server Support on page 4-36*.

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 4-36*.
4. Click the **Config** button to the right of the 802.1X EAP checkbox.

   The 802.1x EAP screen displays.



5. Configure the **Advanced** field as required to 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 10 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 10 retries.

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 Kerboros

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 on the 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

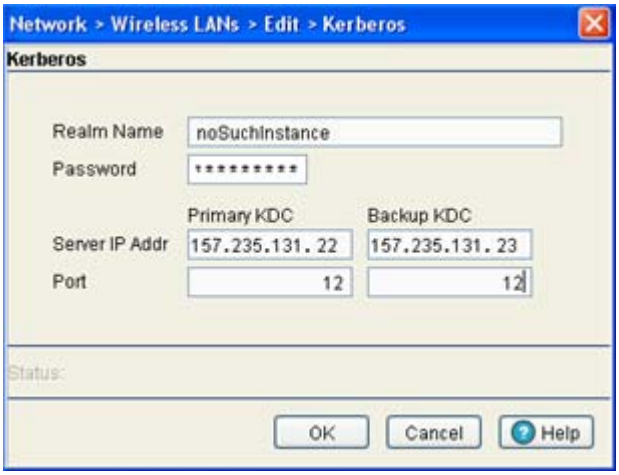
To configure a Kerberos authentication scheme for a WLAN:

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** (for example, MOTOROLA.COM).

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

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

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 Hotspots

A hotspot is essentially a Web page granting user access to the Internet (in this case within a switch managed WLAN). With the inlflux 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.

When a user visits a public hotspot and wants to browse to a Web page, they 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 but its does require the client's WLAN adapter be set to receive its IP configuration through DHCP.

To setup a hotspot on a switch, 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:

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

Switch Hotspot Redirection

To redirect user traffic from a default home page to the login page, the switch uses destination network address translation. 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).

Refer to the following scenario. An unauthenticated hotspot client associates to the hotspot WLAN. The client WLAN adapted initiates a DHCP broadcast. The switch detects this as DHCP broadcast traffic from an unauthenticated hotspot WLAN client. The switch forwards these frames to the DHCP server and does not redirect them. The DHCP server responds with an IP configuration for the client and the client is now ready to access the network.

The user then initiates an HTTP session to *www.xyz.com.* The switch detects this as DNS traffic, and again does not redirect it. The DNS server resolves this domain name to an ip address like 63.44.56.98 (for www.xyz.com). The client initiates a TCP session with host 63.44.56.98. This session begins with the client sending a TCP SYN to target IP 63.44.56.98. The switch intercepts this session and responds with a SNY/ACK back to the client (while in the process modifying the source IP address and source port of this return packet to 63.44.56.98:80). The client completes the TCP 3-way handshake with the switch acting as a proxy for the destination IP 63.44.56.98.

Assuming the TCP session opened, the client now sends an HTTP GET to the destination URL. This HTTP GET is again intercepted by the switch and redirected to the hotspot Web site https://10.0.1.77:444/wlan1/

login.html. The client is now redirected to the Login.htm web page of the hotspot instead of landing on their destination Web site (www.xyz.com). The client enters its identification information and is authenticated with the Radius server. Upon successful authentication, the client is presented with the Welcome.htm page. All client traffic from this point forward is authenticated and is forwarded to the Internet (until the user session expires).

To configure hotspot support for the switch:

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 will become 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 4-36*.
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 4-30*.
   - 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 External Hotspot on page 4-32*.
   - 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 Advanced Hotspot on page 4-34*.

NOTE: The appearance and user defined values for the Hotspot screen differ 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.

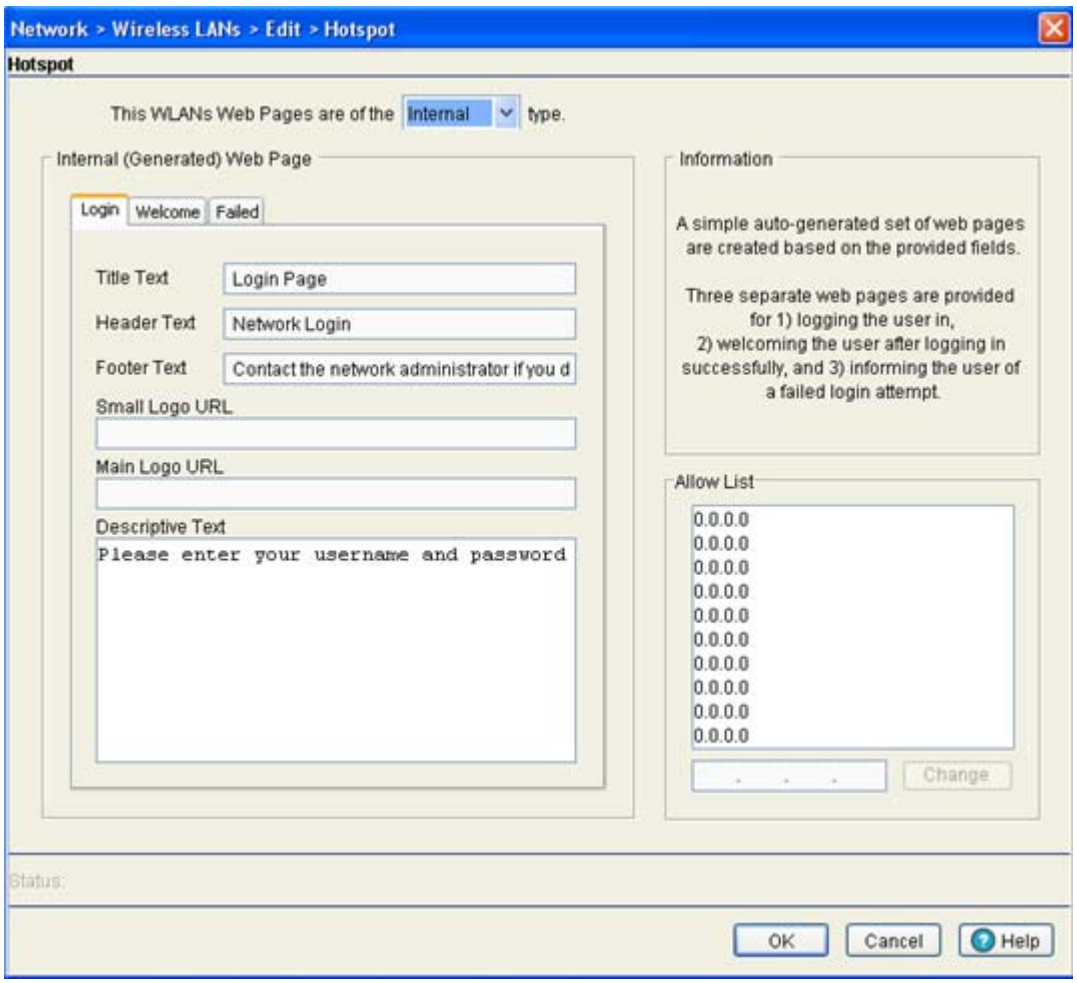
NOTE: As part of the hotspot configuration process, ensure a primary and optional secondary Radius Server have been properly configured to authenticate the users requesting access to the hotspot supported WLAN. For more information on configuring Radius Server support for the hotspot supported WLAN, see *Configuring External Radius Server Support on page 4-36*.

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.

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 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.



3. 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."

4. 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 certain instances, an associated MU may not be able to ping the host within the hotspot. For instance, a hotspot supported WLAN is enabled. Within the Allowed List, a network (157.235.95.0) is added. An MU is associated, and an IP address is obtained for the MU. The MU is then unsuccessful in pinging the host IP address (157.235.95.54) from within the hotspot. Consequently, the Allowed List should be used for host IPs only.

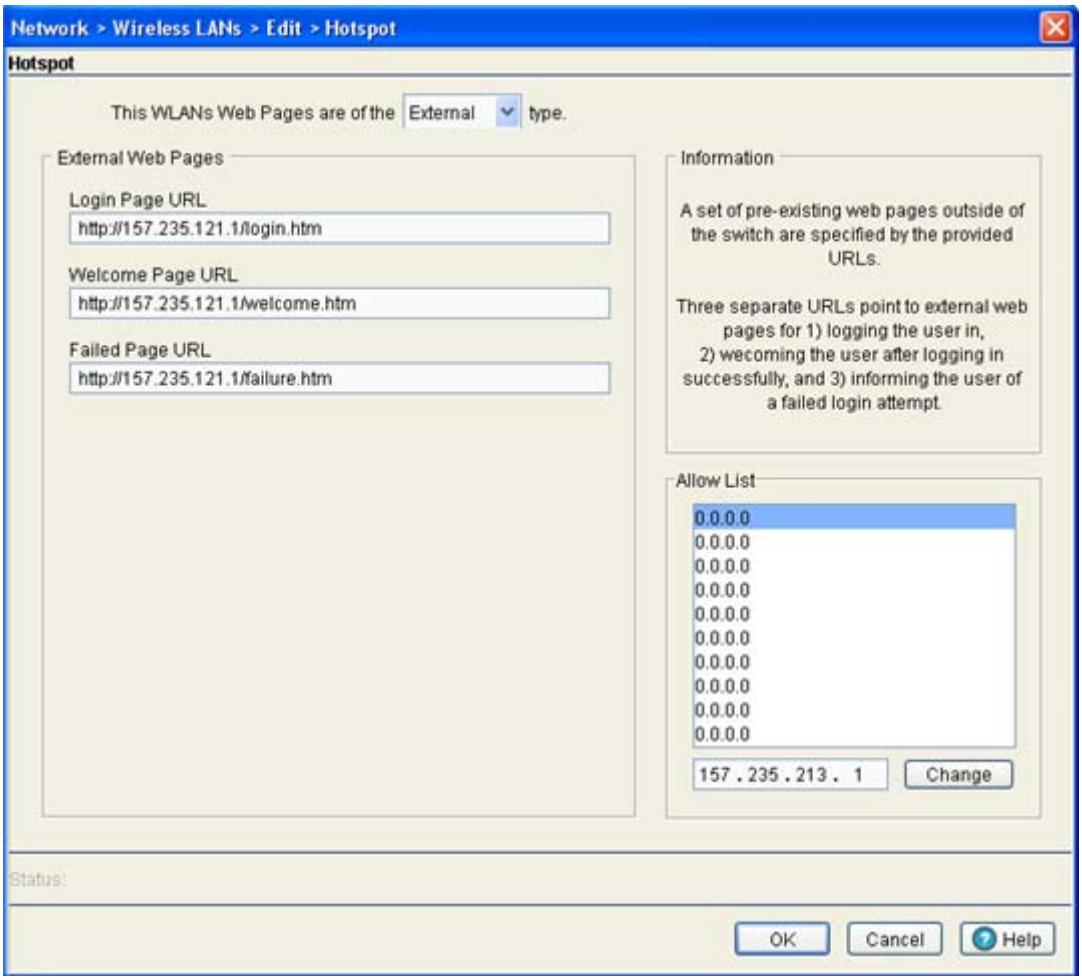
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel**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

Configuring 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. Select an existing WLAN from those displayed within the **Configuration** tab and click the **Edit** button.

2. 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.



3. 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.
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.
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.

4. 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 certain instances, an associated MU may not be able to ping the host within the hotspot. For instance, a hotspot supported WLAN is enabled. Within the Allowed List, a network (157.235.95.0) is added. An MU is associated, and an IP address is obtained for the MU. The MU is then unsuccessful in pinging the host IP address (157.235.95.54) from within the hotspot. Consequently, the Allowed List should be used for host IPs only.

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.

Configuring Advanced Hotspot

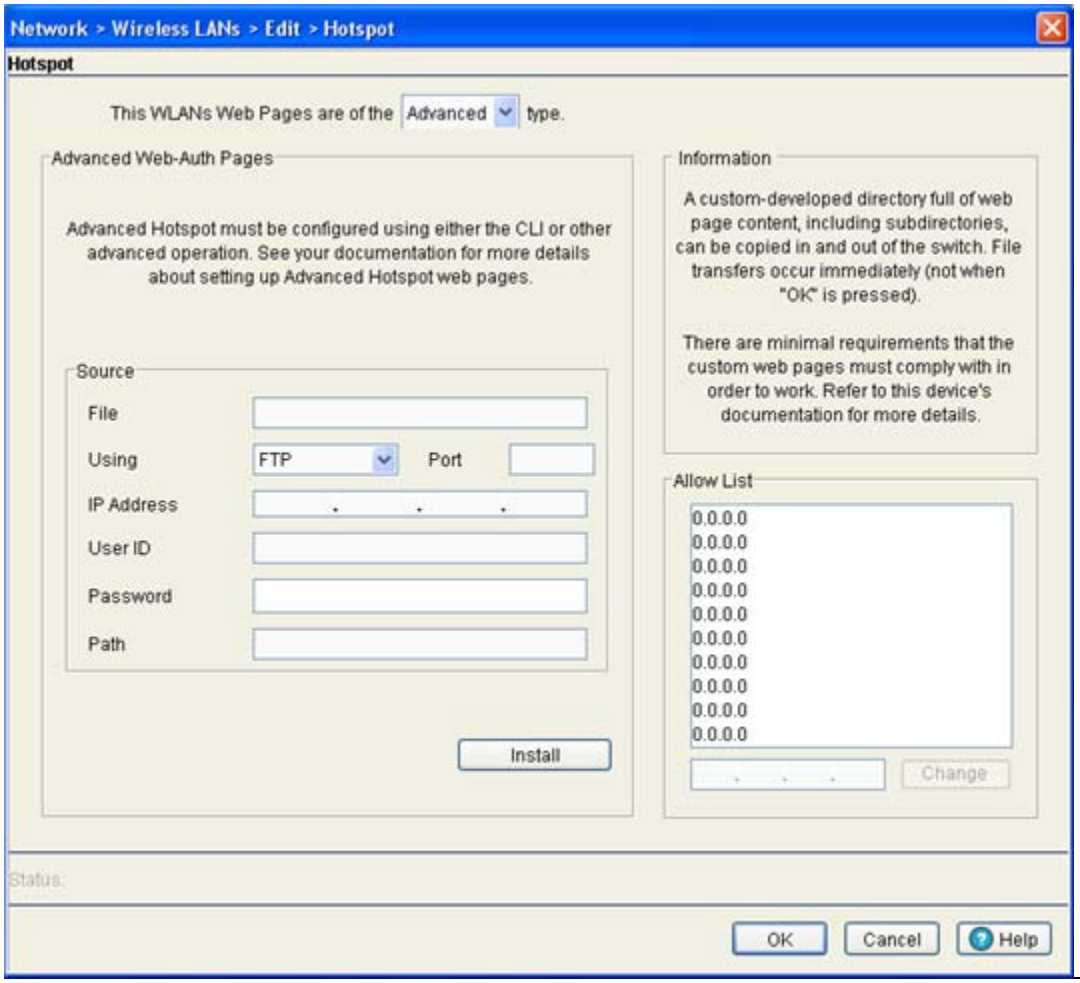
A customer may wish to use advanced Web content (XML, Flash) but might not have (or would not want to use) an external Web server, choosing instead to host the Web pages on the switch's HTTP Web server. Selecting the Advanced option allows for the importing the Web pages from an external source (like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

   a. Specify a source hotspot configuration file. The file used at startup automatically displays within the **File** parameter.

   b. Use 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.

NOTE: In certain instances, an associated MU may not be able to ping the host within the hotspot. For instance, a hotspot supported WLAN is enabled. Within the Allowed List, a network (157.235.95.0) is added. An MU is associated, and an IP address is obtained for the MU. The MU is then unsuccessful in pinging the host IP address (157.235.95.54) from within the hotspot. Consequently, the Allowed List should be used for host IPs only.

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.

Configuring Dynamic MAC ACL

The Dynamic MAC ACL 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 Dynamic MAC ACL configuration 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 Dynamic MAC ACL supported WLAN, see *Configuring External Radius Server Support on page 4-36*.

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 if you elect not use the switch's resident Radius Server.

NOTE: If you elect to use 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 6-62*. The switch's local Radius Server provides an easy setup option and offers a high degree of security and accountability.

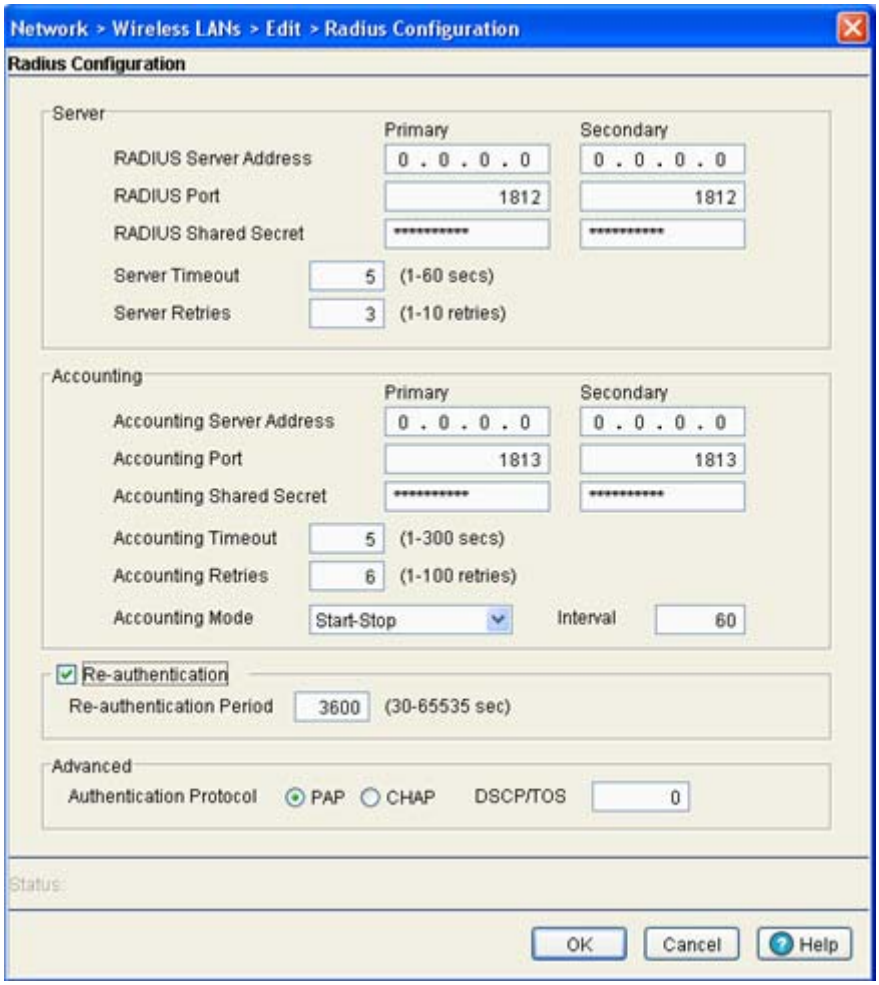
The switch ships with a default configuration defining the local Radius Server as the primary authentication source (default users are admin with superuser privileges and operator with monitor privileges). No secondary authentication source is specified. However, Motorola recommends using an external 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 following the instructions in this section.

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 4-38*.

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 Conig...** button at the bottom of the Network > Wireless LANs > Edit screen.
5. Select the **Radius Conig...** button. The Radius Configuration screen displays for defining an external Radius Server.



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 60 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 10 to indicate the number of times the switch attempts to reach the primary or secondary Radius server before giving up.

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 on 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 periodic re-authentication with the Radius server. Periodic repetition of the authentication process provides ongoing security for current 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 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 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 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 Radius 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.

4.5.1.3 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.

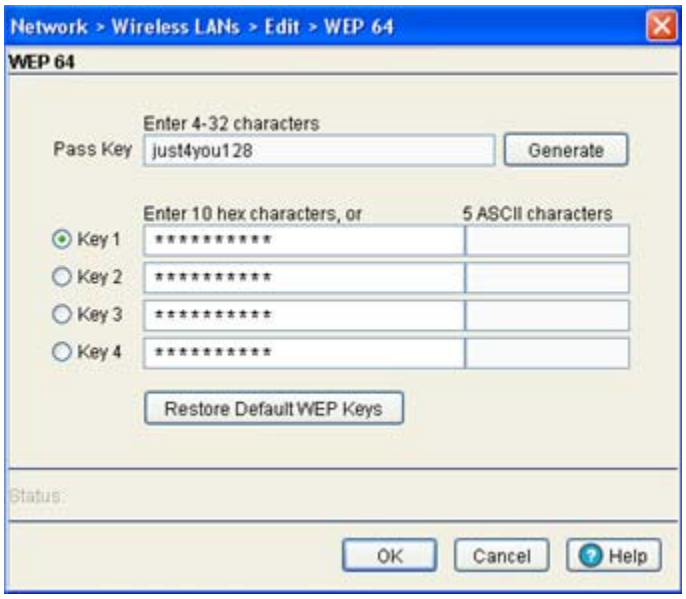
WEP 64 is a less robust encryption scheme than WEP 128 (shorter WEP algorithm for a hacker to duplicate), but WEP 64 may be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. The existing 802.11 standard 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.

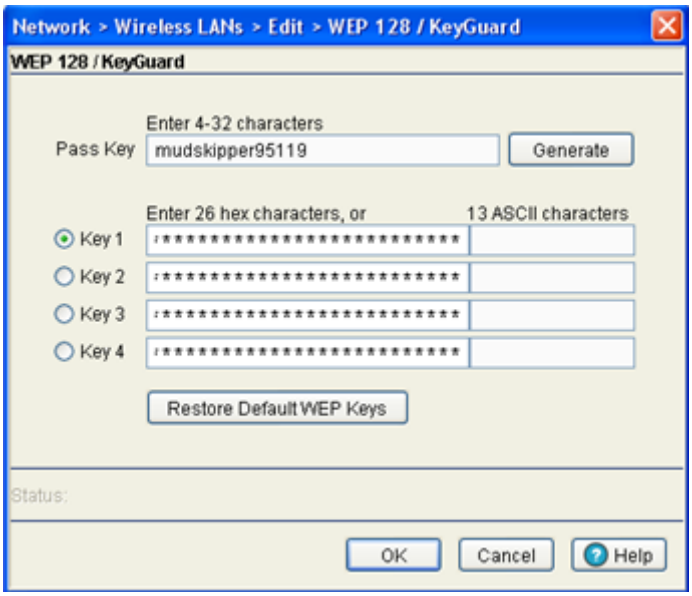
KeyGuard is a proprietary encryption method developed by Motorola Technologies. KeyGuard is Motorola's enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

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 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.

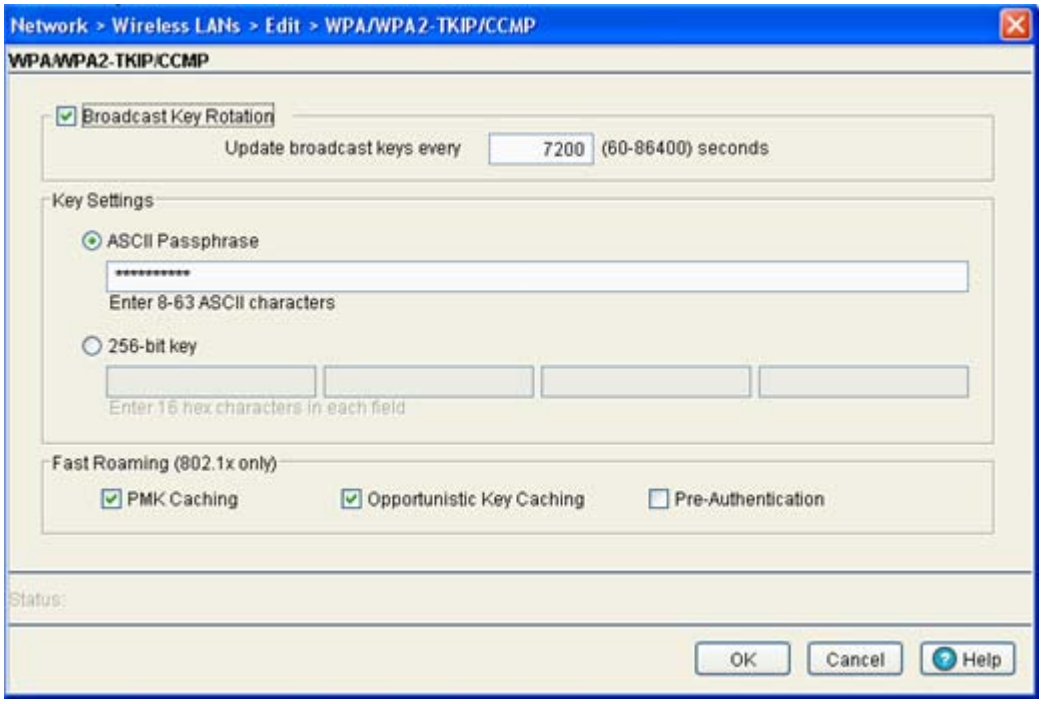
WPA2-CCMP is based on the concept of a *Robust Security Network* (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. 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 the broadcasting of encryption-key changes to MUs.

   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 time interval (at least 60 seconds) for tighter security on the WLAN's wireless connections. Set key broadcasts to a longer time interval (at most, 86400 seconds) to extend the key times for wireless connections. 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.

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 create a shared key between a client device and its authenticator. When a client roams between devices, the clients credentials no longer must be 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 do 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. The switch caches the keying information of the client until it roams to the other switch. This enables the roaming client to send and receive data sooner by not having to conduct an802.1x 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.

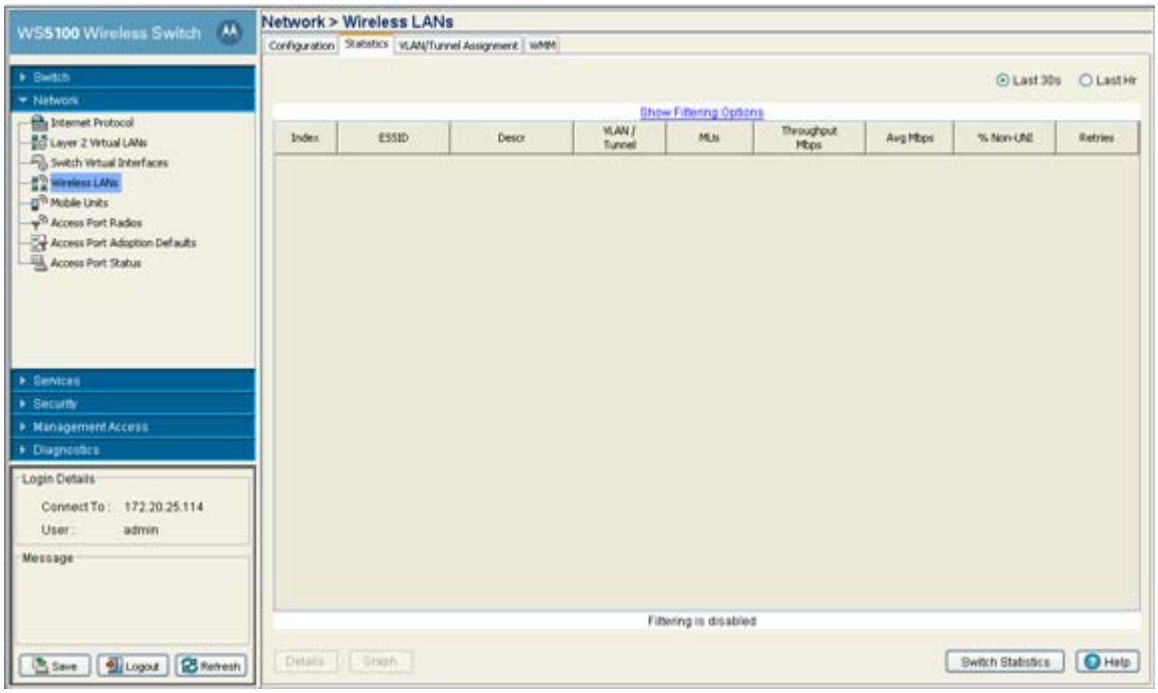
4.5.2 Viewing WLAN Statistics

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.
Last Hr	Click the Last Hr radio button to displays statistics for the WLAN over the last 1 hour.
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.
Descr	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/Tunnel	The VLAN parameter displays the name of the VLAN or tunnel 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 4-47*.

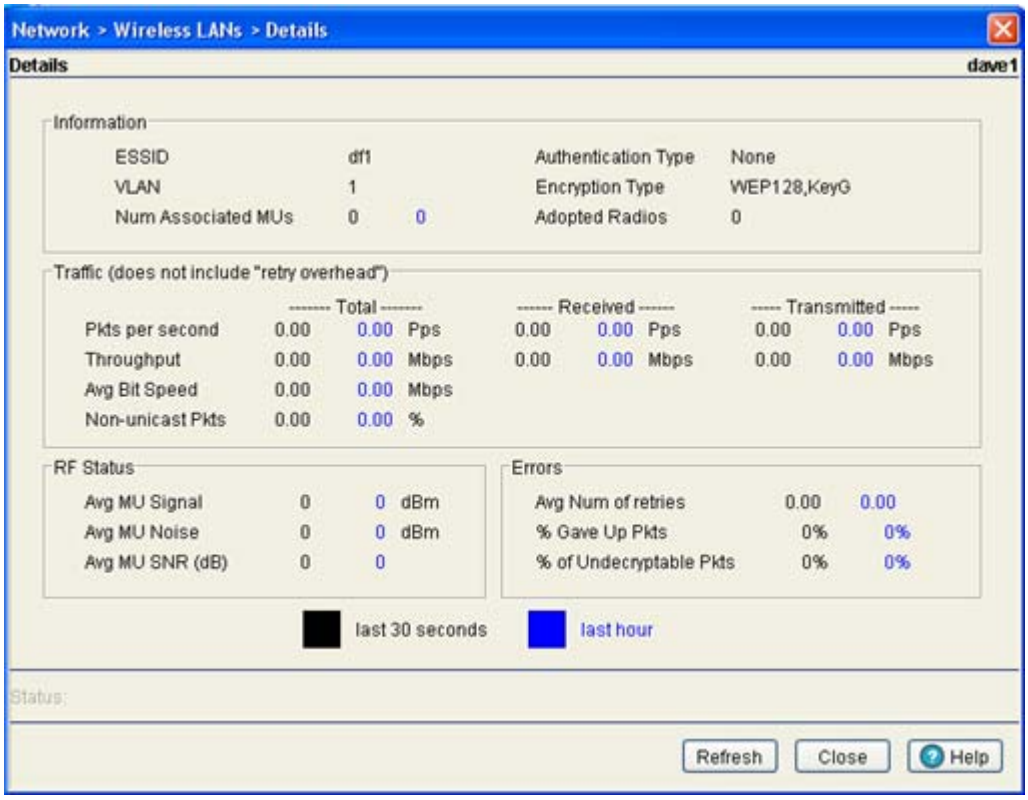
5. To view WLAN statistics in a graphical format, select a WLAN and click the **Graph** button. For more information, see *Viewing WLAN Statistics in a Graphical Format on page 4-49*.
6. To view WLAN packet data rates and retry counts, select a WLAN and click the **Switch Statistics** button. For more information, see *Viewing WLAN Switch Statistics on page 4-51*.

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 individual WLAN information, WLAN traffic throughout information and RF Status and Error information. Use this information to discern if WLAN's require 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. v



4. 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.

5. Refer to the 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 Stations	Displays the total number of MUs currently associated with the selected WLAN.
Authentication Type	Displays the authentication method active on the selected WLAN.
Encryption Type	Displays the method of encryption type active on the selected WLAN.
Adopted Radios	Displays the radios adopted by the selected WLAN.

6. 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 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.

7. 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.

8. 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.

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.

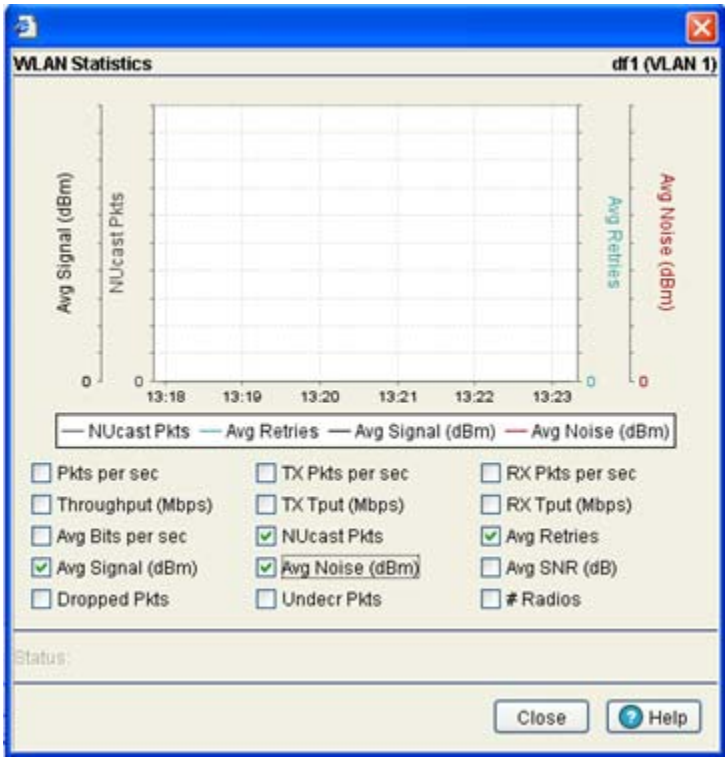
4.5.2.2 Viewing WLAN Statistics in a Graphical Format

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.

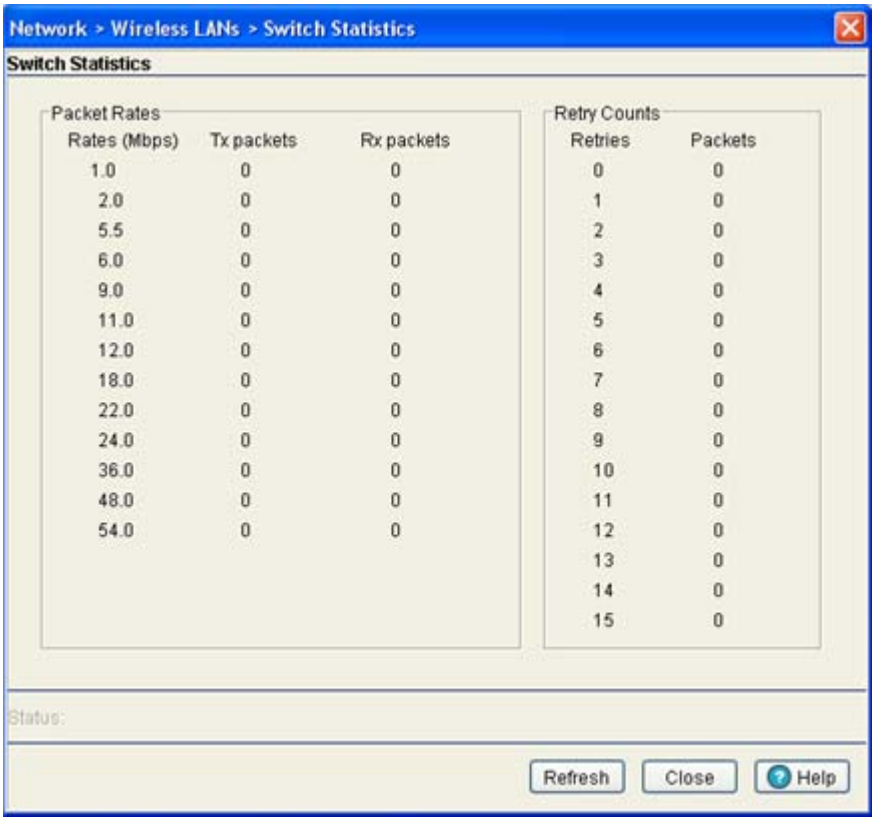
3. Select any of the above listed parameters by clicking on the checkbox associated with it.
4. Click the **Close** button to exit the screen.

4.5.2.3 Viewing WLAN Switch Statistics

The **Switch Statistics** screen is recommended for displaying individual WLAN packet data rate and retry information. Therefore, the Switch Statistics screen is optimal for determining whether the data traffic within each WLAN meets its intended throughput speed based on the WLAN's MU traffic requirements. Use this information to discern if WLAN's require modification to meet network throughput 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 **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 a recommended utility 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.

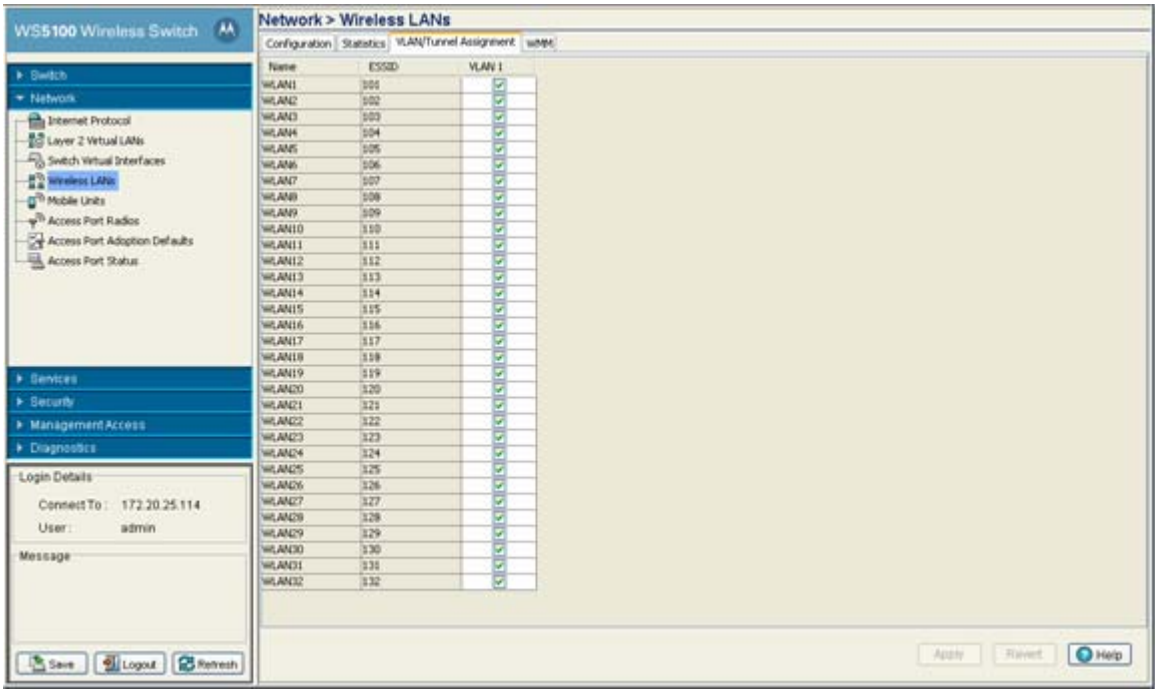
4.5.3 Viewing VLAN/Tunnel Assignments

The VLAN/Tunnel Assignment screen displays current SSID to VLAN assignments. If necessary, use the checkboxes within the screen to associate (or un-associate) existing SSIDs with the VLANs listed. Each configured VLAN is available within the screen and (if necessary) can be mapped to WLAN to ensure mission critical WLANs have an available VLAN interface.

NOTE: Mapping multiple WLANs, on the same VLAN, with different security settings to a single BSS poses a security risk to the system.

To view existing VLAN Assignments:

1. Select **Network** > **Wireless LANs** from the main menu tree.
2. Click the **VLAN/Tunnel Assignment** tab.
3. Select a **SSID** from the table to view its VLAN assignment information.



The **VLAN/Tunnel Assignment** tab displays the following information:

Name	Displays a short description of the WLAN. This description can be added or edited using the Edit button on the Configuration tab within the WLANs page.

ESSID	Displays the Service Set ID (SSID) associated with each WLAN.
VLAN (Number)	Lists all available VLANs, and contains a checkbox that (when selected) will associate the SSID with a particular VLAN ID. At a minimum, VLAN1 is available to each WLAN. Motorola recommends mapping WLANs to as many VLANs as practical to ensure the WLAN has viable interface at all times.

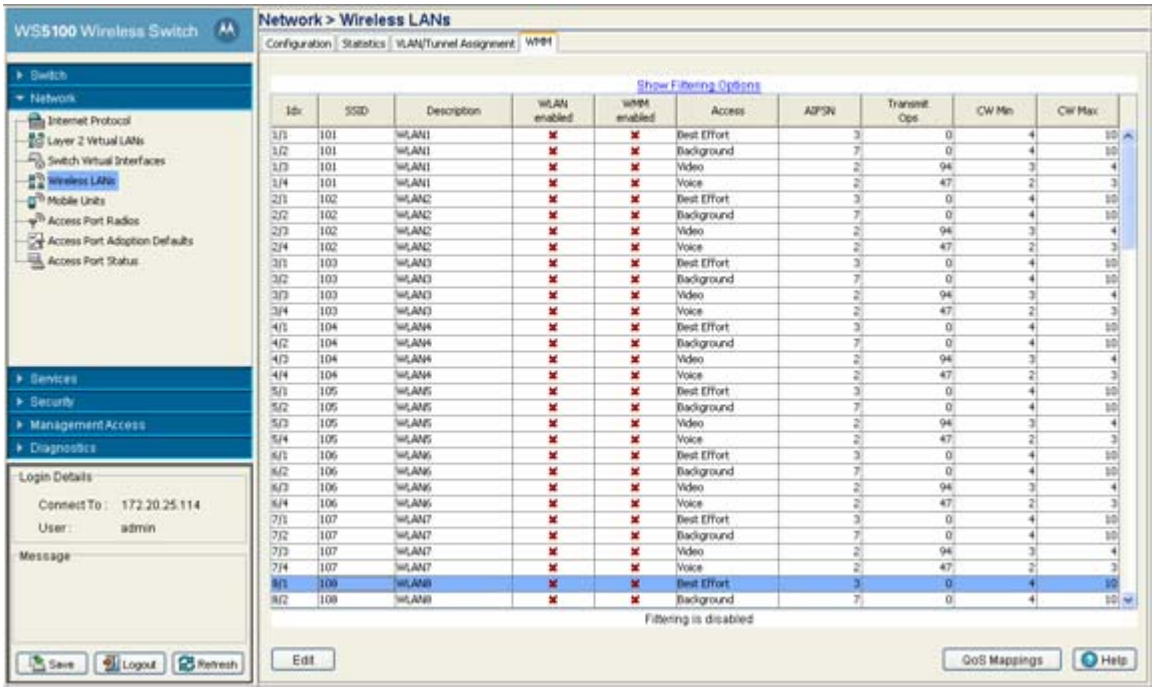
4. Click the **Apply** button to save all changes to the VLAN assignments.
5. Click the **Revert** button to undo any changes and revert back to the last saved configuration.

4.5.4 Configuring WMM

Use the **WMM screen** to review a WLAN's current index (numerical identifier), SSID, description, current enabled/disabled designation, and Access Category. AP WMM is for downstream and WLAN WMM is for upstream.

To view existing WMM Settings:

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



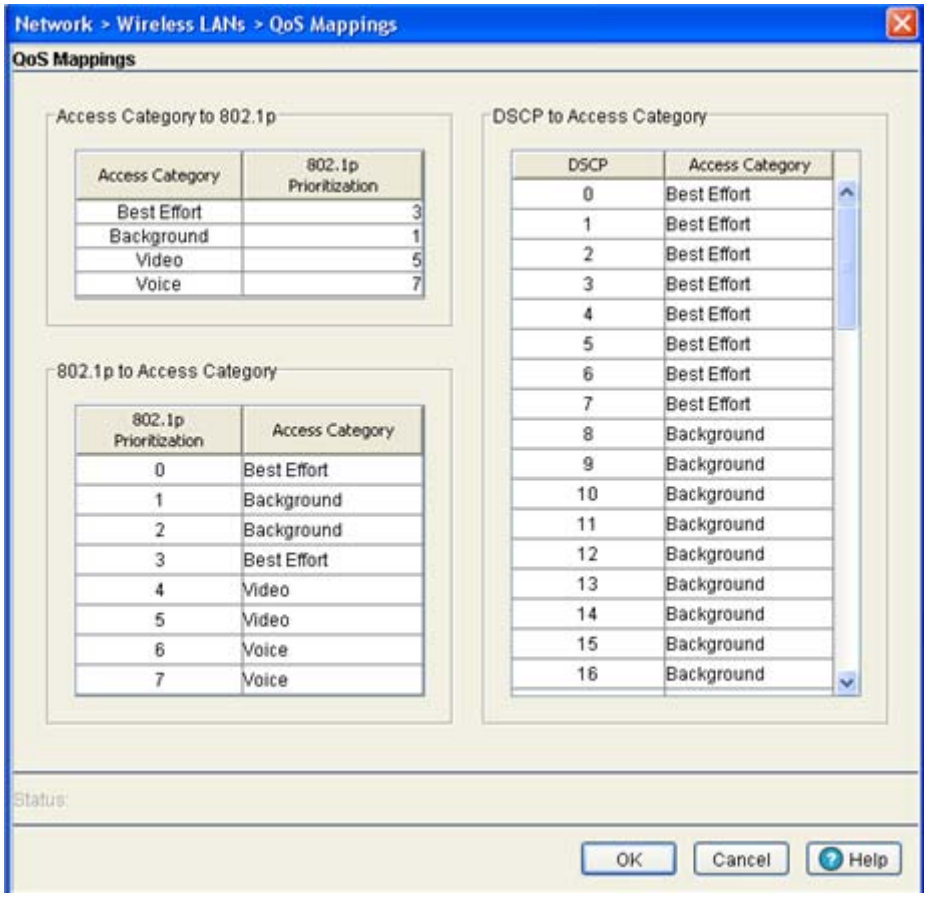
The **WMM** tab displays the following information:

Idx	Displays the WLANs numerical identifier. The WLAN index range is from 1 to 32. 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. 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 • 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 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.
CW Min	The CW Min is combined with the CW 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.
CW Max	The CW Max is combined with the CW 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.

3. Click the **Edit** button to display a screen used to modify the WMM parameters. For more information, see *Editing WMM Settings on page 4-56*.

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 as required for each access category to better 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.

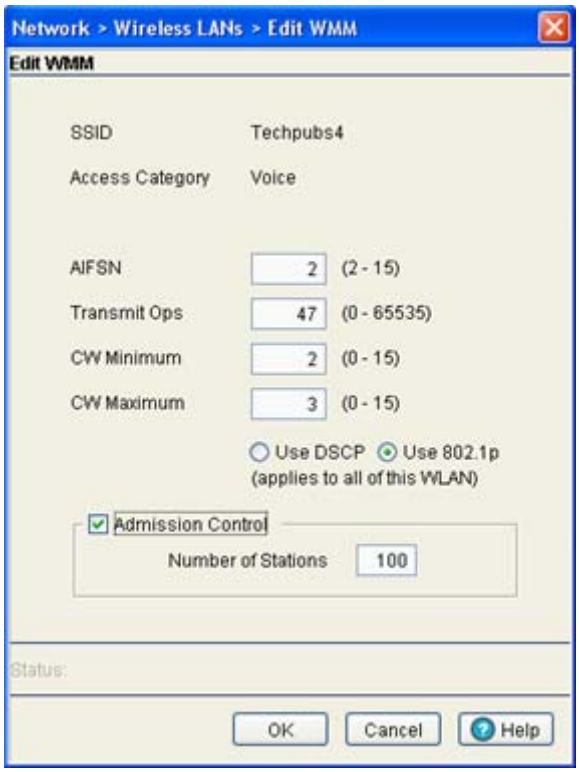
Differentiated Services Code Point (DSCP) is a field in an IP packet that enables different levels of service to be assigned to network traffic. This is achieved by marking each packet on the network with a DSCP code and appropriating to it the corresponding level of service or priority. QoS enabled programs request a specific service type for a traffic flow through the generic QoS (GQoS) application programming interface (API).

4.5.4.1 Editing WMM Settings

Use the WMM Edit screen to modify the existing Access Category settings for the WLAN selected within the WMM screen. This could be necessary in instances when the data traffic has changed and high-priority traffic (video and voice) must be accounted for by modifying the AIFSN Transmit Ops and CW values accordingly. WMM is for downstream and WLAN WMM is for upstream.

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
- Voice: Optimized for voice traffic

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 higher.
CW Minimum	The CW Minimum is combined with the CW 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.
CW Maximum	The CW Maximum is combined with the CW 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
Use DSCP or 802.1p	Select the DSCP or 802.1p radio buttons to choose between DSCP and 802.1p.

5. Select the **Admission Control** checkbox (enabled for only Voice and Video access categories) to define (limit) the number of MUs permitted to interoperate within this multimedia supported WLAN.

   Once selected, the maximum number of MUs allowed is 250. Limiting MU traffic in a multimedia (voice or video) supported WLAN is a good idea to maintain data rates and throughput.
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.

4.6 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*
- *Viewing MU Statistics*

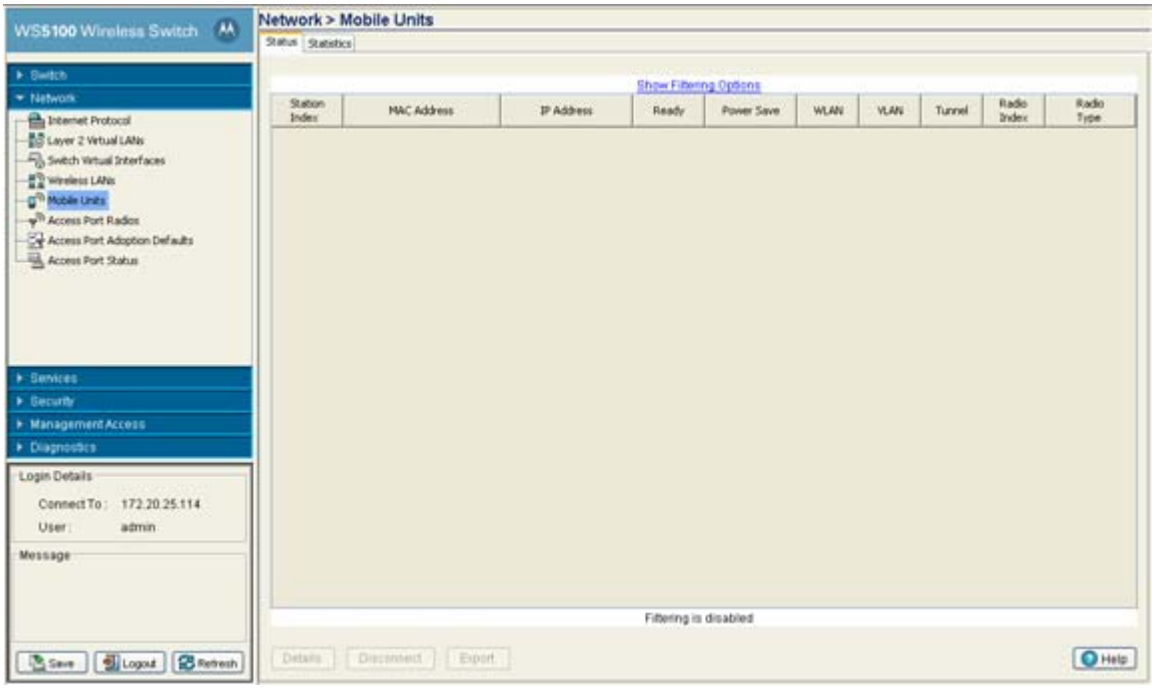
NOTE: The *Motorola RF Management Software* is a recommended utility to plan the deployment of the switch and view its configuration once operational in the field. Motorola RFMS can help optimize the positioning and configuration of a switch in respect to a WLAN's MU throughput requirements and can help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

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.
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 transmitting with the switch's access ports frequently and for periods of two hours or greater.
WLAN	Displays the name of the switch created WLAN an MU's associated AP is currently interoperating with.
VLAN	Displays the specific VLAN 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 4-59*

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.

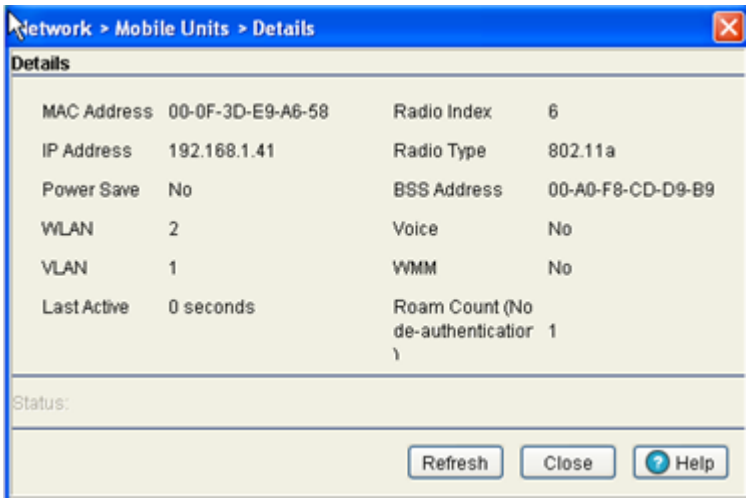
5. Click the **Export** button to export the content of the table to a *Comma Separated Values* file (CSV).

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 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 those 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.
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 and 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 it is 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 Viewing MU Statistics

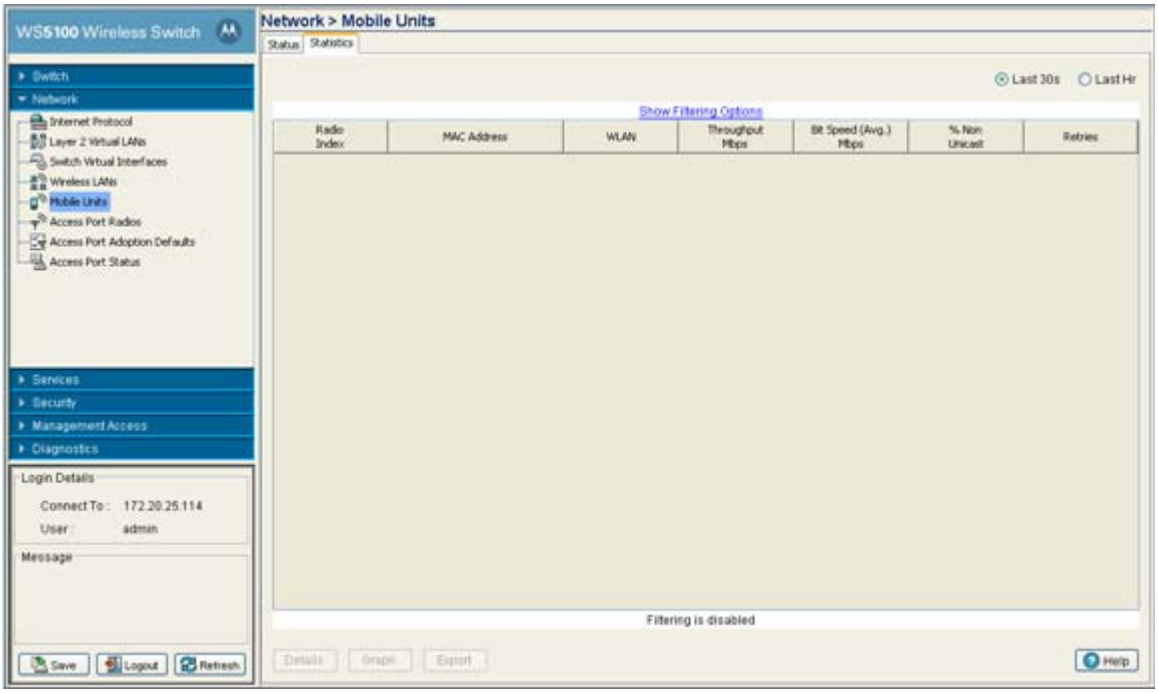
The **Statistics** screen displays read-only statistics for each MU. Use this information to assess if configuration changes are required to improve network performance. If a more detailed set of MU statistics is required, select a MU from the table and click the **Details** button.

NOTE: Each switch can support a maximum of 4096 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 as gathered over the last 30 seconds.
4. Select the **Last HR** checkbox to display MU statistics as gathered over the last hour.
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.
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 coverage area of the MU.
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.

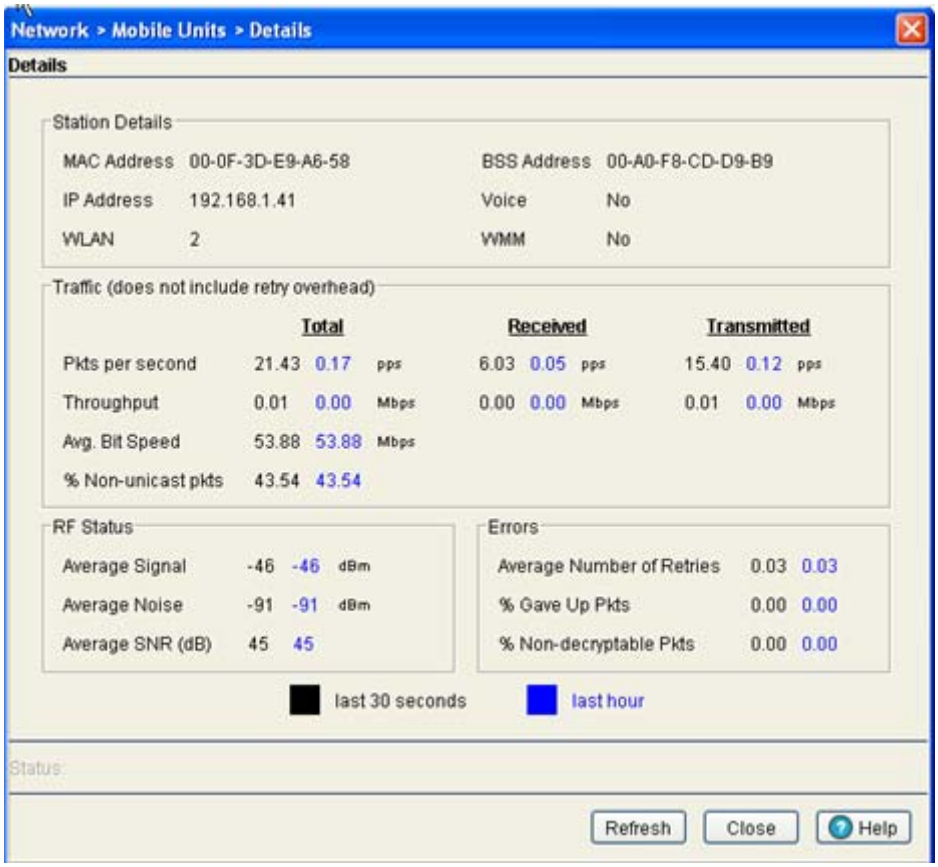
6. Click the **Details** button to launch a screen with additional information about the selected MU. For more information, see *Viewing MU Statistics in Detail on page 4-62*.

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 4-64*.
8. Click the **Export** button to export the content of the table to a *Comma Separated Values* file (CSV).

4.6.2.1 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.

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 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 the operation of the switch.

5. Refer to the **Traffic** field for the following information:

Pkts per second	Displays the average total packets per second received by the selected MU. The Rx column displays the average total packets per second received on the selected MU. The Tx column displays the average total packets per second sent on the selected MU.
Throughput	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.
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 selected 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 your 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.

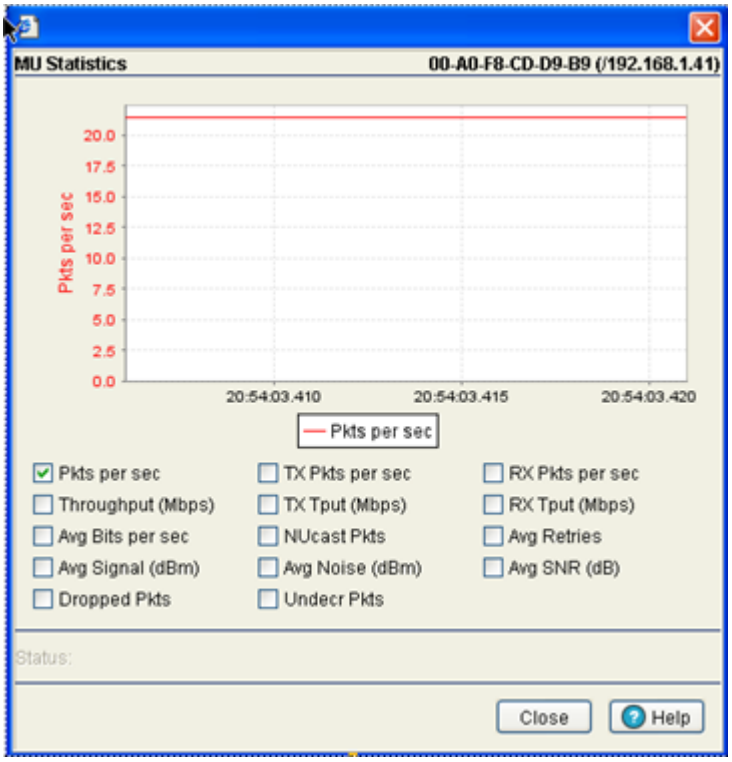
8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

4.6.2.2 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 performance 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. Choose as many of the values displayed to chart that behavior graphically within the graph. However, 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.

4.7 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: Each switch can support a maximum of 48 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 in the field. 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:

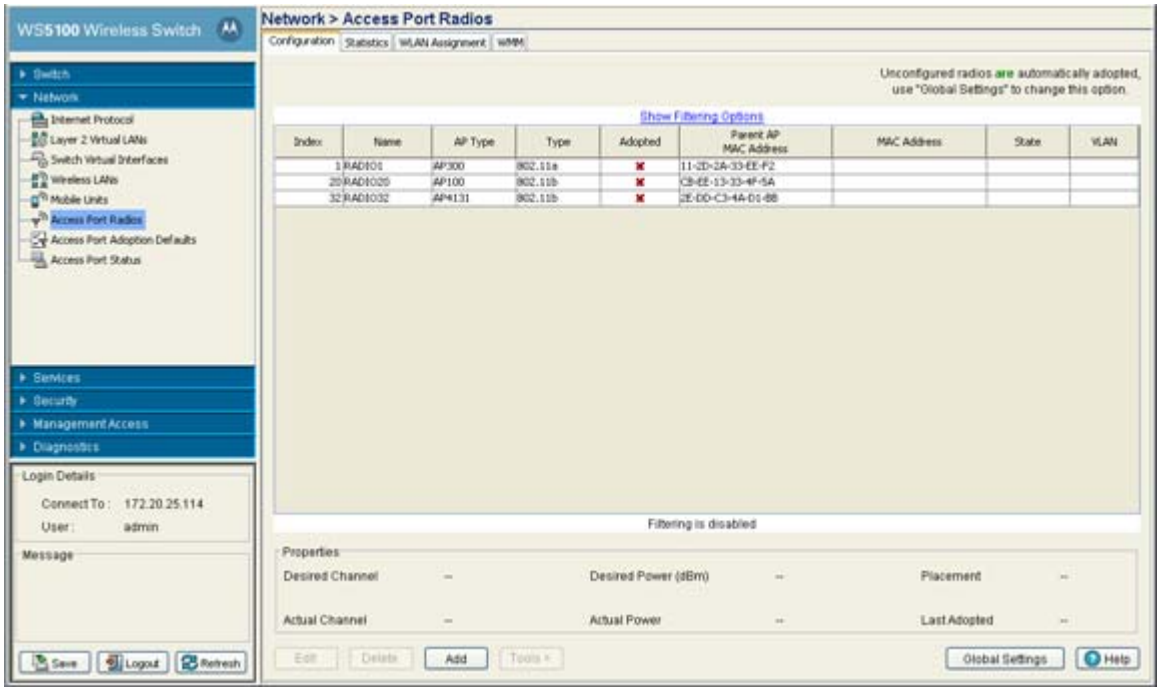
- *Configuring Access Port Radios*
- *Viewing AP Statistics*
- *Configuring WLAN Assignment*
- *Configuring WMM*

4.7.1 Configuring Access Port Radios

Refer to the **Configuration** tab to view current radio configurations. After reviewing the radios listed, you have the option of editing the properties of an existing radio, deleting a radio, adding a new radio, resetting a radio, scan available channels or exporting a radio.

To view WLAN 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.
Name	Displays a user assigned name for the radio.

AP Type	Displays whether the AP is an AP100 or AP300 model Motorola access port or an AP-4131 model access point, if configured to operate as an access port.
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 current operational mode that the Radio is set for. If the radio is set as a Detector AP the state will display "Detector", otherwise the state will read "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 makes the channel designation.
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.
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.
Last Adopted	Displays the time this radio was last adopted by the switch.

5. Click the **Edit** button to launch a screen used to configure radio specific parameters.
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.
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).

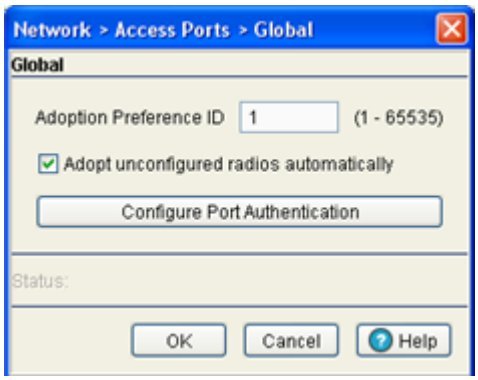
10. Click the **Global Settings** button to display a screen with settings applying to all radios on the system. For more information, see *Configuring an AP's Global Settings on page 4-67*.

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 to 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 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 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.

   Setting the preference ID to a 0 value essentially means you "do not care" what the value is and the switch will automatically assign a preference ID.

   The adoption preference ID is used for AP load-balancing. A switch preferentially adopt APs which have the same adoption-preference-id as the switch itself. 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 4-88.

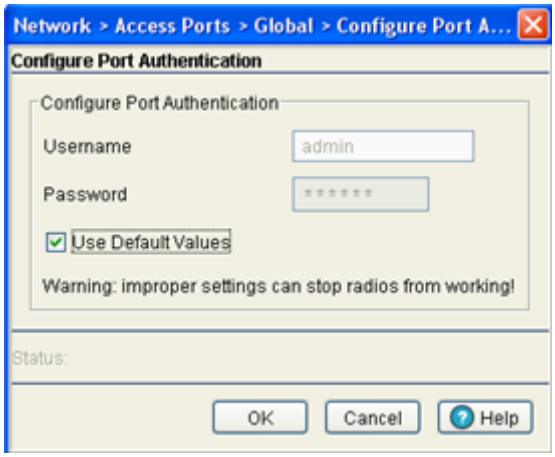
5. To enable automatic adoption of non-configured radios on the network, check the box marked **Adopt unconfigured radios automatically**. Default radio settings are applied to access ports when they are automatically adopted. Enable this option to allow the adoption of access ports even when they are not configured. Default radio settings are applied to access ports adopted automatically.
6. Click the **Configure Port Authentication** button to open a new dialogue with port authentication configuration information.

7. 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.
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: The 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 will not automatically receive the username and password.

NOTE: After setting the username and password to factory default settings, the system must be rebooted before the factory default settings will take effect.

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

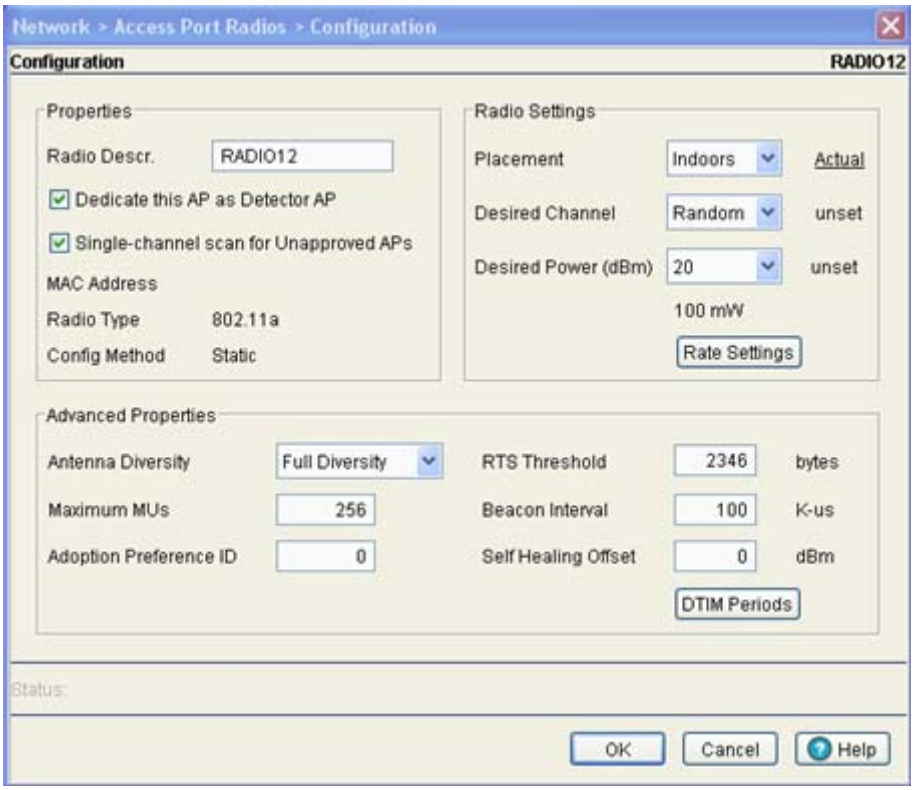
The **Edit** screen provides a means of modifying the properties of an existing radio. This is often necessary when the radio's intended function has changed and its name needs modification or if the radio now needs to be defined as a detector radio. The Edit screen also enables you to modify placement, 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 display of the screen 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. In the **Radio Descr.** field, enter a brief description to identify the radio. The Radio Description is used to differentiate multiple radios of the same type and can be used to locate a radio if there are any problems.
6. Select the **Dedicate this Radio as Detector 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.
7. Select the **Single-channel scan for Rogue APs** checkbox to enable the switch to scan for rogue devices using the switch's current channel of operation.

8. 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.

9. 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.

10. 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 displays in mW.

11. 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 4-72*.

12. 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 make the radios 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 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

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.

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 access port uses an external antenna. For additional information on determining the offset value, see the documentation shipped with the access port.
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 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 10 beacons for BSS 1-4.

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

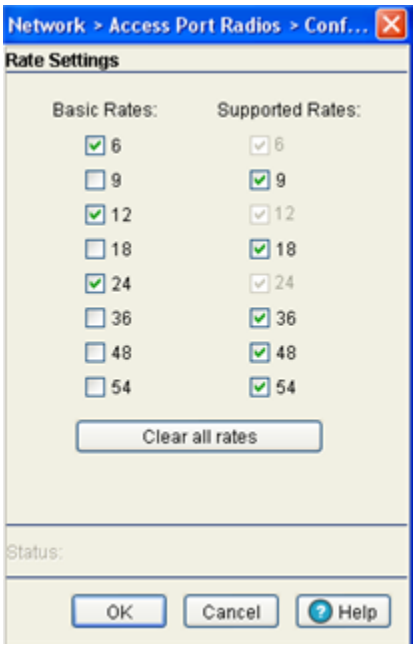
Configuring Rate Settings

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 default rates available to an 802.11b radio, 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.

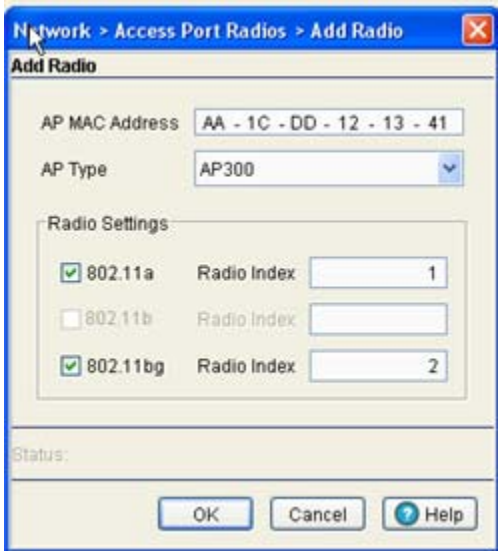
4.7.1.3 Adding APs

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 **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 model access point, its access port conversion will render the access point a "thin" access port.
6. Select the radio type checkboxes corresponding to the type of AP radio used.
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. 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.

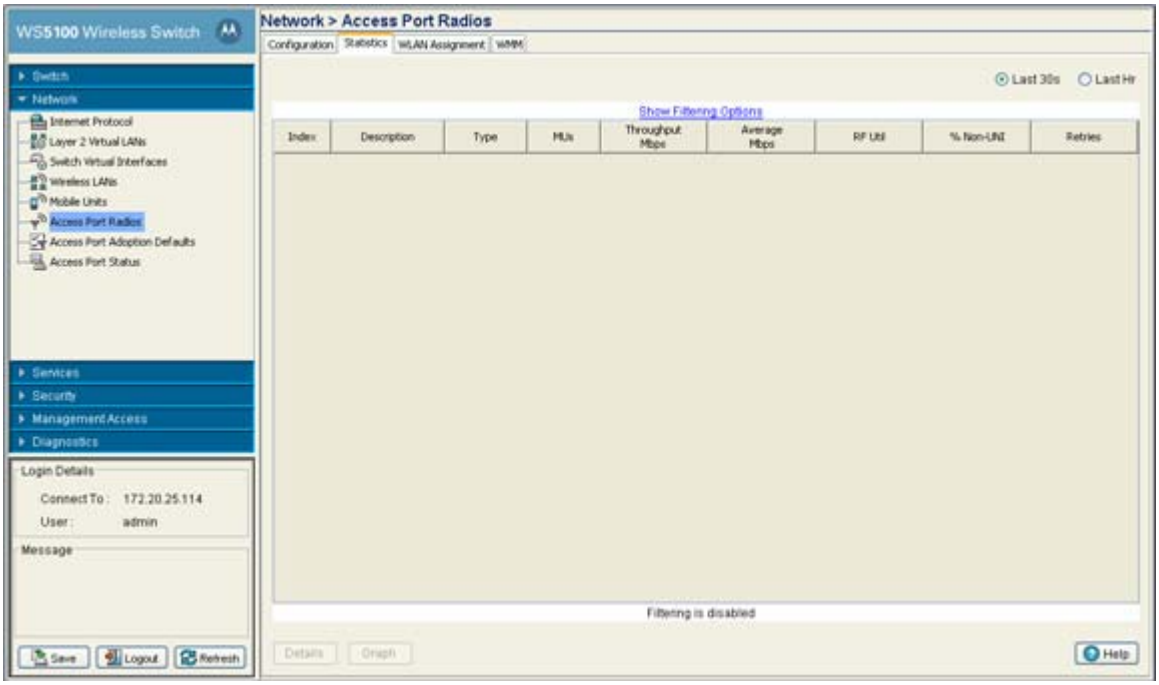
4.7.2 Viewing AP Statistics

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	The Type value 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.
Average Mbps	Displays the average bit speed in Mbps on the selected access port. This value includes all packets that are 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 the total 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 4-76*.
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 4-76*.

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 sections: **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.
AP Type	Displays the access port model.
Current Channel	The 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.

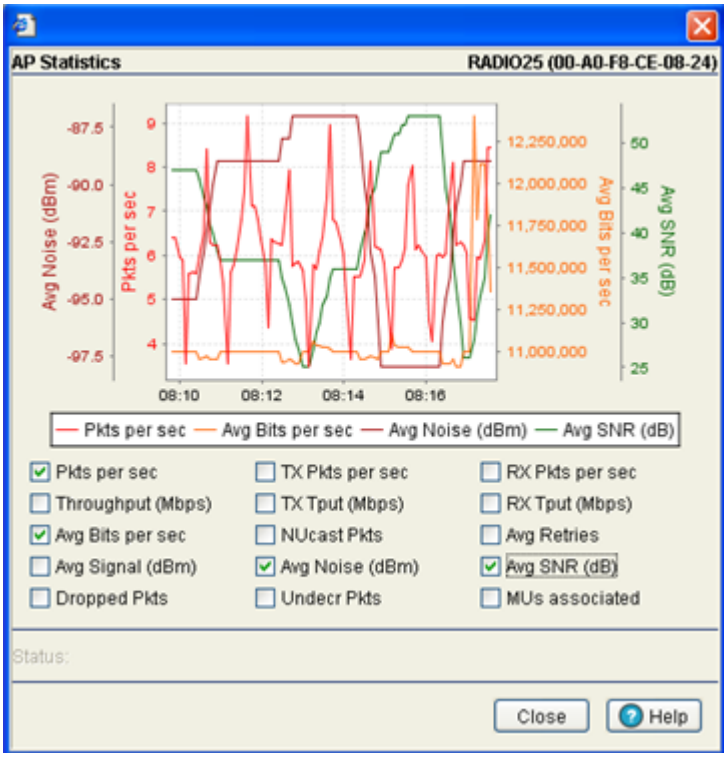
4.7.2.2 Viewing AP Statistics in Graphical Format

The Access Port Radios Statistics tab has an option for displaying detailed access port radio statistics in a graphical format. This information can be used to chart associated switch radio performance and help is diagnosing 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. Choose as many of the values displayed to chart that behavior graphically within the graph. However, 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.

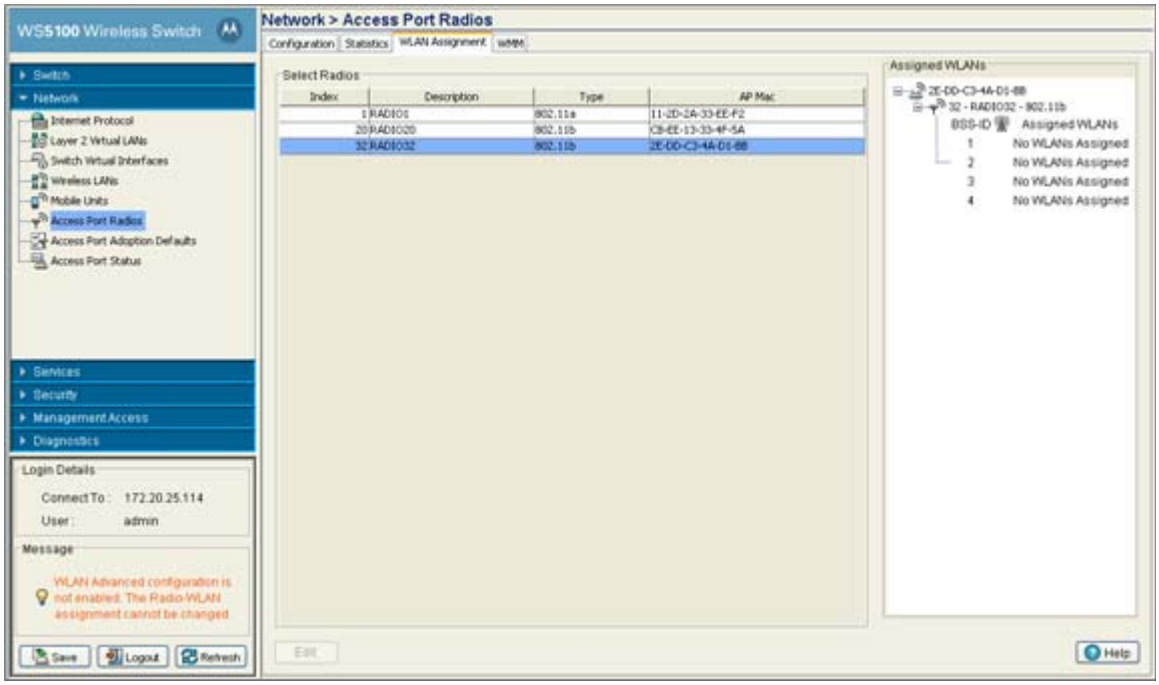
4.7.3 Configuring WLAN Assignment

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. Use the Filter Options facility (by clicking the Show Filter Options link) to specify if information is filtered by Index (default setting), Description, Type or AP MAC. Select **Turn Filtering Off** to disable filtering.

4. 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**.

5. 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** section displays the WLANs associated to each of the BSSIDs used by the radios within the radio table. There can be 0 – 16 WLANs associated with each BSS. Out of these, one WLAN must be the primary WLAN.

6. 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 4-79*.
7. 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 sections displays the WLANs associated to each of the BSSIDs used by the radios within the radio table. The Select/Change Assigned WLANs section can be used 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.

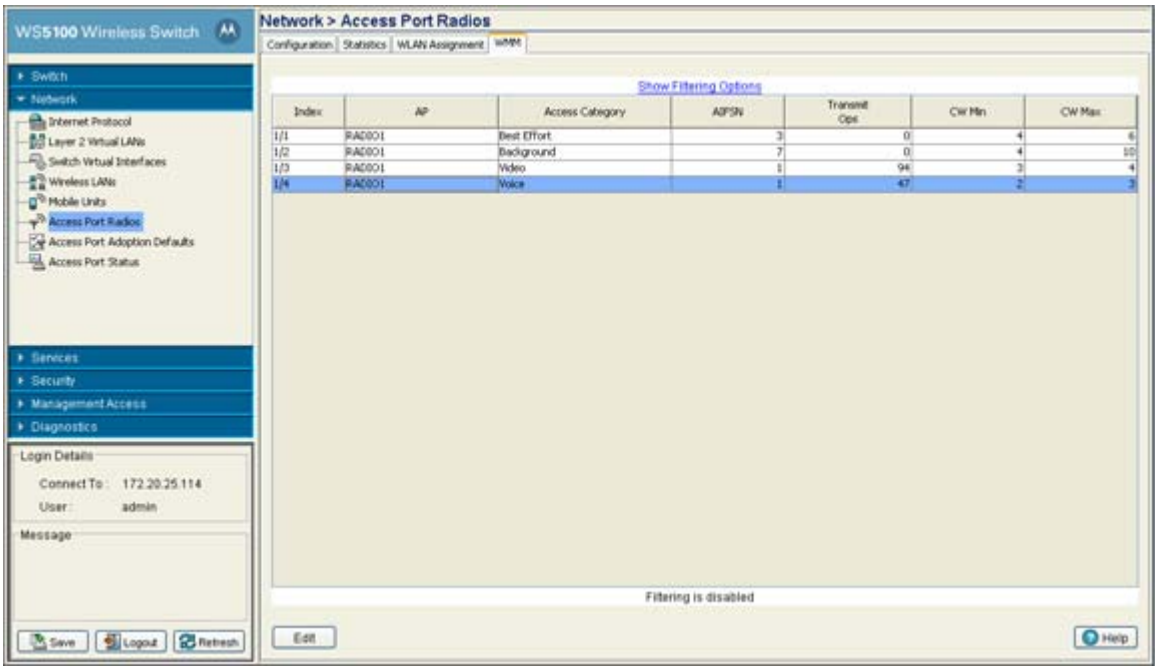
4.7.4 Configuring WMM

Use the **WMM** tab to review each radio's current index (numerical identifier) the Access Category that defines which data type (Video, Voice, Best Effort and Background) the radio has been configured to process 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 WLAN 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. For Higher-priority traffic categories, this value should be set higher.
CW Min	Displays the CW 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.
CW Max	Displays the CW 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.

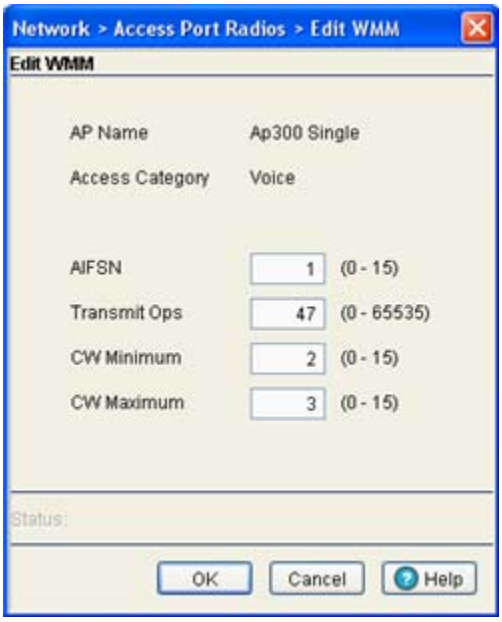
3. Select a radio and click the **Edit** button to modify its properties. For more information, see *Editing WMM Settings on page 4-81*.

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.

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 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.

4.8 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 4-88*.

- *Configuring AP Adoption Defaults*
- *Configuring Layer 3 Access Port Adoption*
- *Configuring WLAN Assignment*
- *Configuring WMM*

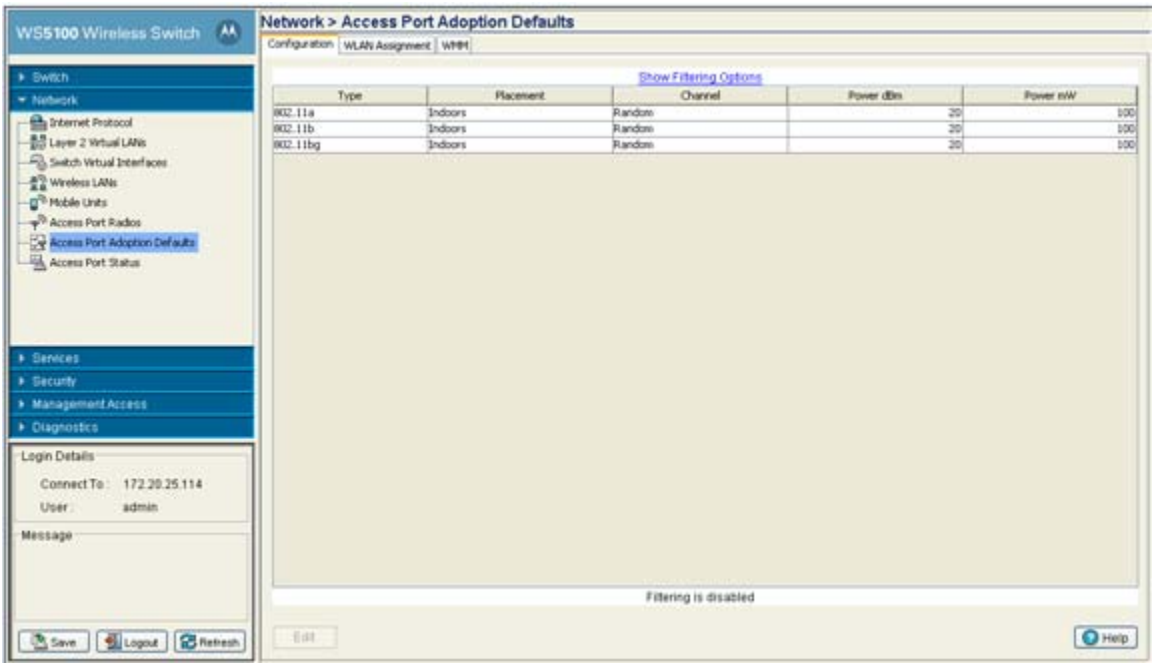
4.8.1 Configuring AP Adoption Defaults

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 Radio Adoption Settings on page 4-84*.

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:

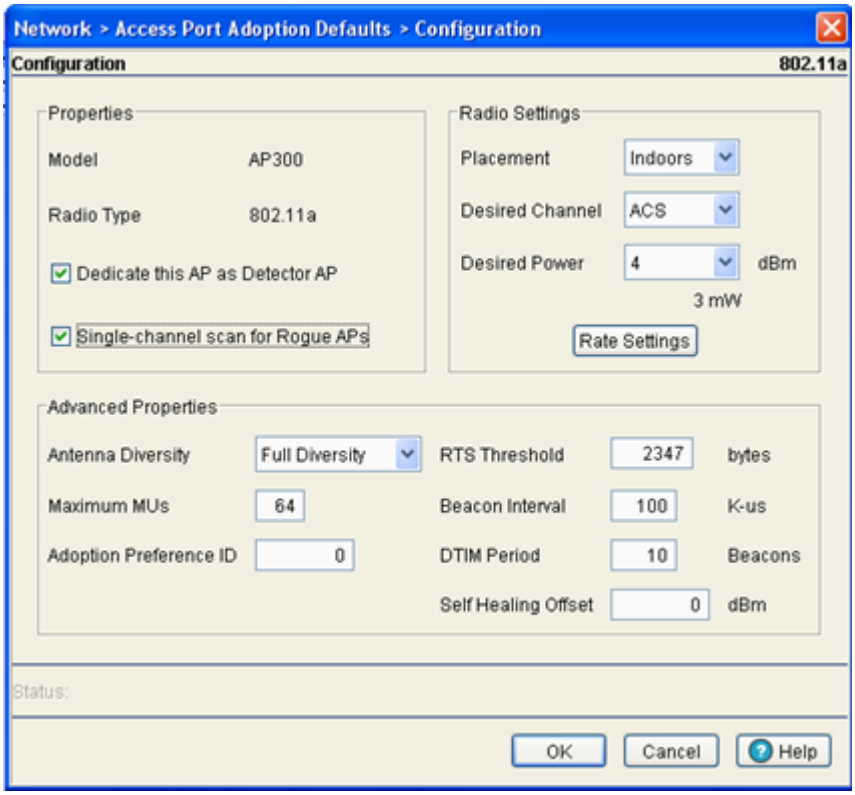
- Configure DHCP option 189 to specify each switch IP address.
- Configure a DNS Server to resolve an existing name into the IP of the switch. The access port has to get DNS server information as part of its DHCP information. The default DNS name requested by an AP300 is "Symbol-CAPWAP-Address". However, 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 Radio 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** > **Radio 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 Radio as Detector.** 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 Rogue APs** checkbox to enable the switch to detect rogue devices using its only its current channel of operation.
7. 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.

8. 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.

9. 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.

10. 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 4-72*.

11. 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 64.
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.

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 i, 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.

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 **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.

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

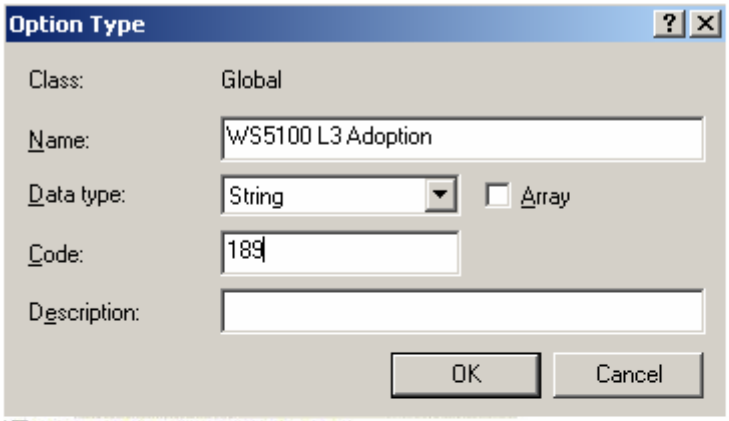
The configuration activity required for adopting access ports in a layer 3 environment is unique. In a layer 3 environment, switch discovery is attempted in the following ways:

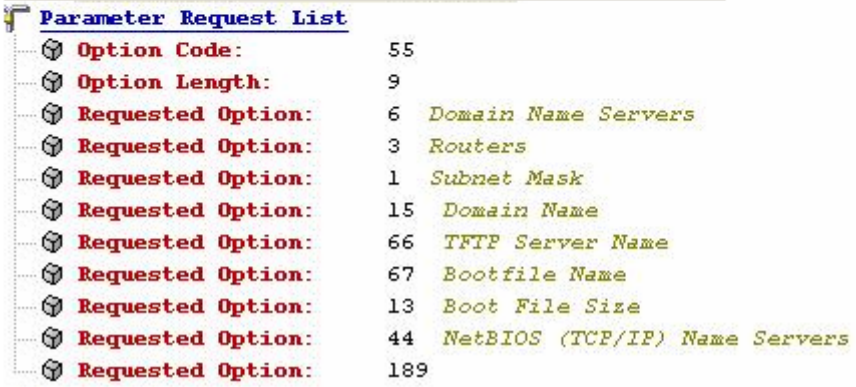
- On the local VLAN
- Through the DHCP Server

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.

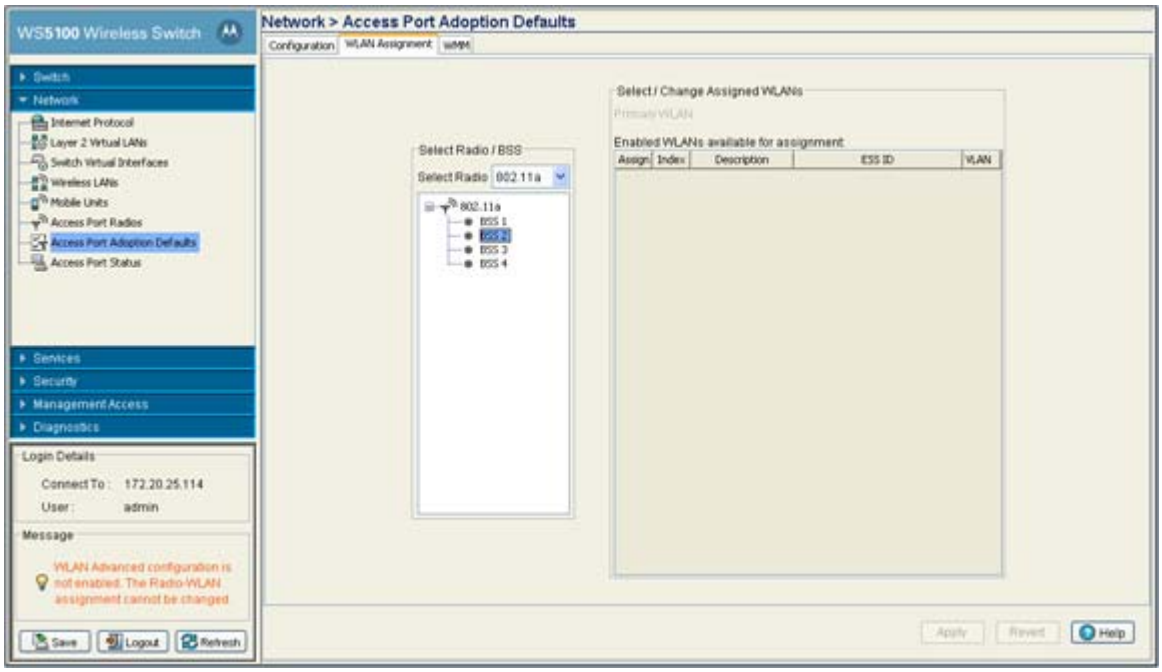
4.8.3 Configuring WLAN Assignment

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 t**ab.



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 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 mean of identifying particular WLANs after they have been assigned to different radio BSSIDs. A BSSID cannot support two WLANs with the same numerical index value.
Description	Use the WLAN Description (along with the WLANs index) as a means of identifying particular WLANs after they have been 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	Displays the VLAN ID of VLANs assigned to WLANs. By default, all WLANs are assigned to VLAN 1.

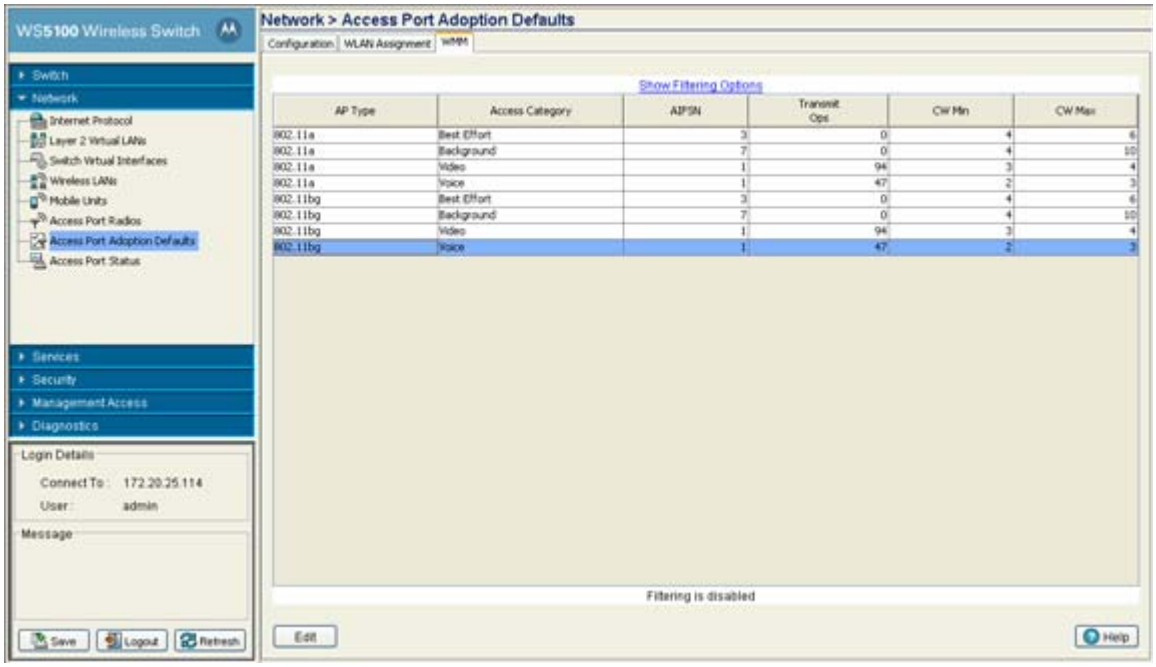
6. Click **Apply** to save the changes made within the screen.
7. Click **Revert** to cancel the changes made and revert back to the last saved configuration.

4.8.4 Configuring WMM

Use the **WMM** tab to review each radio type, as well as the Access Category that defines which data type (Video, Voice, Best Effort and Background) the radio has been configured to process. Additionally, the WMM screen displays the transmit intervals defined for the target access category. Radio WMM parameters are for downstream while WLAN WMM parameters are for upstream

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. 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. For Higher-priority traffic categories, this value should be set higher.

CW Min	The CW Min is combined with the CW 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.
CW Max	The CW Max is combined with the CW 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.

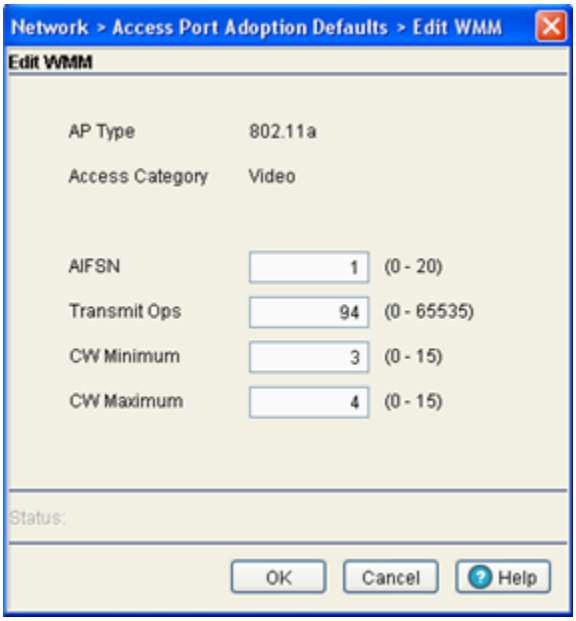
4. To modify the properties of WMM Adoption Settings, select a radio and click the Edit button. For more information, see *Editing Access Port Adoption WMM Settings on page 4-91*.

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 to be adjusted to compensate for larger data packets and contention windows.

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 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 **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 Viewing Access Port Status

Use the **Access Port Status** screen to view device hardware address and software version information for adopted and unadopted access ports. The Access Port Status screen has the following tabs:

- *Viewing Adopted Access Ports*
- *Viewing Unadopted Access Ports*

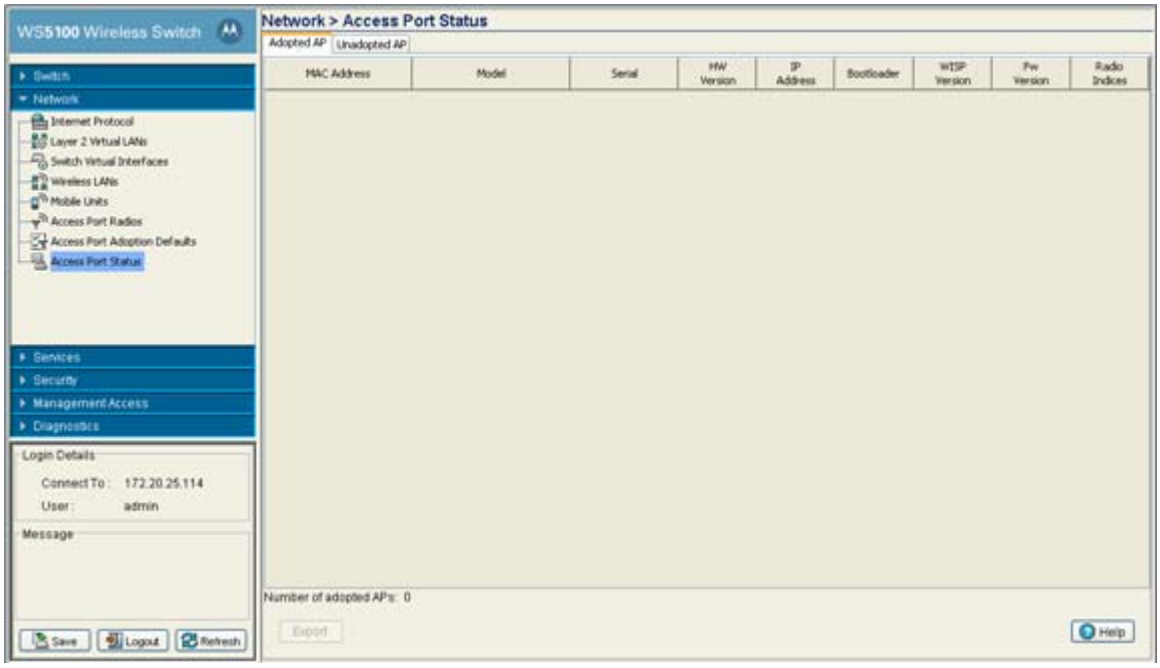
4.9.1 Viewing Adopted Access Ports

Use the **Adopted AP** tab for gathering device hardware address and software version information for the access port.

To view existing Radio Configuration information:

1. Select **Network** > **Access Port Status** from the main menu tree.

2. Click the **Adopted AP** tab.



3. Refer to the **Adopted AP** screen for the following information:

MAC Address	Displays the radio's first MAC address when it is adopted by the switch.
Model	Displays s the Model Number of the access port.
Serial	Displays the serial number of the access port, and is used for management purposes by the switch. 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	The Bootloader value displays the software version the access port boots from. This information can be helpful when troubleshooting problems.
WISP 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 firmware version on the access port 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.

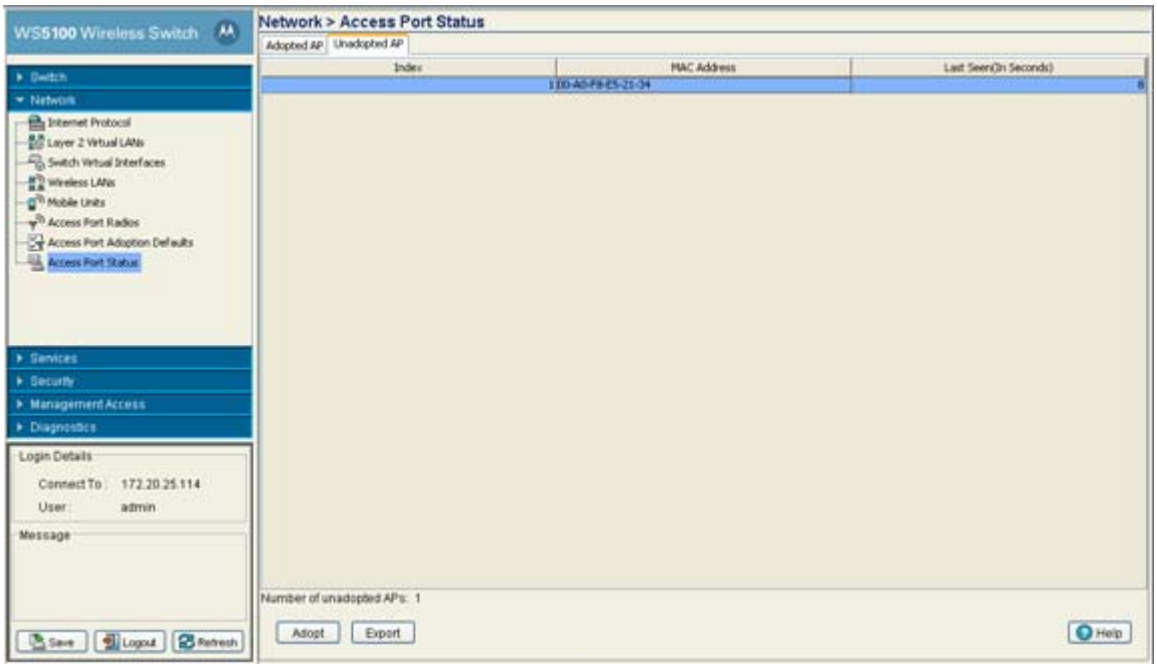
4. Click the **Export** button to export the contents of the table to a Comma Separated Values file (CSV).

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 Status** from the main menu tree.
2. Click the **Unadopted AP** tab.



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.

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).

5

Switch Services

This chapter describes the following Services main menu information used to configure the switch.

- *Displaying the Services Interface*
- *DHCP Server Settings*
- *Configuring Secure NTP*
- *Configuring Switch Redundancy*
- *Layer 3 Mobility*
- *Configuring GRE Tunnels*
- *Configuring Self Healing*
- *Configuring Switch Discovery*

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

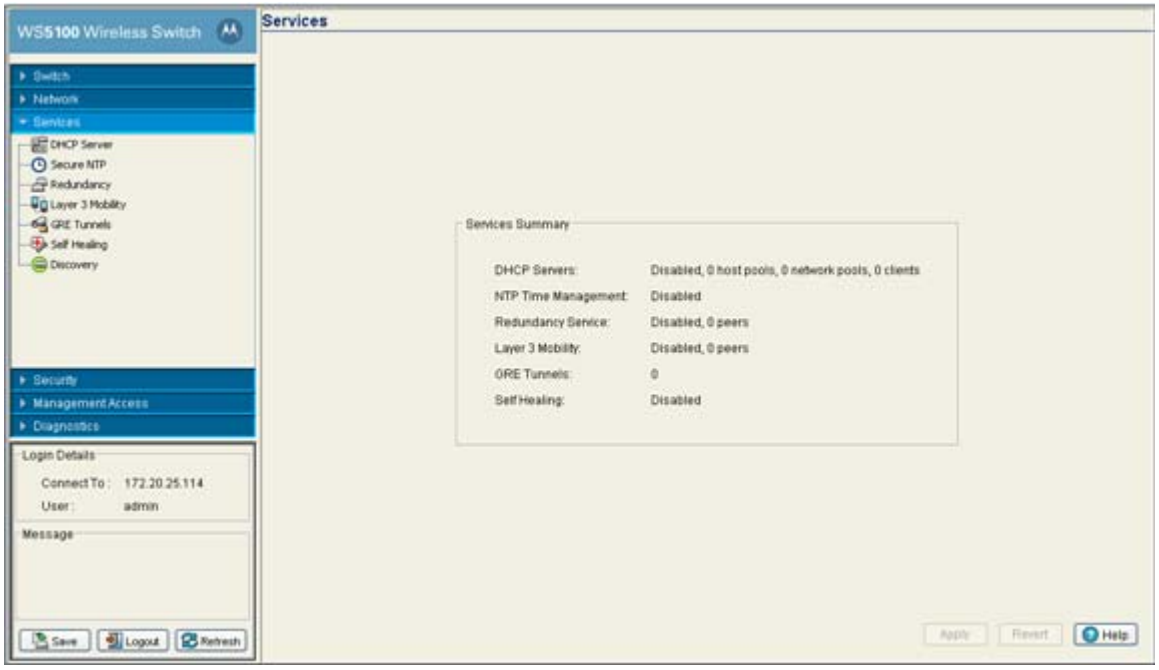
5.1 Displaying the Services Interface

Refer to the **Services** main menu interface to review a summary describing the availability of several of the 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 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 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 Servers is enabled and the current configuration. For information on configuring DHCP Server support for the switch, 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 environment. NTP is a client/server implementation.
Redundancy Service	Displays whether Redundancy is currently enabled or disabled for the switch. 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 on page 5-25*.

Layer 3 Mobility	Displays whether Layer 3 Mobility is currently enabled or disabled for the switch. 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 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 5-35*.
GRE Tunnels	Displays the number of GRE tunnels currently configured on the switch. Tunneling involves encapsulating a packet that supports one protocol within another packet, which may run on the same protocol or on a different protocol. It is generally used to support evolving networks, its capacity and security requirements. *Generic Routing Encapsulation* (GRE) is one of the many commonly used protocols for IP tunneling. For information on configuring GRE tunneling, see *Configuring GRE Tunnels on page 5-41*.
Self Healing	Displays whether Self Healing is currently enabled on the switch. 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 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. For information on configuring self healing, see *Configuring Self Healing on page 5-46*.

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 DHCP Server Relay Information*
- *Viewing DHCP Server Status*

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 the 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 amount of time chosen by the administrator. Before leases expire, the clients to which leases are assigned

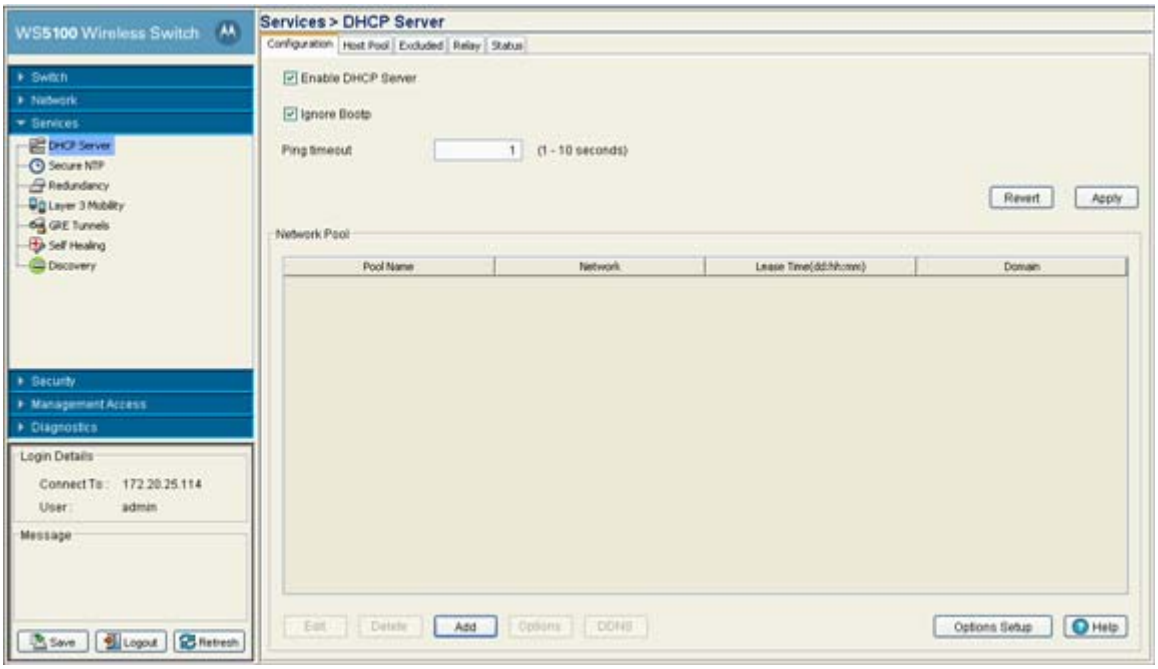
are expected to renew them to continue to use the addresses. Once a lease has expired, the client to which that lease was assigned is no longer permitted to use the leased IP address.

NOTE: DHCP Server setting updates are only implemented when the switch is restarted.

To configure DHCP:

1. Select **Services** > **DHCP Server** from the main menu tree.

   The DHCP Server screen displays with the **Configuration** tab displayed.



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 time interval** variable, the switch uses it to intermittently ping and find out if the "DHCP client" requested IP is already used in network or not.
5. Refer to the following information 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 for which addresses can be assigned. However, the relationship between pools and interfaces is implicit, not explicit as was the case with previous implementations of the switch.
Network	Displays the IP address for the clients on this interface.

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 number of seconds 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 mobile-unit 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 to the switch, 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 insert a global pool name into the list of available pools. However, individual pool options require initial setup using the **Options Setup** functionality before they can be made available for use with individual pools. 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 that can be 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 initially configure individual pool options available using the Options button. Pool options require initial configuration using the Options Setup functionality before they can be selected using the Options button.
12. Click **Apply** to save any changes to the screen. Navigating away from the screen without clicking the Apply button 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.

   The DHCP Server screen displays with the **Configuration** tab displayed.
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) 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.

- A **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.
- 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 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.

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 time interval for clients to use the DHCP server assigned addresses. The default lease time is 600 seconds, with a minimum setting of 10 seconds and a maximum value of 946080000 seconds.
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

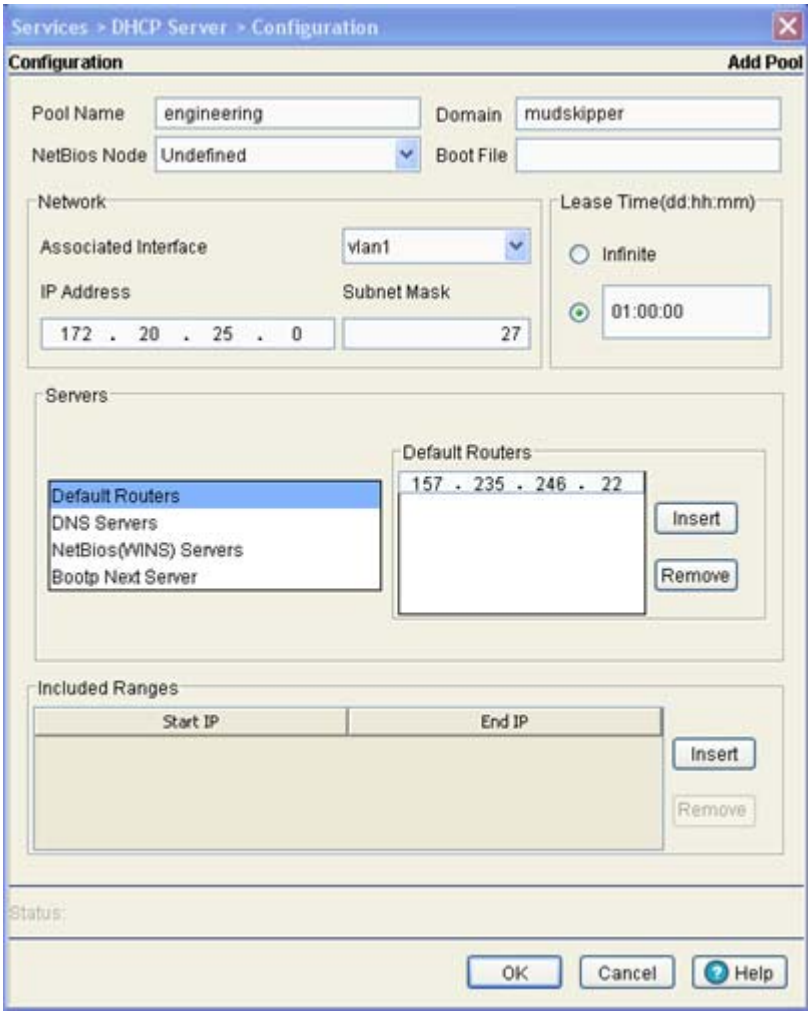
Add a new DHCP pool as needed to suit the address distribution requirements of your network.

To add a DHCP pool:

1. Select **Services** > **DHCP Server** from the main menu tree.

   The DHCP Server screen displays with the **Configuration** tab displayed.

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 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 used the assigned address indefinitely.
   - Actual Interval - Select this checkbox to manually define the time interval for clients to use the DHCP server assigned addresses. The default lease time is 600 seconds, with a minimum setting of 10 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

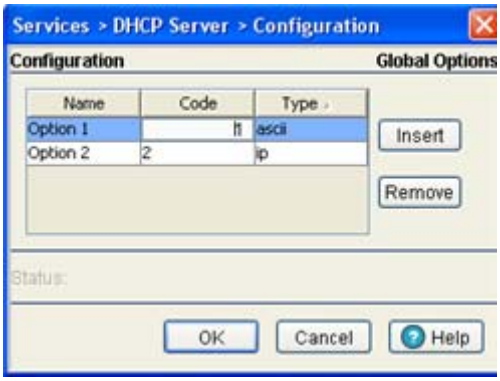
The DHCP Server screen’s Configuration and Host Pool tabs can be used to display an additional **Global Options** screen.

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.

   The DHCP Server screen displays with the **Configuration** tab displayed.

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** value 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 and Host Pool tabs can be used to display an additional **DDNS** screen. Use this screen to define a DDNS domain name and address.

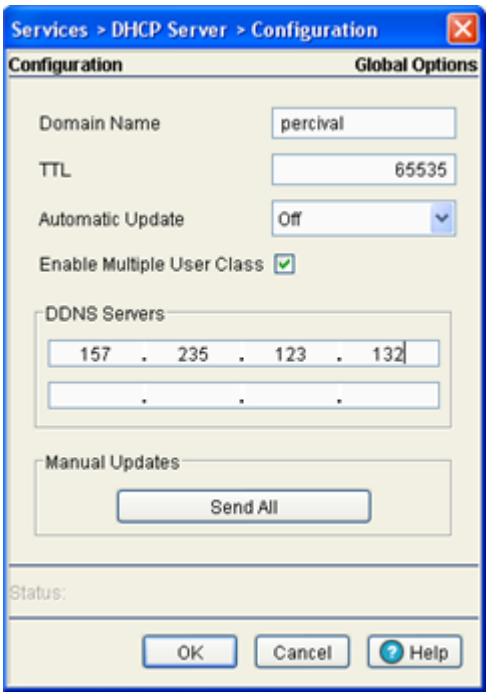
NOTE: For an additional (in depth) discussion on the DDNS setup options available to the WS5100 switch (using both the switch CLI and Web UI), refer to Chapter 7 of the *WS5100 Migration Guide* available for download from the corporate Website.

To configure a global domain name and DDNS server address:

1. Select **Services** > **DHCP Server** from the main menu tree.

   The DHCP Server screen displays with the **Configuration** tab displayed.

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 65535 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 DDNS update from DHCP server or 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 the **Send All** button (within the **Manual Updates** field) to send manual DDNS updates to all DNS servers.
9. Click **OK** to save and add the changes to the running configuration and close the dialog.
10. 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.

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

5.2.2 Viewing the Attributes of Existing Host Pools

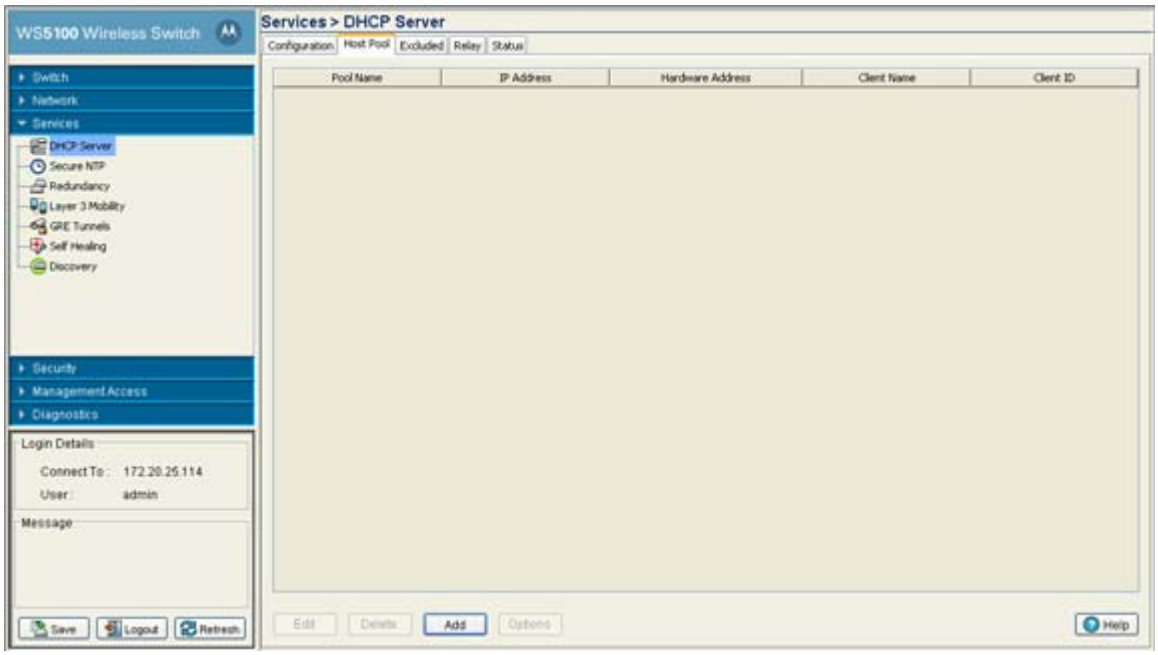
Refer to the **Host Pool** tab within the DHCP Server screen to view how the host pools reserve IP addresses for specific MAC addresses. This information can be an asset in determining if a new pool needs to be created or an existing pool requires modification.

To view the attributes of existing host pools:

1. Select **Services** > **DHCP Server** from the main menu tree.

   The DHCP Server screen displays with the **Configuration** tab displayed.

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 the current 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 a same host pool.

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 to the switch, highlight the pool from within the Network Pool 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

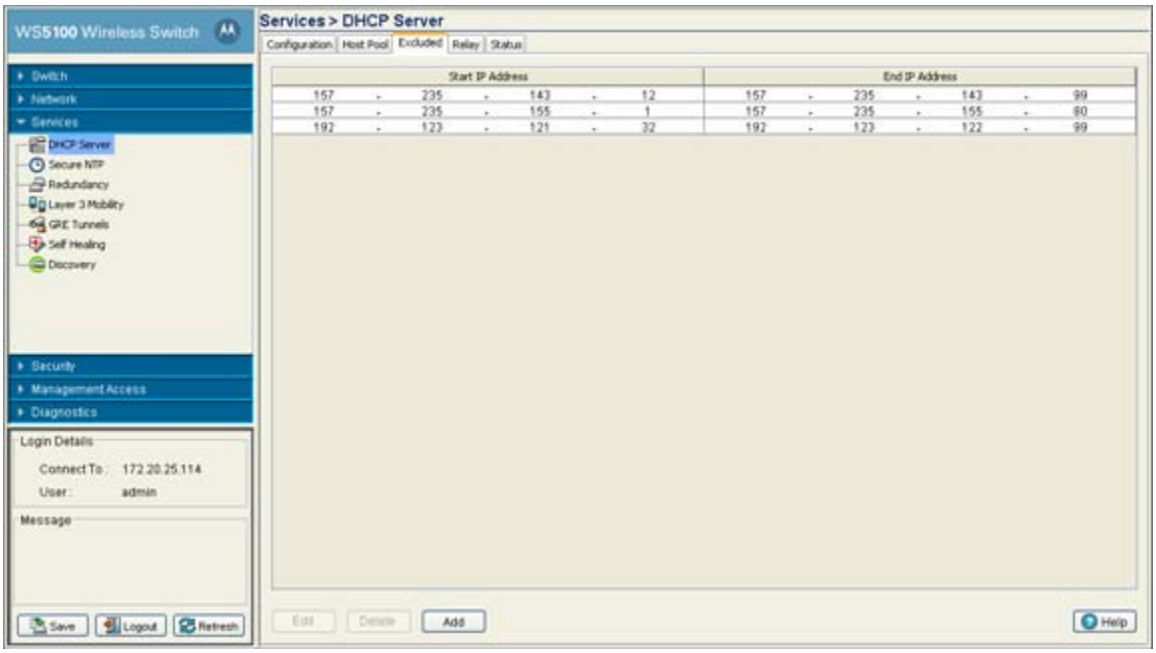
The DHCP Server may have some IP addresses unavailable to it when assigning IP address ranges for a pool. If IP addresses have been manually assigned and fixed, they need to be made available for the administrator to exclude from possible selection.

To view excluded IP address ranges:

1. Select **Services** > **DHCP Server** from the main menu tree.

   The DHCP Server screen displays with the **Configuration** tab displayed.

2. Click the **Excluded** tab.



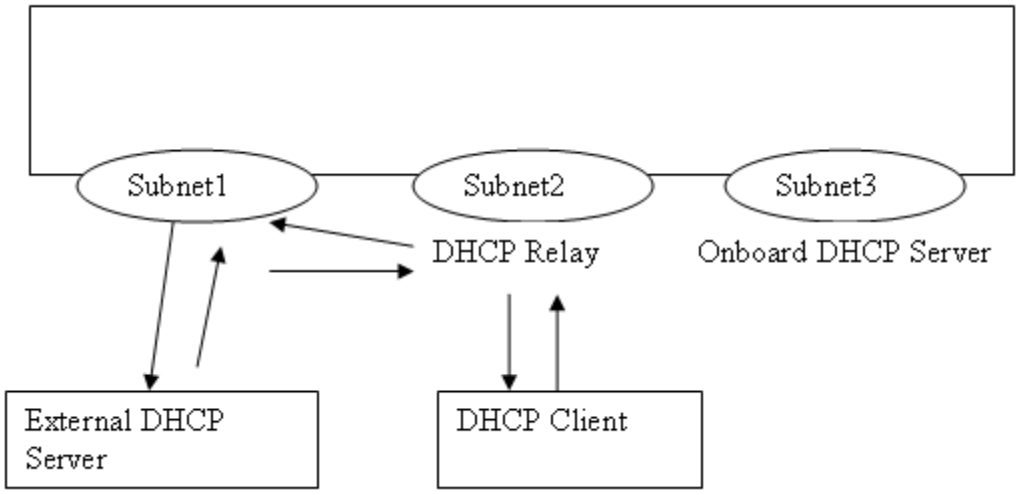
   The Excluded tab displays those “fixed” IP addresses that have been statically assigned and are now unavailable for assignment with a pool.

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 DHCP Server Relay Information

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 isv"ip helper-address <subnet1 External DHCP Server IP > <subnet1 Interface Name>"). When configuring a DHCP Relay address, specify the other interface name through which 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 in the above scenario. Consequently, the DHCP Server cannot run on either subnet1 or subnet2, it must be both.

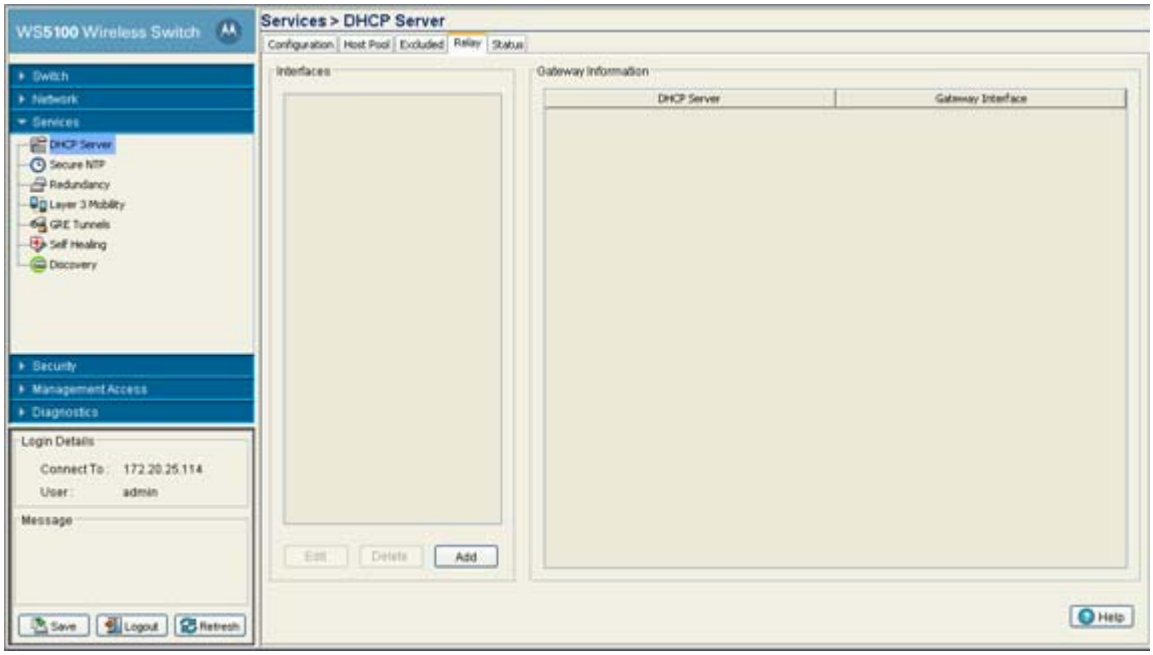
However, you can run the onboard DHCP server on subnet3 to provide DHCP requests for clients in subnet3. This is independent of the DHCP relay configuration. You cannot run onboard DHCP Server on subnet1 to provide IP addresses to DHCP clients requesting IP addresses using DHCP relay.

To view and configure DHCP relay information:

1. Select **Services** > **DHCP Server** from the main menu tree.

   The DHCP Server screen displays with the **Configuration** tab displayed.

2. Click the **Relay** tab.

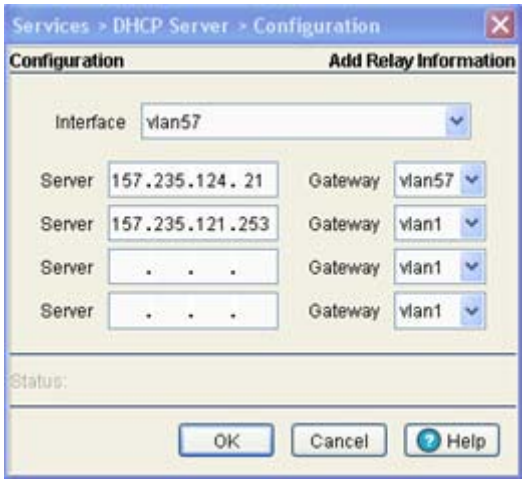


3. Refer to the **Interface** field for the names of the interfaces available to route information between the DHCP Server and DHCP clients. If this information is insufficient, consider creating a new IP pool or edit an existing pool.
4. Refer to the **Gateway Information** field for DHCP Server and Gateway Interface IP addresses ensure these address are in no way in conflict with the addresses used to route data between DHCP Server and client. The gateway address should not be set to any 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 one and 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 DHCP Server Status

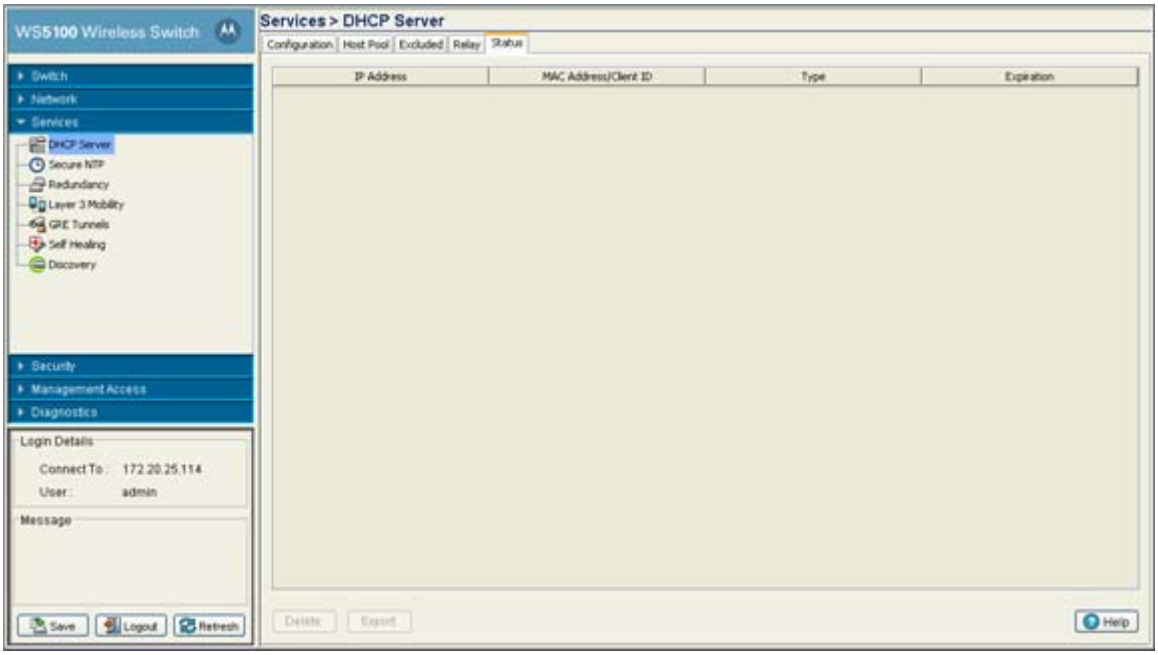
The switch DHCP Server screen can display a tab with information on the MUs using a leased IP address from the switch DHCP server. User this information to assess whether the MU is still a viable client for receiving switch DHCP resources.

To view detailed DHCP Server status:

1. Select **Services** > **DHCP Server** from the main menu tree.

   The DHCP Server screen displays with the **Configuration** tab displayed.

2. Click the **Status** tab.



3. Refer to the contents of the **Status** tab for the following:

IP Address	Displays the IP address for the client with the MAC Address listed in the MAC Address/Client ID column.
MAC Address/Client ID	Displays the MAC address (client ID) of the client using the switch's DHCP Server to access switch resources. The MAC address is read-only and cannot be modified.
Type	Displays the client type interoperating with the switch's DHCP server.
Expiration	Displays the expiration date for the lease used by this particular DHCP client interoperating with the switch's DHCP server.

4. To delete an entry from the list, highlight the address (by IP or MAC address) and click **Delete**.
5. Click the **Export** button to display a screen used to export DHCP Server status to secure location.
6. 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*.

5.3 Configuring Secure NTP

Secure Network Time Protocol (SNTP) is central for networks that rely on their switch managed infrastructure 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 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 found secure for switch interoperation. When configuring a NTP server, the status will take approximately 15 minutes to update (within the switch Web UI) after the clock is synchronized.

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*
- *Defining a SNTP Neighbor Configuration*
- *Viewing SNTP Associations*
- *Viewing SNTP Status*

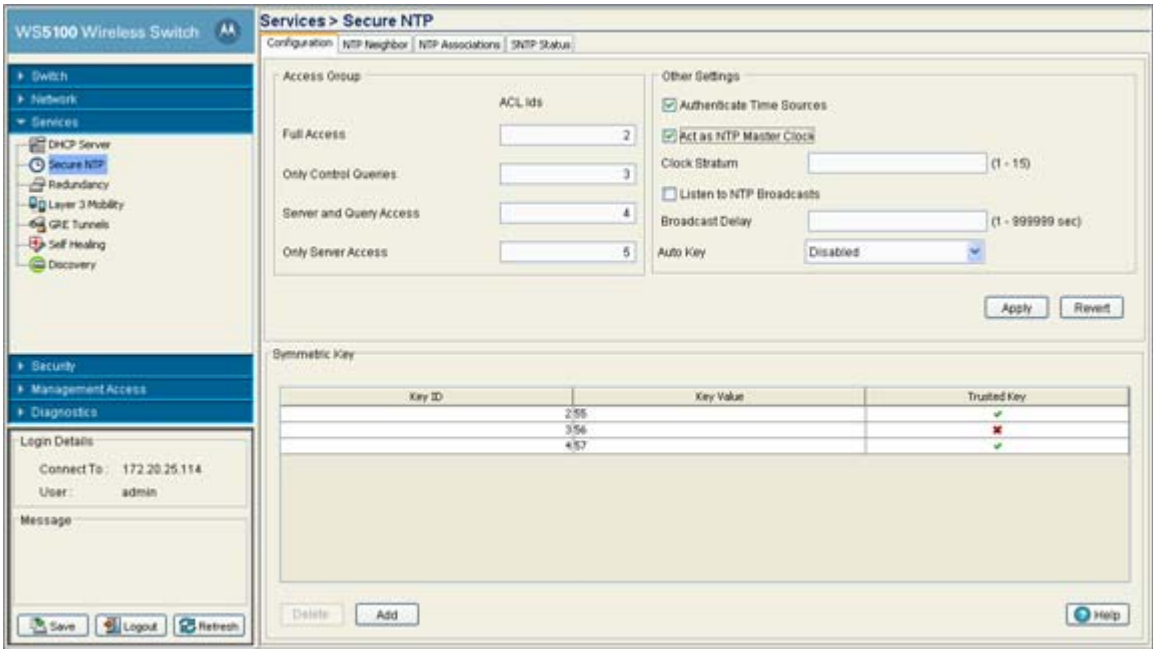
5.3.1 Defining the SNTP Configuration

SNTP provides synchronized timekeeping between the switch and a time server. Use the Configuration tab to define how SNTP resources are authenticated before interacting with the switch and enable ACL IDs to be mapped to SNTP access groups.

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 to enable the supplied ACL ID full access.
Only Control Queries	Supply a numeric ACL ID to enable the supplied ID only control query access to SNTP resources.
Server and Query Access	Enter a numeric ACL ID to enable the supplied ACL ID Server and Query access to SNTP resources.
Only Server Access	Define a numeric ACL ID to enable the supplied ACL ID 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 a credential authentication step is included between the SNTP server and the switch. When this checkbox is selected, the Apply and Revert buttons become enabled to save or cancel settings within the Other Settings field.
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 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.
6. Click the **Revert** button to undo the changes to the screen and revert to the last saved configuration.
7. Refer to the **Symmetric Key** field to view the following information.

Key ID	Displays 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.
Key Value	Displays the authentication key 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 allows key information from the server to be considered secure. The authentication procedures requires that both the local and remote servers share the same key and key identifier. Therefore, using key information from a trusted source is important.

8. Select an existing Key and click the **Delete** button to permanently remove it from the list of Key IDs.
9. Click the **Add** button to create a new Symmetric Key that can be used by the switch. For more information on adding a new key, see *Adding a New SNTP Symmetric Key on page 5-18*.

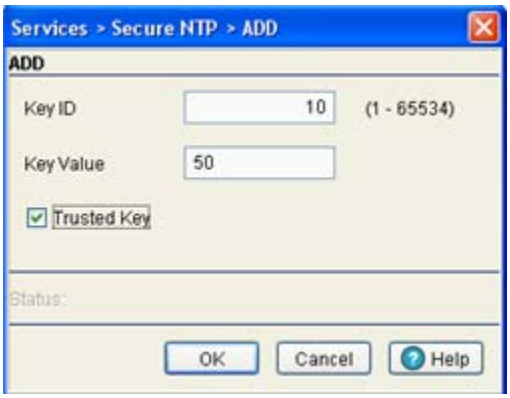
CAUTION: After an NTP synchronization using a Symmetric Key, the NTP status will not automatically be updated (it takes approximately 15 minutes to update within the switch Web UI.

5.3.2 Adding a New SNTP Symmetric Key

To add a new key to the Configuration tab:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **Configuration** tab.

3. Click the **Add** button.



4. 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.
5. Enter the authentication **Key Value** used to secure the credentials of the NTP server providing system time to the switch.
6. 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.
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 **OK** to save and add the changes to the running configuration and close the dialog.
9. Click **Cancel** to close the dialog without committing updates to the running configuration.

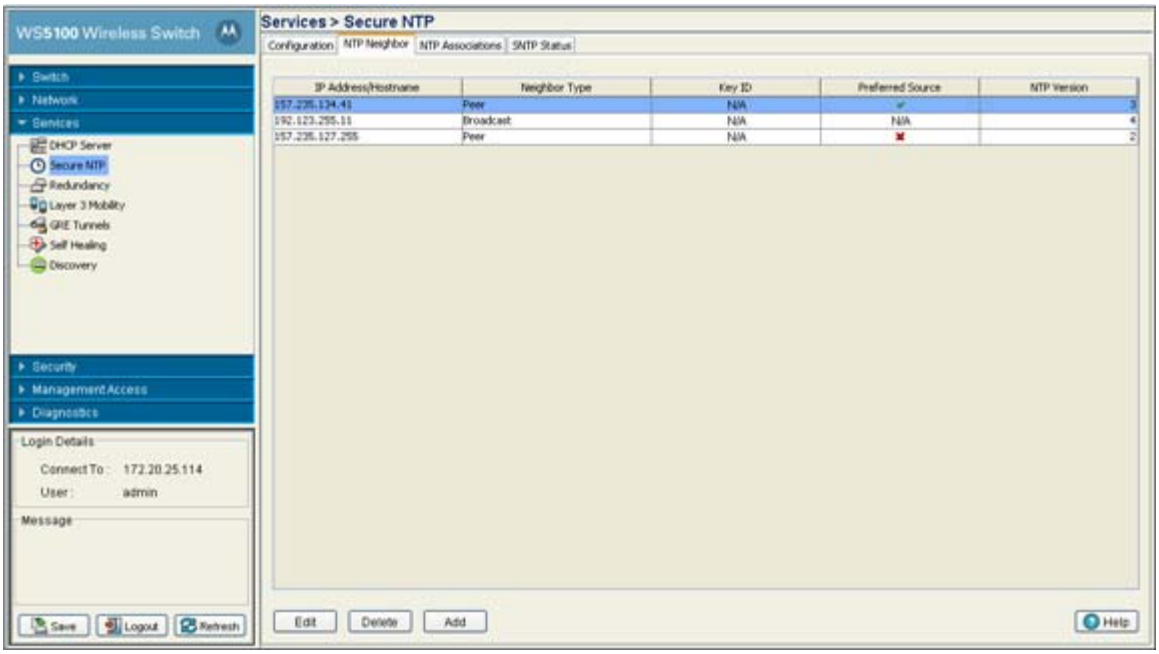
5.3.3 Defining a SNTP Neighbor Configuration

The switch's SNTP 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.

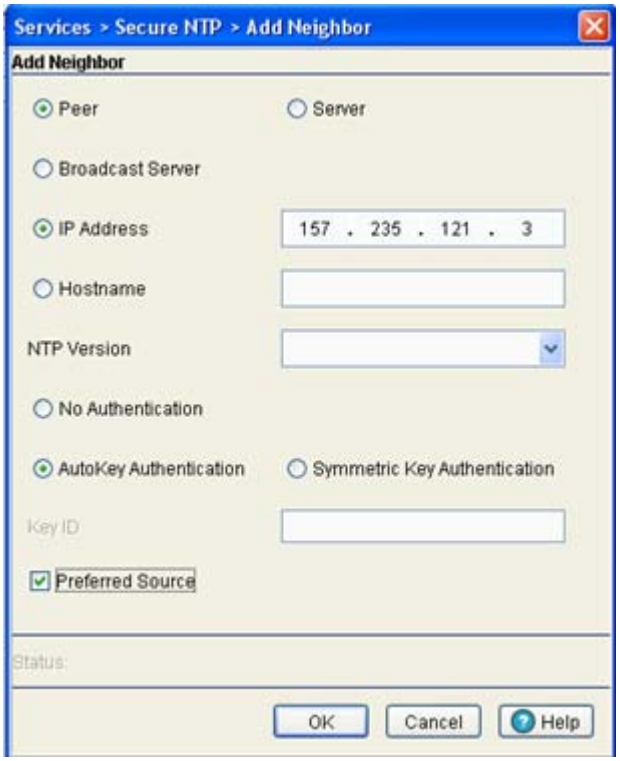
IP Address/ Hostname	Displays the numeric IP address of the resource (peer or server) providing SNTP resources for the switch. Ensure the server is on the same subnet as the switch in order to provide SNTP support.
Neighbor Type	Displays whether the NTP resource is a Peer (another associated peer device capable of SNTP support) or a Server (a dedicated SNTP 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 version 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 5-21*.

5.3.4 Adding an NTP Neighbor

To add a new NTP peer or server neighbor configuration to those available to the switch 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 reduces 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 with this configuration.
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.

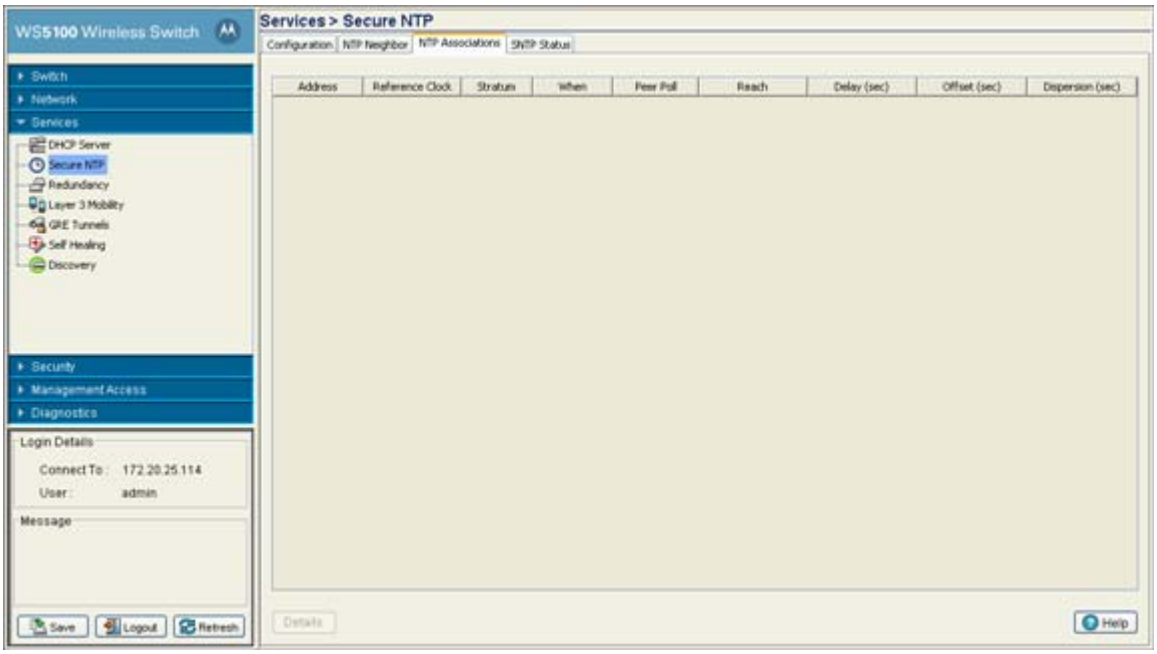
5.3.5 Viewing SNTP Associations

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 number. 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

4. Select an existing NTP association and click the **Details** button to display additional information useful in discerning whether the association should be maintained.

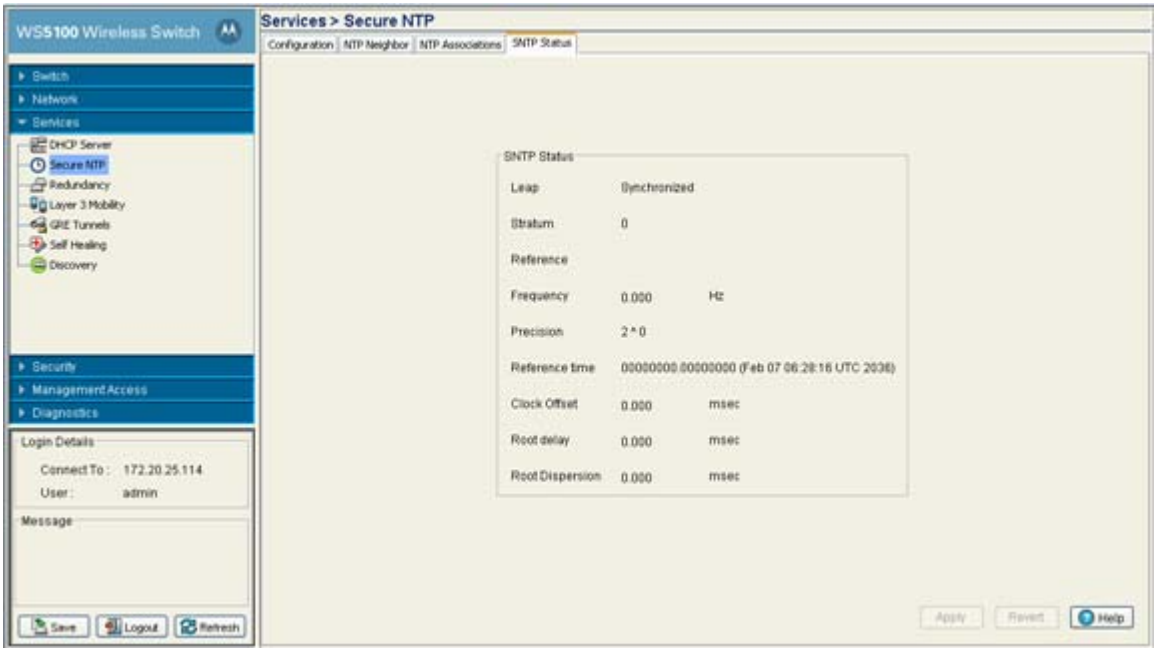
5.3.6 Viewing SNTP Status

Refer to the **SNTP 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 be updated (it takes approximately 15 minutes to update within the switch Web UI.

To review the switch's current NTP associations:

1. Select **Services** > **Secure NTP** from the main menu tree.
2. Select the **SNTP 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

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 goes one step further to provide centralized management from any single switch in the network without restricting or dedicating a 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.

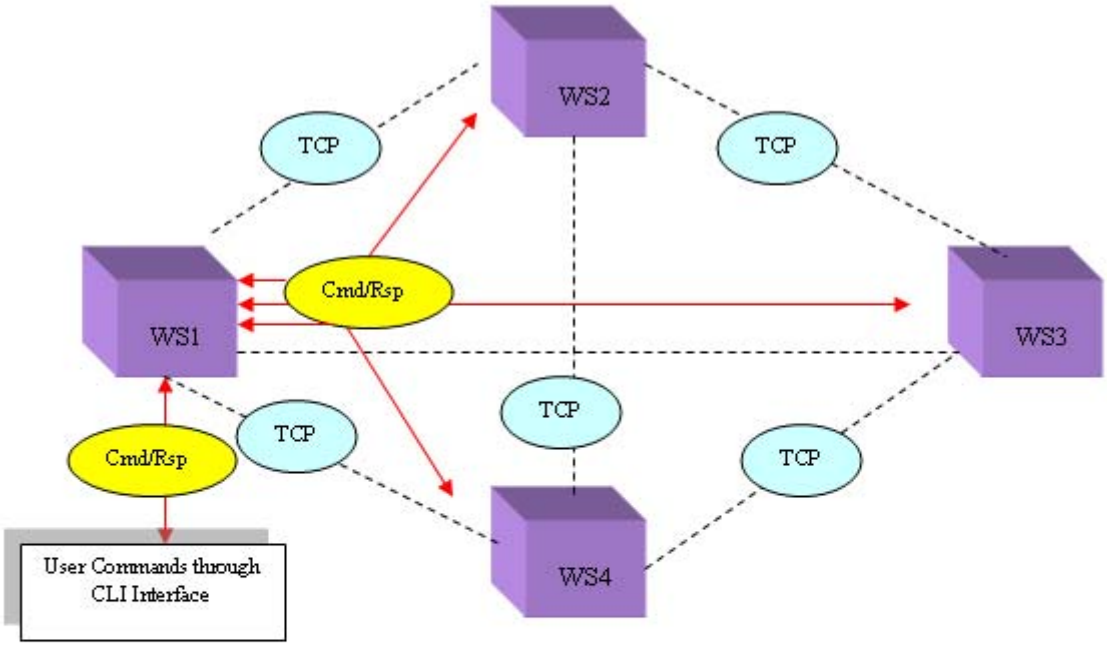
A redundancy group (cluster) is a set of switches (nodes) uniquely identified by group/cluster ID. Within the redundancy group, member switches discover and establish connections to other members of the group. The redundancy group has full mesh connectivity using TCP as the transport layer connection.

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 based options. This new functionality provides an alternative method for configuring members collectively from a centralized location, instead of configuring specific redundancy parameters on individual switches.

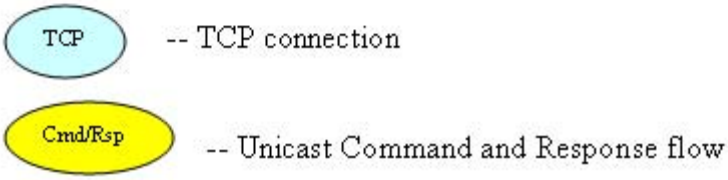
Configure each switch in the cluster by logging in to one participating switch. The administrator does not need to login to each redundancy group member, as one predicating switch can configure each member in real-time without “pushing” configurations between switches. A new CLI context called "cluster-cli" is available to set the configuration for all members of the cluster. All switch CLI commands are considered cluster configurable.

In the example below, there are four wireless switches (WS1, WS2, WS3 and WS4) forming a redundancy group. Each switch has established a TCP connection with the other switches 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. To view status and membership information, refer to the following:



Legends:



After sending the command to the 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. The members that respond to this command 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). For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-34*.

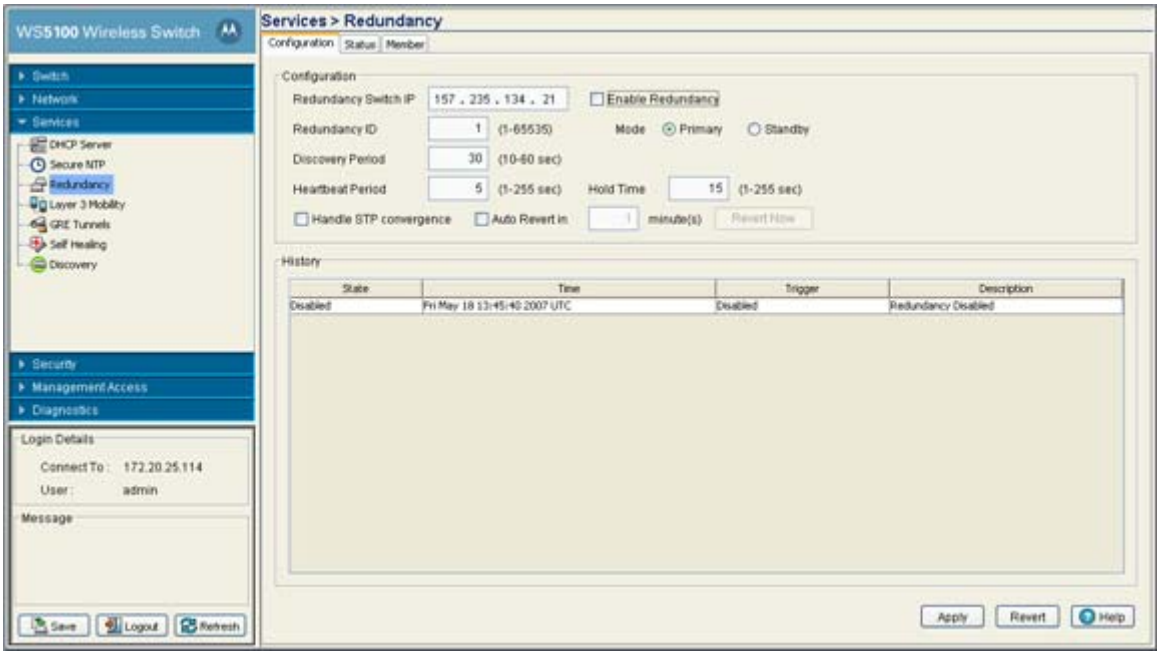
To view status and membership data and define a redundancy group configuration, refer to the following:

- *Reviewing Redundancy Status*
- *Configuring Redundancy Group Membership*

To configure switch redundancy:

1. Select **Services** > **Redundancy** from the main menu tree.

   The Redundancy screen displays with the Configuration tab selected.



2. Refer to the **Configuration** field to define the following:

Redundancy Switch IP	Define the IP address the redundancy feature uses to send heartbeats and update messages.
Enable Redundancy	Select this checkbox to enable/disable clustering. Clustering must be disabled to set any redundancy related parameter. All the modifiable values are grayed out if redundancy is enabled.
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 for an ID is 1-65535.
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.
Discovery Period	Use the **Discovery Period** field to configure cluster member discovery time. During the discovery time, a switch discerns the existence of other switches within the redundancy group.
Heartbeat Period	The **Heartbeat Period** is the interval heartbeat messages are sent. Heartbeat messages are used to discover the existence and status of other members within the redundancy group.

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 to be 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 greater than the heartbeat interval.
Handle STP convergence	Select the **Handle STP convergence** checkbox to enable STP convergence for the switch. STP stands for *Spanning Tree Protocol*. 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 forward is 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 execution is important to load balance Access Ports at startup.
Revert Now	Click the **Revert Now** button to immediately revert back to the previous version of the redundancy configuration. Clicking this button disregards any interval that may have been set using the Auto Revert In feature. If you have made extensive changes, and then change your mind about them, you can get rid of them by reading in the previous version of the file.

3. 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.

4. 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.
5. Click the **Revert** button to undo the changes to the screen and revert to the last saved configuration.

5.4.1 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.

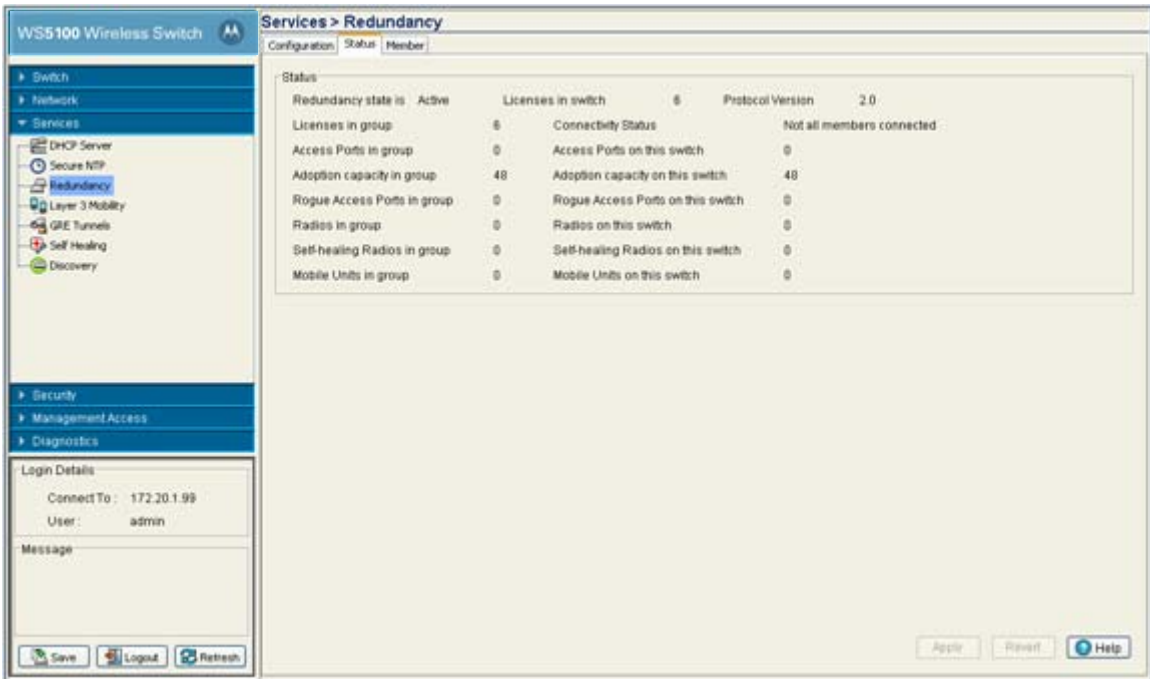
NOTE: When ETH2 of one of the group members is unplugged, the other members report that this member as gone, but an AP will continue to be adopted by the switch with no ETH2 connectivity.

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.

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 "Startup" state. From "startup" it goes to "Discovery" state immediately if the STP convergence is not enabled. Otherwise, it remains in "Startup" state 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 determine the redundancy group authorization level. After discerning memberships, it moves to an Online state. There is no difference in state execution for the Primary and Standby modes of operation.
Licenses in switch	Displays the number of licenses installed to adopt access ports on the current switch.
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.
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 5-34*.
Access Ports in group	Displays the total of the number of access ports 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 all 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.
Connectivity Status	Displays the current connectivity status of the cluster membership.
Access Ports on this switch	Displays the total of the number of access ports adopted by this switch within the redundancy group.
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 5-34*.
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 with a particular (or this) switch.
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 the radios within the cluster 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 particular 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.

5.4.2 Configuring Redundancy Group Membership

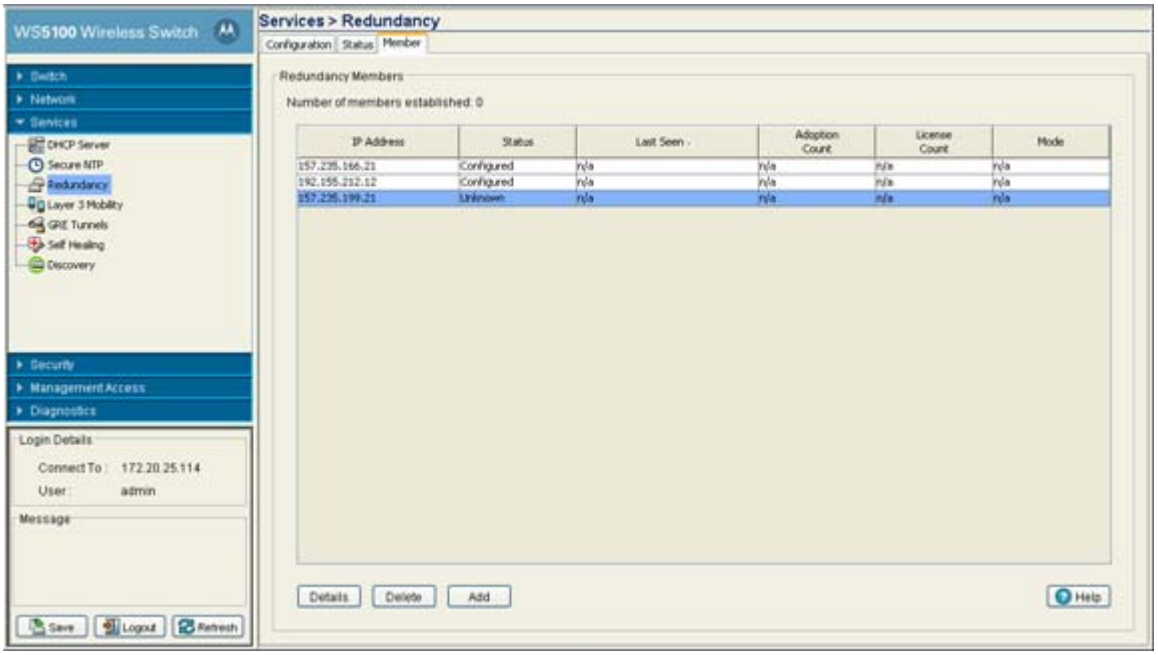
The redundancy group should be disabled to conduct an Add/Delete operation. There are a minimum of 2 members needed to comprise a Redundancy Group, including the initiating switch

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.
Adoption Count	Displays the number of access ports adopted by this member.
License Count	Displays the number of 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 5-32*.
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 5-34*.

5.4.2.1 Displaying Redundancy Member Details

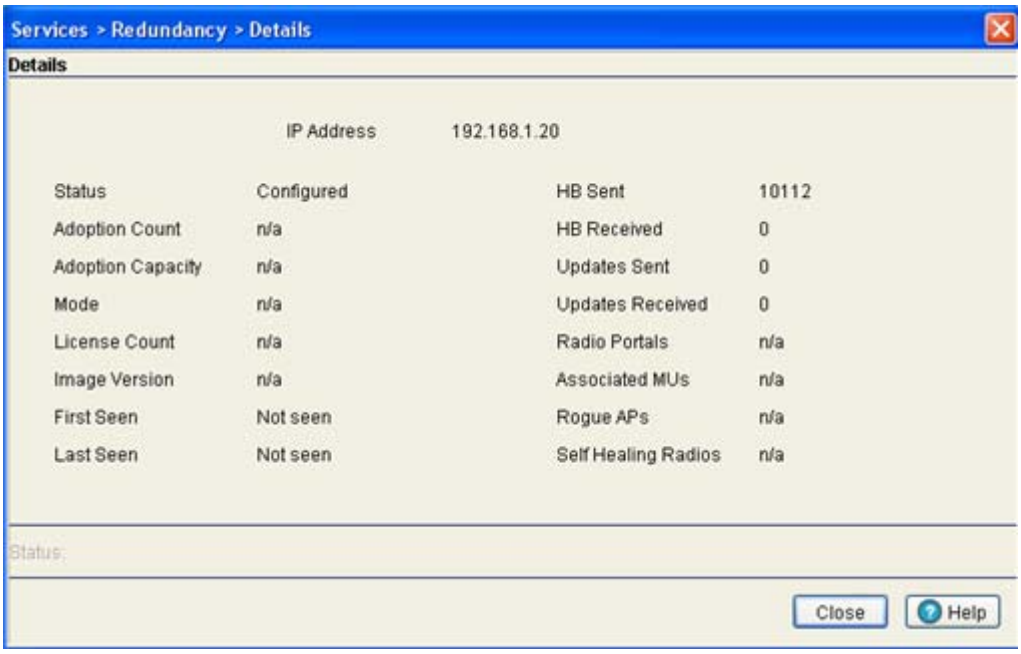
Use the **Details** screen (in conjunction with its parent Member screen) to display additional (more detailed) information on the redundancy group (cluster) member selected within the Member screen.

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.

Adoption Count	Displays the number of 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 5-34*.
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
License Count	Displays the number of port licenses available for this switch. For information on licensing rules impacting redundancy group members, see *Redundancy Group License Aggregation Rules on page 5-34*.
Image Version	Displays the image version currently running on the selected member. Is this 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.
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 listed. 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.

5.4.2.2 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.

5.4.3 Redundancy Group License Aggregation Rules

Refer to the following for the rules governing license usage amongst the members of a redundancy group:

- A redundancy group license is determined by adding individual switch installed license values.
- Do not allow different port speed/duplex settings on sa members. All members should be identical.
- 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 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 will initiate 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.

5.5 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 which enables 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 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.

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 to be configured to be part of the same mobility domain (using a mobility domain string identifier) such that MUs roaming between these switches can retain their Layer 3 address and thus 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 for the MU is the switch in the mobility domain to which it is currently associated to, and keeps changing as the MU continues to roam amongst. The current switch is also 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.

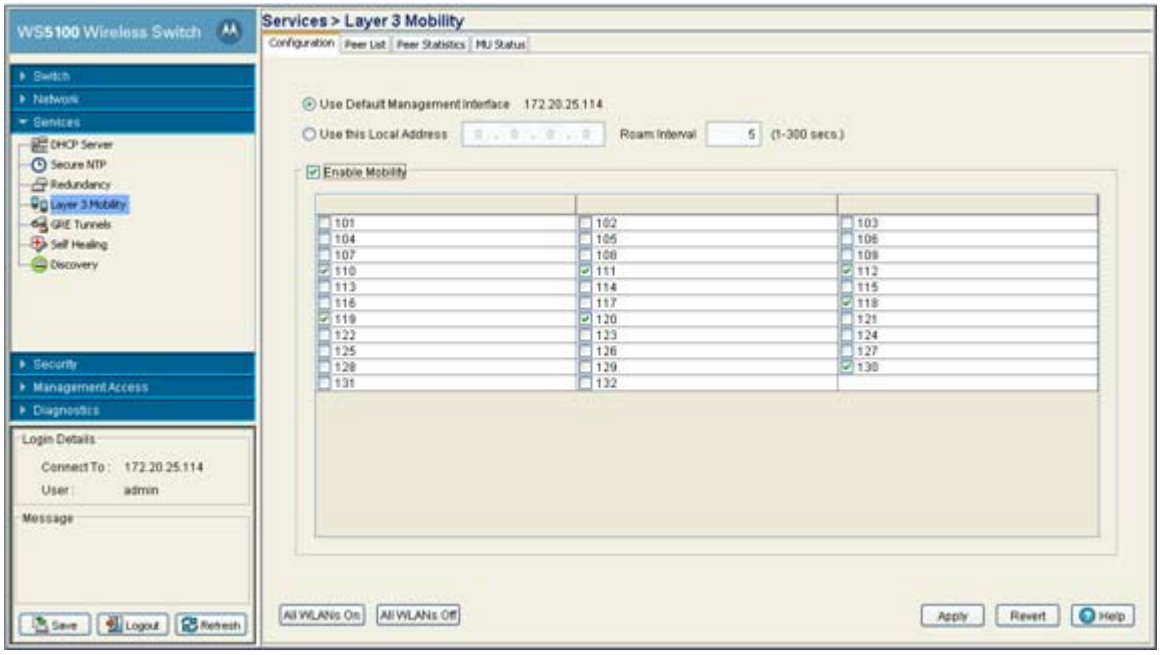
Key aspects of Layer 3 Mobility include:

- 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
- 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 L2 packet inside GRE with a proprietary code-point.
- When MUs roam within the same VLAN (L2 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 L3 subnet to another are symmetric.

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 the MUs roaming amongst different Layer 3 subnets,. The IP address displayed to the right of the checkbox will be used by the Layer 3 MU traffic.
3. If wanting to use a local IP addresses (non switch management interface) for the MUs roaming amongst different Layer 3 subnets, select the **Use this Local Address** checkbox and enter the 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, these MUs within these WLANs will be able to 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 you want to enable mobility for each WLAN, manually select just the few 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

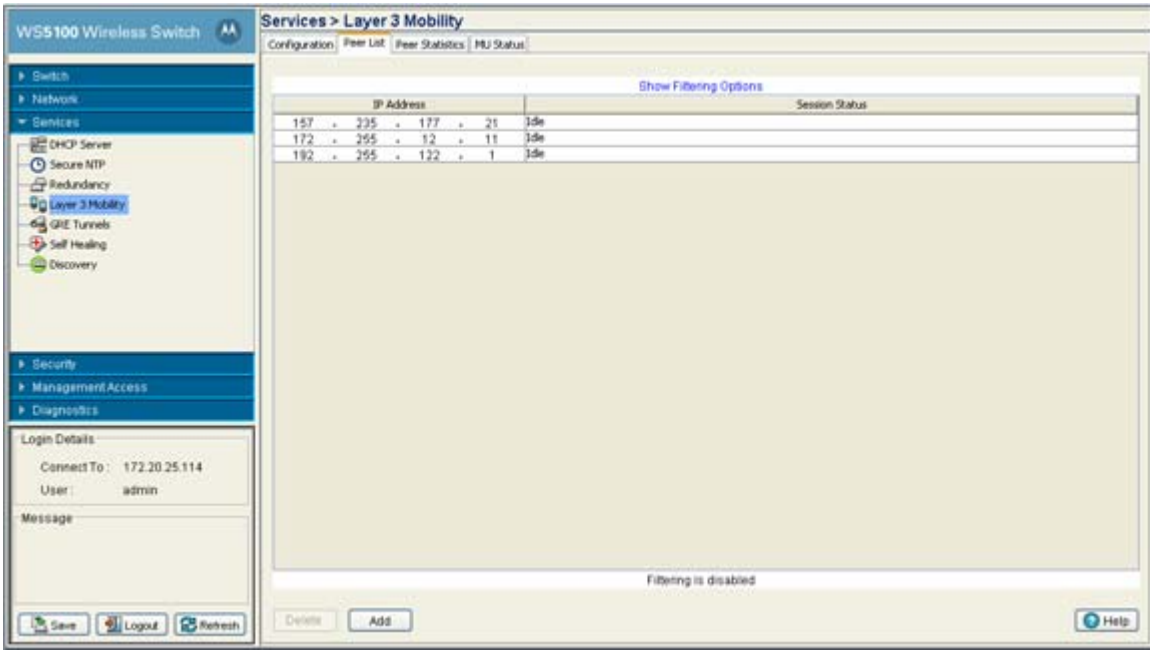
The Layer 3 Peer List contains the IP addresses MUs are using to roam amongst various subnets. This screen is helpful in display the IP addresses available to the MUs requiring access to different subnet resources.

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.

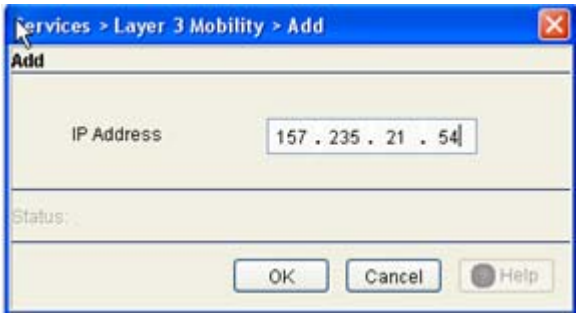


3. Refer to the contents of the Peer List table for existing IP addresses and Layer 3 MU session status.

   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 gets to keep 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). However the MU must send a DHCP request again and obtain a new IP address.

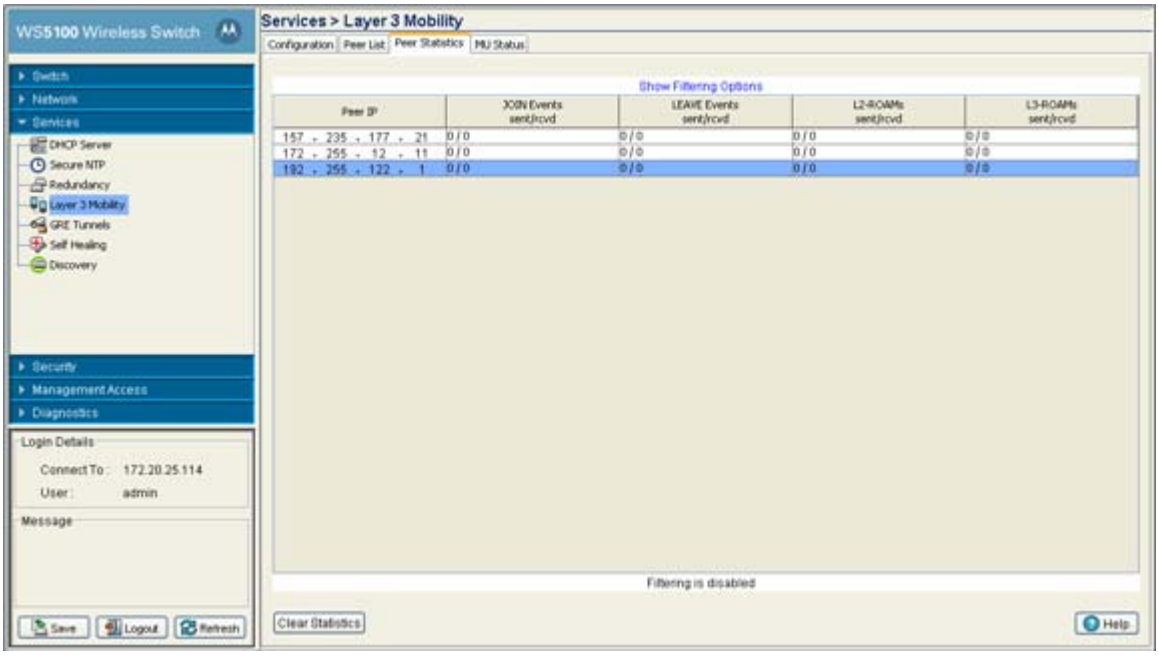
Tracking these message counts is important to gauge the behavior within the mobility domain.The Layer 3 Mobility screen contains a tab dedicated to tracking the message sent between the current switch, home switch and MU.

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 handle up to a maximum of 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 the its 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 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 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

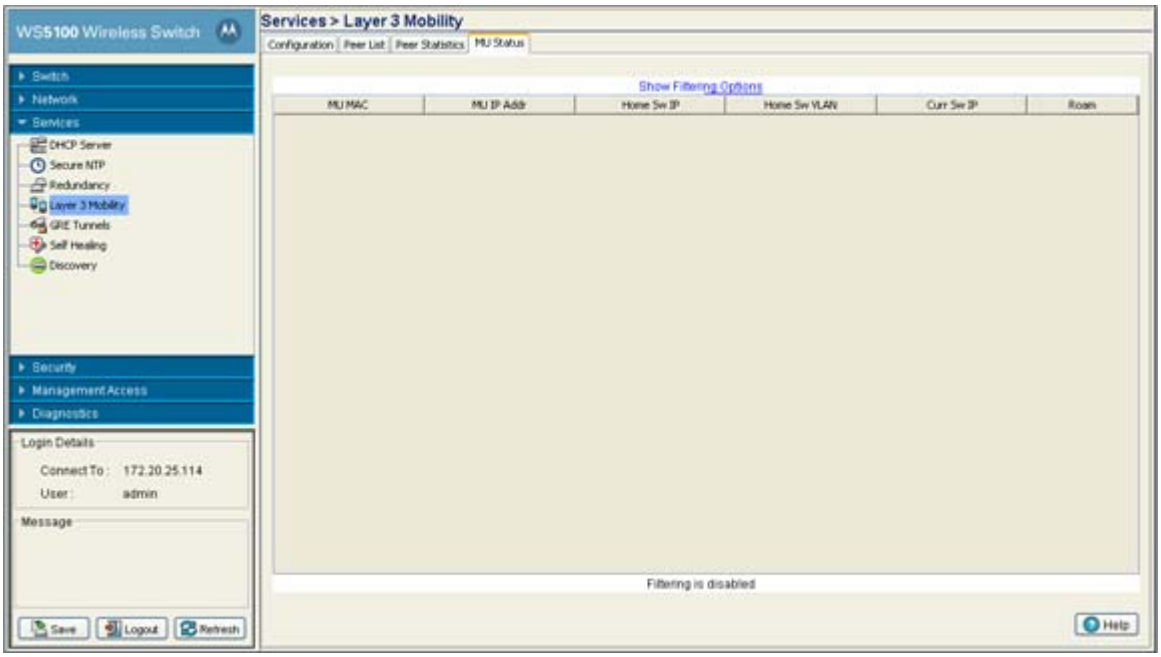
The Layer 3 Mobility **MU Status** tab displays a set of MU stats for associated MUs within the mobility domain. Use the MU status information to familiarize yourself with these MUs and their mobility-related parameters to distinguish new MUs entering the network from existing MUs roaming within the mobility domain.

To view Layer 3 mobility MU statistics

1. Select **Services** > **Layer 3 Mobility** from the main menu tree.

   The **Layer 3 Mobility** screen appears with the Configuration tab displayed.

2. Select the **MU Status** tab.



3. Refer to the following information within the MU Status tab:

MU MAC	Displays the factory hardcoded MAC address of the MU. This value is set at the factory and cannot be modified. Thus, it should be consistent as the MU roams within the mobility domain.
MU IP Addr	Displays the IP address the MU is using within the mobility domain. Again, this may not be the IP address used by the MU for initial association with the switch, but it is the IP address set for the MU to roam amongst subnets. For more information, see *Configuring Layer 3 Mobility on page 5-35*.
Home Sw IP	Displays the MU's home switch IP address. This is the IP address of the switch the MU is initially associated with, before roaming across subnets as part of its layer 3 mobility activity.
Home Sw VLAN	Displays the MU's home switch VLAN identifier. This is the VLAN index value set for the MU when it was originally configured as part of a VLAN with its home switch.
Curr Sw IP	Displays the IP address of the switch the MU is currently associated to within the mobility domain.
Roam	Displays the number of times the MU has roamed to a different layer 3 subnet.

5.6 Configuring GRE Tunnels

Tunneling involves encapsulating a packet that supports one protocol within another packet, which may run on the same protocol or on a different protocol. It is generally used to support evolving networks, its capacity and security requirements. *Generic Routing Encapsulation* (GRE) is one of the many commonly used protocols for IP over IP tunneling.

IP Tunneling allows network designers to implement policies like:

- Assigning routes to different types of traffic

- Assigning priority to different types of traffic
- Assigning security levels to different types of traffic

The advantages of using Tunnel include:

1. It provides communication between sub-network that have invalid or non-contiguous network addresses.
2. Multiple protocols types can be consolidated on a common backbone for reduced operational cost.
3. Assurance of privacy and security in shared networks that support multiple enterprise customers.

GRE is a multi protocol carrier and it encapsulates IP and other packets inside IP tunnel. In a GRE tunnel, a router at each side of the tunnel encapsulates protocol-specific packets in an IP header and creates a virtual point-to-point link to the routers at the other end of an IPcloud, where the IP header is stripped off. By connecting multi-protocol sub-networks in a single-protocol backbone environment, IP tunneling allows network expansion across a single-protocol backbone environment.

GRE allows a newly created tunnel to pass traffic to the other end of the tunnel. This enables the network administrator access to traffic mapped to the GRE tunnel. The switch provides a path to tunnel all WLAN traffic to the other end of the tunnel. This enables network administrators to forward MU traffic to a remote network without modifying their network configuration and thereby enabling them to span their subnet across the intermediate network. Each GRE tunnel however, must be on a unique subnet to function properly.

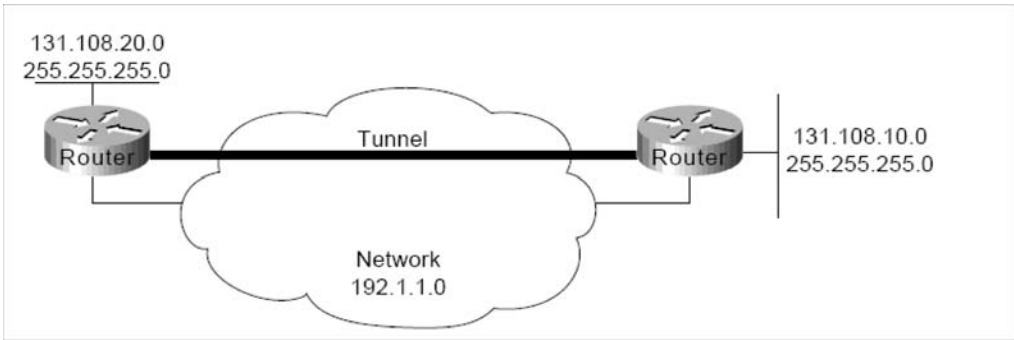
All data packets going from the configured WLAN to the GRE tunnel are forwarded to the mapped GRE tunnel using GRE encapsulation. The other end of the GRE tunnel is responsible for removing the GRE header and forwarding it to the destination IP.

The current implementation of GRE makes use of the management IP stack to route GRE encapsulated traffic. Encapsulation and decapsulation is done in the user space, which affects the performance of the switch. All the non-GRE packets continue to get forwarded as is.

GRE tunneling consists of three protocol types:

- Passenger—The protocol is encapsulated (IP)
- Carrier— GRE Protocol provides carrier services
- Transport—IP carries the encapsulated protocol.

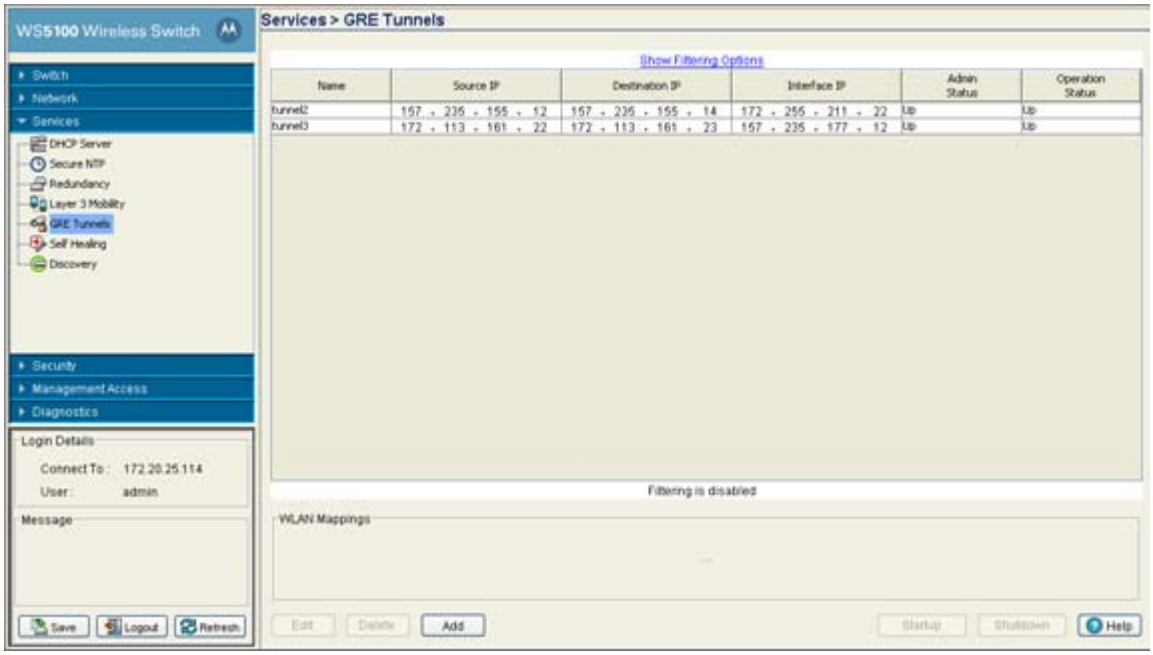
GRE tunneling allows desktop protocols to take advantage of the enhanced route selection capabilities of IP. With GRE Tunneling, it is possible for the two sub-networks of network 131.108.0.0 to talk to each other even though they are separated by another network.



To configure GRE tunnelling on the switch:

1. Select **Services** > **GRE Tunnels** from the main menu tree.

   The GRE Tunnels screen displays with existing GRE tunnels.



2. Refer to the top portion of the GRE Tunnels screen for the following information:

Name	Displays the names of each GRE tunnel defined for the switch.
Source IP	Displays the IP address where packets are originated by the switch and sent out through the tunnel interface. This defaults to the management VLAN's IP address.
Destinations IP	The destination IP address of the remote end of the GRE tunnel should be the default gateway for MUs that are associated on WLANs mapped to GRE tunnels. When the switch receives packets on the GRE tunnel interface, it first decapsulates the outer IP and GRE headers. An IP lookup is then performed on the destination IP of the inner IP packet using a MU table. If the lookup succeeds, the IP packet is encapsulated in an 802.11 frame (destined to the MU's MAC) and sent out on the WLAN port. If the lookup fails, the packet is dropped. Verify the gateway address has not been set to any VLAN interface used by the switch.

Interface IP	Displays the network IP address used to route GRE packets to their destination address.
Admin Status	Displays the status of a tunnel as either the active tunnel used currently for the switch or disabled.
Operation Status	Displays the status of tunnels as either the active (in use) or disabled.

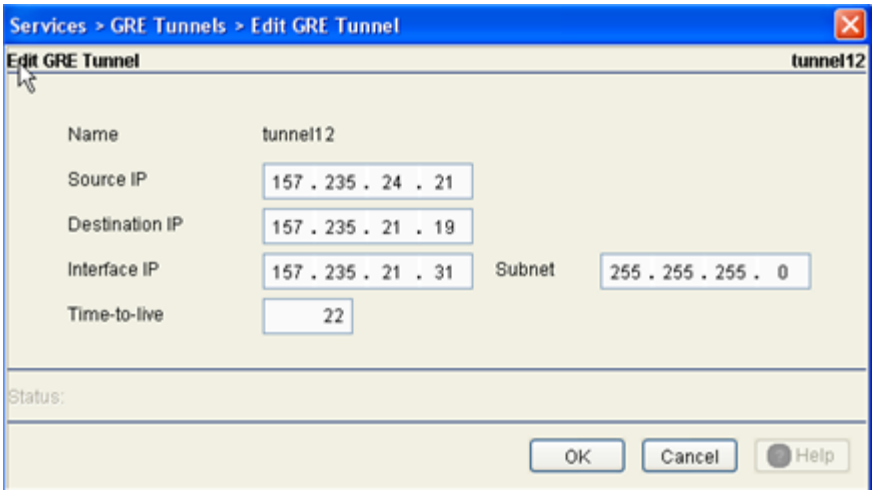
3. Highlight an existing tunnel and click the **Edit** button to modify the properties of the tunnel. For more information, see *Editing the Properties of a GRE Tunnel on page 5-44*.
4. Highlight an existing tunnel and click the **Delete** button to remove it from the list of tunnels available to the switch.
5. Click the Add button at the bottom of the screen to define the properties of a new tunnel. For more information, see *Adding a New GRE Tunnel on page 5-45*.
6. Highlight an existing tunnel and click the **Startup** button to make the selected tunnel active for the switch. Activating a new tunnel disables the previously enabled tunnel.
7. Highlight the active tunnel and click the **Shutdown** button to disable the selected tunnel.

5.6.1 Editing the Properties of a GRE Tunnel

Existing GRE tunnels can be selected and their properties modified as the source, end point or other existing tunnel information requires modification.

To edit the properties of an existing tunnel:

1. Select **Services** > **GRE Tunnels** from the main menu tree.
2. Highlight an existing tunnel and click the **Edit** button.



3. Refer to the following within the **Edit** screen and revise those properties necessary to re-create a functional tunnel

Name	Displays the read-only numerical name associated with the tunnel. To create a tunnel using a new name, you must click the **Add** button and configure a new GRE tunnel.
Source IP	Modify the IP address used in the src-IP field of the IP header when packets are originated by the switch and sent out through the tunnel interface. This would default to the management VLAN's IP address.

Destination IP	Traffic received on a GRE tunnel will be forwarded to MUs based on the Destination IP address defined.
Interface IP	Modify the network IP address (if necessary) used to route GRE packets to their destination address.
Subnet	Define the subnet address used to route GRE tunnel packets between end-points. Each GRE tunnel must have a unique subnet to function properly and independent of one another.
Time-to-live	Modify the period of time (in seconds) packets are kept alive between tunnel destinations. The defined interval ensures IP reachability between the tunnel end-points.

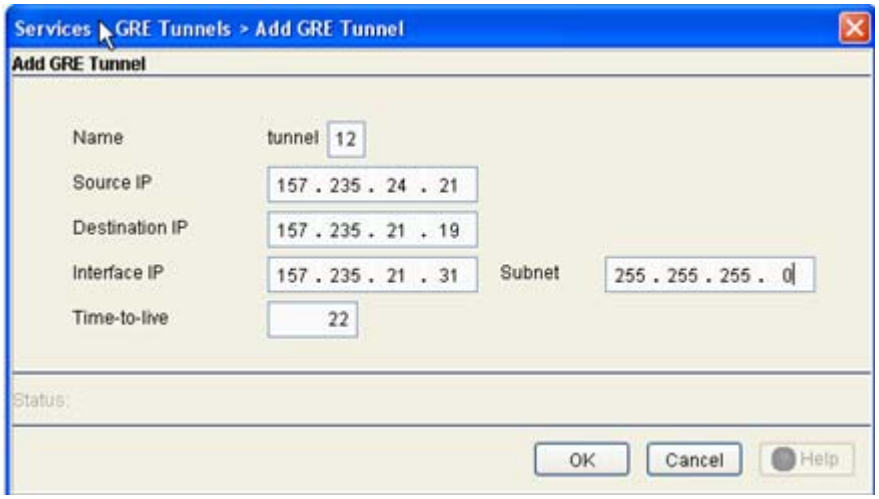
4. Click **OK** to save the contents of the screen and return to the main GRE Tunnels screen.
5. Click **Cancel** to exit the screen without updating the properties of the existing GRE tunnel.

5.6.2 Adding a New GRE Tunnel

If modifying an existing tunnel does not provide an adequate solution for your network, consider creating a new tunnel.

To create a new GRE tunnel:

1. Select **Services** > **GRE Tunnels** from the main menu tree.
2. Click the **Add** button from the bottom of the screen.



3. Configure the properties of the new GRE tunnel based on the following user-defined parameters.

Name	Define a numerical name for the tunnel. This value cannot be modified (using the Edit function) once originally created for a new tunnel.
Source IP	Define the IP address used in the src-IP field of the IP header when packets sent out through the tunnel interface.
Destination IP	Traffic received on a GRE tunnel will be forwarded to MUs based on this Destination IP address.
Interface IP	Define the network IP address used to route GRE packets to their destination address.

Subnet	Define the subnet address used to route GRE tunnel packets between end-points. Each GRE tunnel must have a unique subnet to function properly and independent of one another.
Time-to-live	Configure the period of time (in seconds) packets are kept alive between tunnel destinations. The defined interval ensures IP reachability between the tunnel end-points.

4. Click **OK** to save the contents of the screen and return to the main GRE Tunnels screen.
5. Click **Cancel** to exit the screen without updating the properties of the existing GRE tunnel.

5.7 Configuring Self Healing

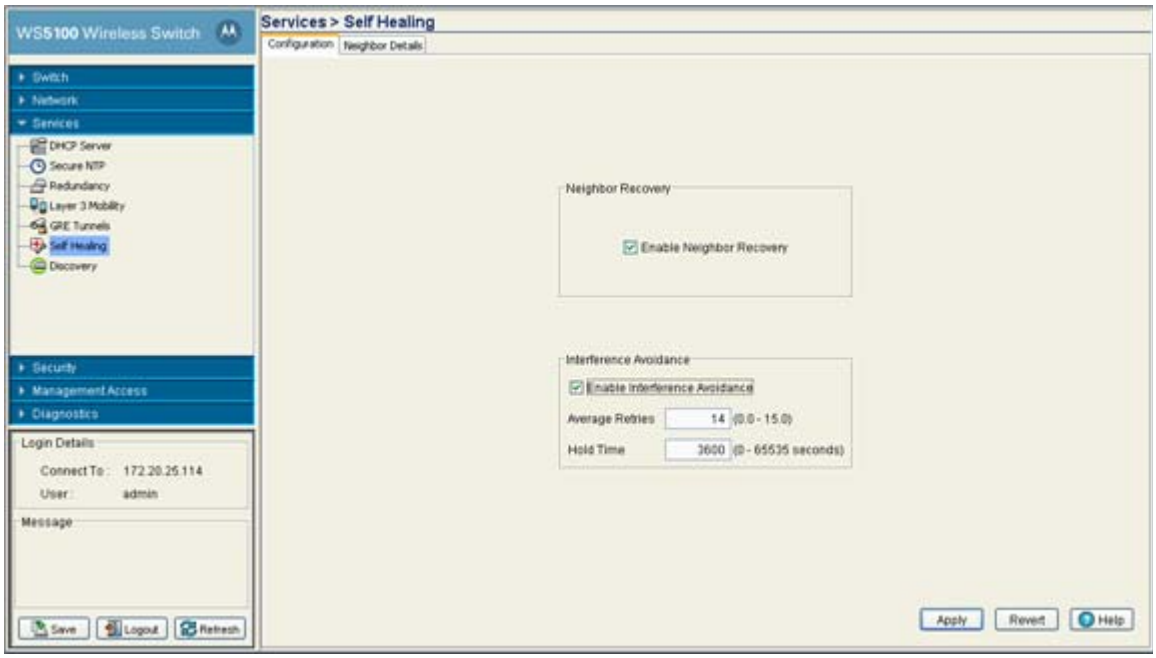
The switch supports a feature called *Self Healing* that enables radios to take corrective action when one or more radios fail. To enable the feature the user must specify radio neighbors that would self heal if either one goes down. The neighbor radios do not have to be of the same type. Therefore, 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 triggers the self healing action 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	Select **Enable Interference Avoidance** to enable the Interference Avoidance feature. The switch is capable of switching channels on an access port (Automatic Channel Selection) if the interference is observed on the current operating channel.
Average Retries	The Average Number of Retries is 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. The Average Retries is a threshold value, when exceeded ACS is initiated.
Hold Time	Set the interval (in seconds) that disables interference avoidance after detection. The hold time prevents the radio from re-running ACS continuously.

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.

5.7.1 Configuring Self Healing Neighbor Details

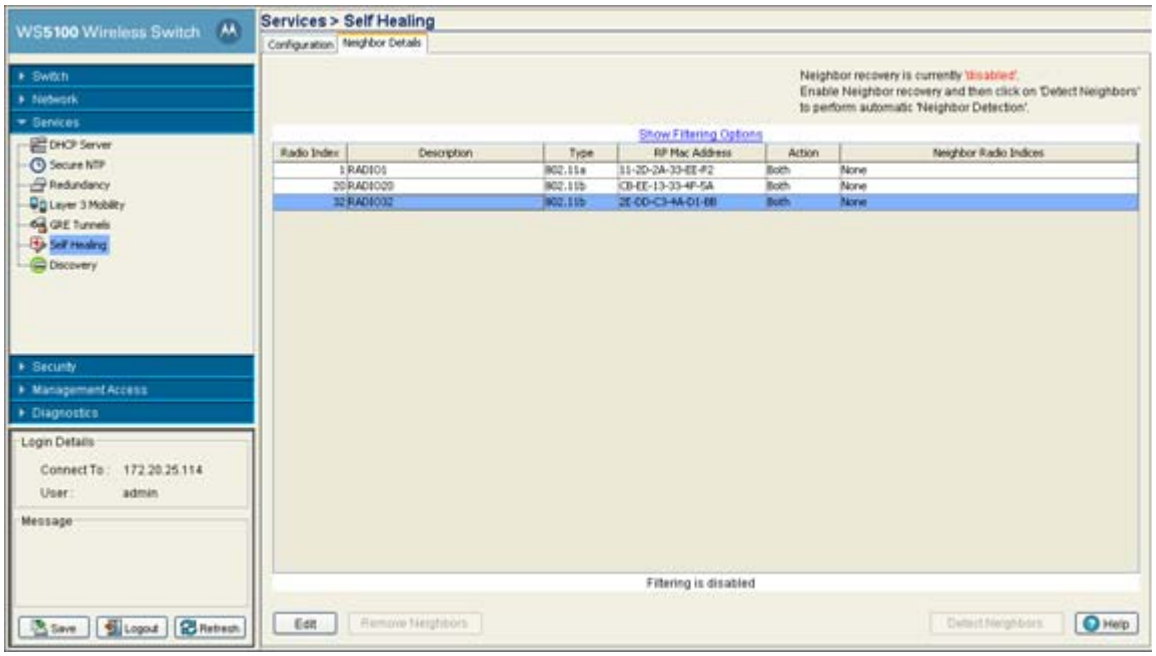
The Neighbor Details page displays all the radios configured on the switch and their neighbor designations.

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 of the screen displays whether Neighbor recovery is currently enabled or disabled. To change the state, click the Enable Neighbor Recovery checkbox on the Self Healing Configuration screen.

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 an identifier 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 5-48*.
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 their current neighbor list and move into detection mode to detect neighboring radios.

Detect Neighbors only works properly if all the radios are configured and adopted. Starting the automatic neighbor detection feature disassociates all of the MUs and clears the current neighbor configuration.

5.7.1.1 Editing the Properties of a Neighbor

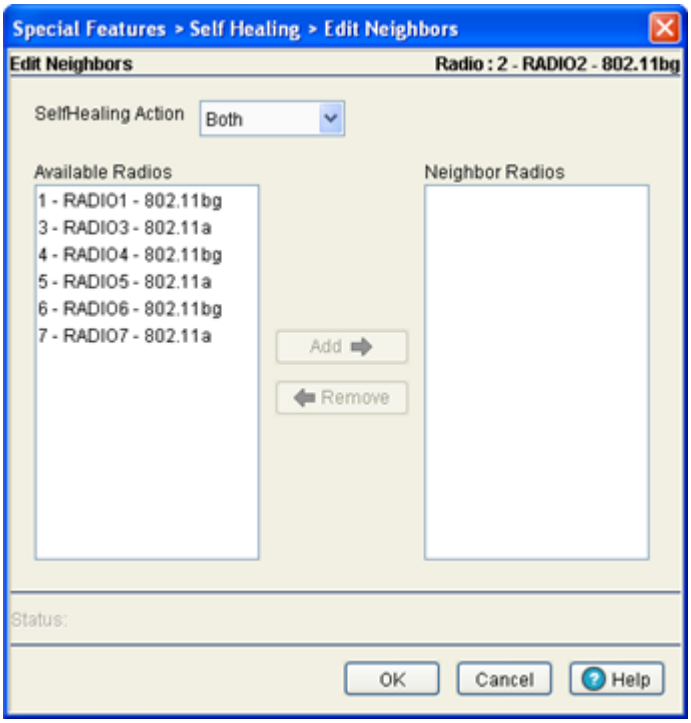
Use the **Edit** screen to specify the neighbor of a selected radio and the action the radio performs in the event its neighbor radio fails.

To edit the properties of a neighbor:

1. Select **Services** > **Self Healing** from the main menu tree.

   The Self Healing page launches with the **Configuration** tab displayed.
2. Select the **Neighbor Details** tab.

3. Select an existing neighbor and click the **Edit** button.



   The radio index and description for the current radio 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. Do this dedicate the neighbors for this radio.
6. Select a radio and click the **Remove** button to move the radio from the Neighbor Radios list to 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.

5.8 Configuring Switch Discovery

Switch discovery enables the SNMP discovery (location) of Motorola devices (running switch software version 3.0 or later). 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 of the specified network. If the value of the requested *object identifier* (OID) starts with Motorola enterprise OID the device is considered a Motorola device. The results of the discovery process are helpful for isolating devices compatible for operation within 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 **Saved 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.

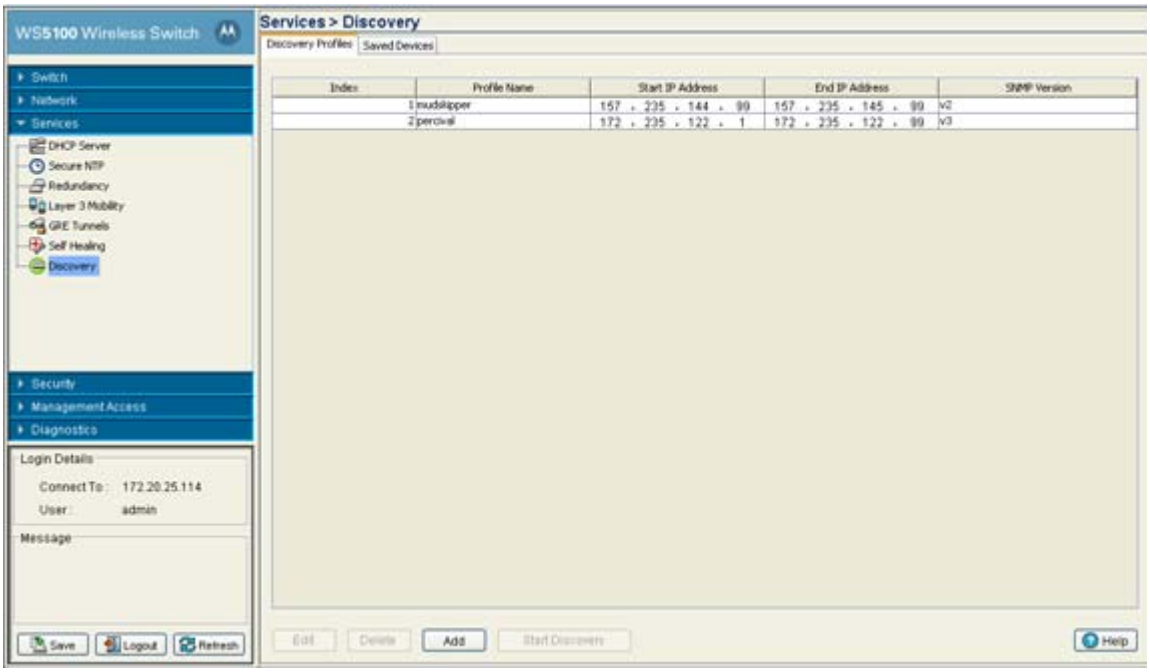
CAUTION: Switch discovery can be a time consuming operation. However, the switch discovery operation is a standalone process. This allows users to perform other configuration operations when discovery is running in the background.

5.8.1 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 WEB UI supplied 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 used to title 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. Selecting an existing profile and click the **Delete** button to remove this profile from the list of available profiles available for device discovery.
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 5-52*.
6. Click the **Start Discovery** button to display a **Read Community String** (SNMP v2) or V3 **Authentication** (SNMP v3) screen.

   Storing SNMP credentials as a string within switch's discovery profile table (SNMP table) can 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 the discovered devices within the Saved 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 entered is 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.

5.8.1.1 Adding a New Discovery Profile

If the contents of an existing profile are to 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.

   The **Discovery** page launches with the **Discovery Profiles** tab displayed.

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 are anticipated to 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 SNMP Version drop-down menu to define the version of the SNMP (either SNMP 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.

5.8.2 Viewing Discovered Switches

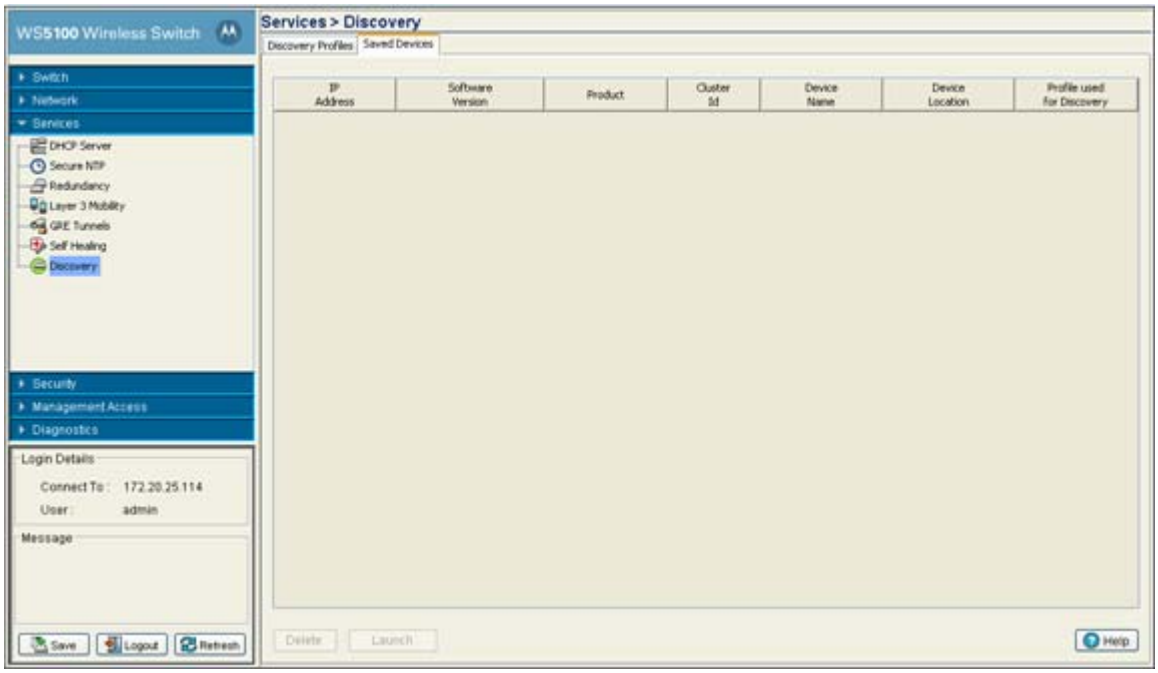
Refer to the **Saved Devices** tab to view a table of those devices discovered by the current discovery process. Each discovered device compatible with the locating switch (running switch software version 3.0 or higher) is displayed in a shaded color to distinguish it from non-compatible devices. The 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.

   The **Discovery** page launches with the **Discovery Profiles** tab displayed.

2. Select the **Saved Devices** tab.



3. Refer to the following information within the Saved 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.
Cluster ID	If the discovered device is part of a cluster (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 Saved 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 Saved 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 the purpose of its current configuration.

6

Switch Security

This chapter describes the security mechanisms available to the switch. This chapter includes the following:

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

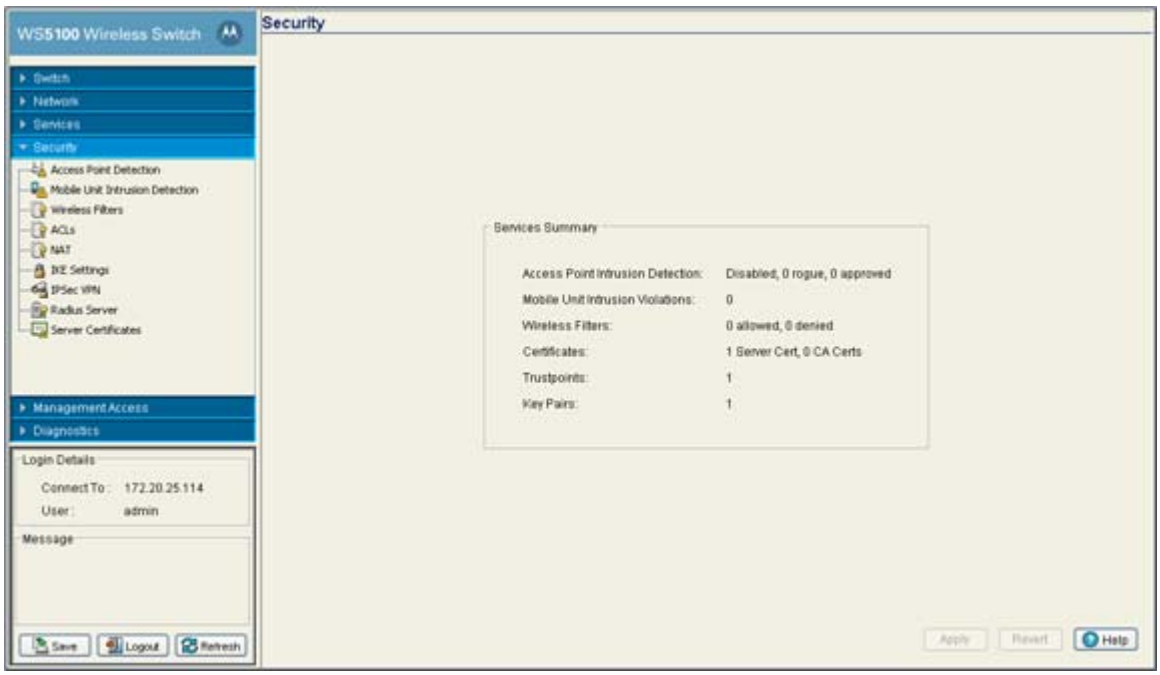
6.1 Displaying the Main Security Interface

Refer to main menu **Security** interface for a high level overview of the state of several 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 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 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:

Access Port Intrusion Detection	Displays the Enable or Disable state of the switch to detect potentially hostile access ports (the definition of which defined by you). Once detected, these 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 6-3*.
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 6-9*.
Wireless Filters	Displays the state of the current 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 Wireless Filters on page 6-12*.
Certificates	Displays the number of Server and CA certificates currently used by the switch. For more information, see *Creating Server Certificates on page 6-74*.
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 6-75*.
Key Pairs	Displays the number of Key Pairs currently used by the switch. For more information, see *Configuring Trustpoint Associated Keys on page 6-81*.

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

6.2 AP Intrusion Detection

Use the **Internet Protocol** sub-menu to view and configure network related IP information. The Internet Protocol screen consists of the following tabs:

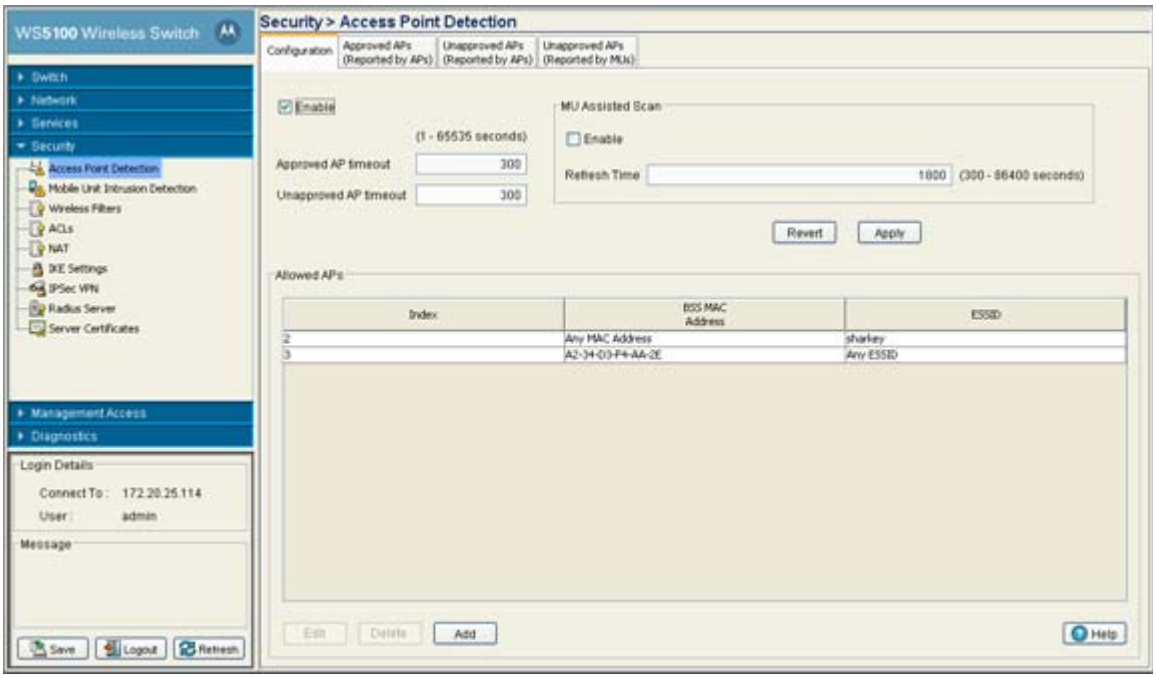
- *Enabling and Configuring AP Detection*
- *Approved APs (Reported by APs)*
- *Unapproved APs (Reported by APs)*
- *Unapproved APs (Reported by MUs)*

6.2.1 Enabling and Configuring AP Detection

Use the **Configuration** screen to enable 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 enables both access ports and MUs to scan and detect access points within the switch managed network. Continually re-validating the credentials of associated access points 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 within the switch managed network. The range is from 300 - 86400 seconds, with a default of 1800 seconds.

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 allowed access points within the switch managed network.

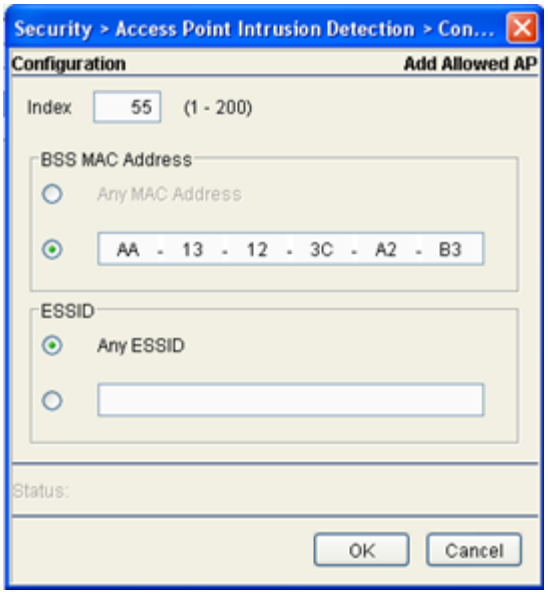
Index	Displays the numerical identifier (index value) assigned to this particular set of Allowed AP parameters. Assign this value by clicking **Add** for a new set of access point address information or click the **Edit** button to revise the index. The Index can be used as reference to group specific 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 a 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 a 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 range or modify the address range used to designate devices as Allowed APs:

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 located on the network as an Allowed AP. This is not necessary if a specific MAC address is used with this particular 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 used for this index 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.

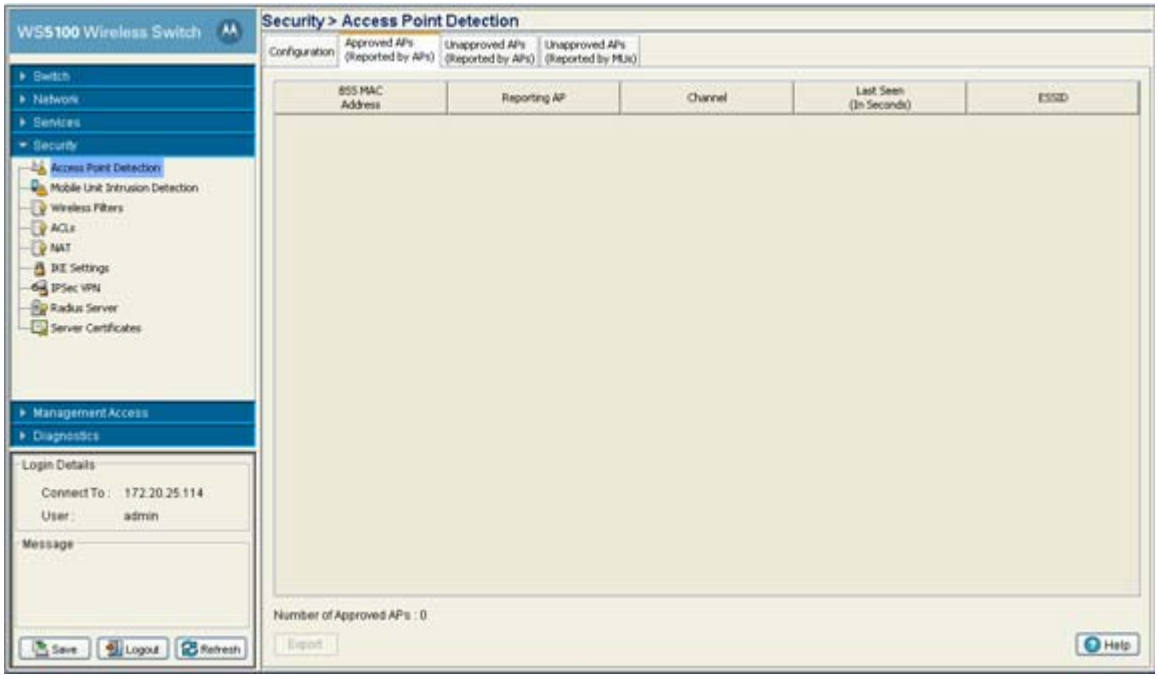
7. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
8. Click **OK** to use the changes to the running configuration and close the dialog.
9. Click **Cancel**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

6.2.2 Approved APs (Reported by 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 an approved device 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 (Reported by APs)** tab.



3. The **Approved APs (Reported by APs)** table displays the following information:

BSS MAC Address	Displays the MAC Address of each Approved AP. These MAC addresses are access points observed on the network meeting the criteria (MAC and ESSIDs) of allowed APs.
Reporting AP	Displays the numerical value for 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, then perhaps the device is correctly defined as an approved AP.
Last Seen (In Seconds)	Displays the time (in seconds) the approved AP was last seen on the network.
ESSID	Displays the SSID of each approved AP.

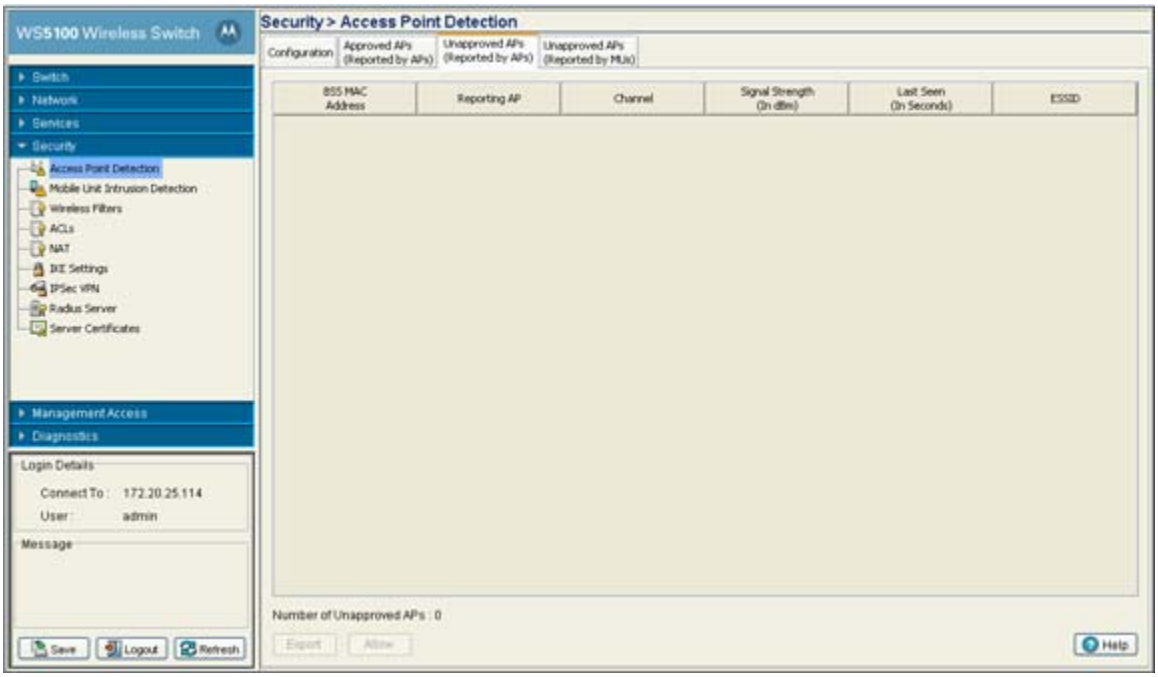
4. The **Number of Approved APs** is simply the sum of all of approved access point MAC Addresses detected.
5. Click on the **Export** button to export the contents of the table to a Comma Separated Values file (CSV).

6.2.3 Unapproved APs (Reported by APs)

Use the **Unapproved APs (Reported by APs)** tab to review access points detected by associated switch access port radios that have been 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 (Reported by APs)** tab.



3. The **Unapproved APs (Reported by APs)** 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 to a new Allowed AP index.
Reporting AP	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 (in 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 (in 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 MAC address is listed incorrectly, highlight the Radio MAC Address and click the **Allow** button.

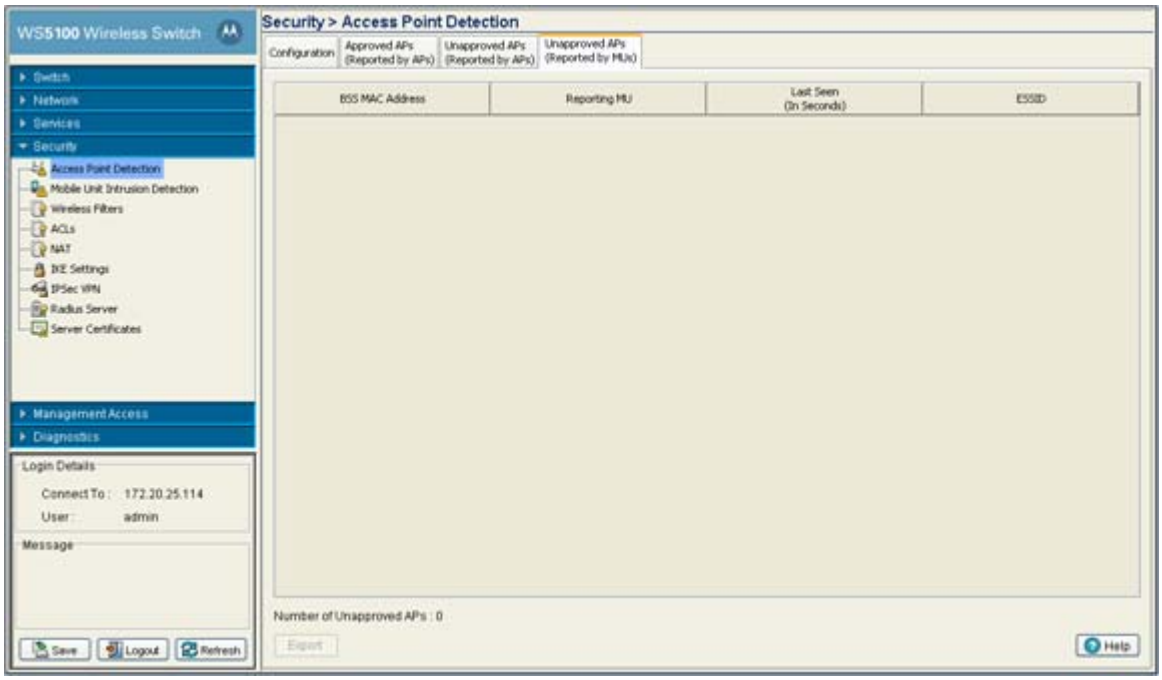
   Assign an Index and complete the required device address information to move the device into the list of approved access point MAC addresses. The number of Unapproved APs updates accordingly as devices are added and removed.
6. Click the **Export** button to export the contents of the table to a Comma Separated Values file (CSV).

6.2.4 Unapproved APs (Reported by MUs)

Use the **Unapproved APs (Reported by MUs)** tab to review unapproved access points detected by associated MUs. The criteria for switch restriction was defined using the **Security** > **Access Port Intrusion Detection** > **Configuration** screen, using the values defined within the **MU Assisted Scan** field.

To view MU detected unapproved access points:

1. Select **Security** > **Access Port Intrusion Detection** from the main menu tree.
2. Click on the **Unapproved APs (Reported by MUs)** tab.



3. The **Unapproved APs (Reported by MUs)** 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 (In 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).

6.3 MU Intrusion Detection

Unauthorized attempts to access the switch managed LAN by MUs is a significant threat to the network. The switch can protect against threats from MUs trying to find network vulnerabilities. Basic forms of this behavior can be monitored and reported.

Use the **Mobile Unit Intrusion Detection** sub-menu to view and configure MU intrusion related information. The Mobile Unit Intrusion Detection screen consists of the following tabs:

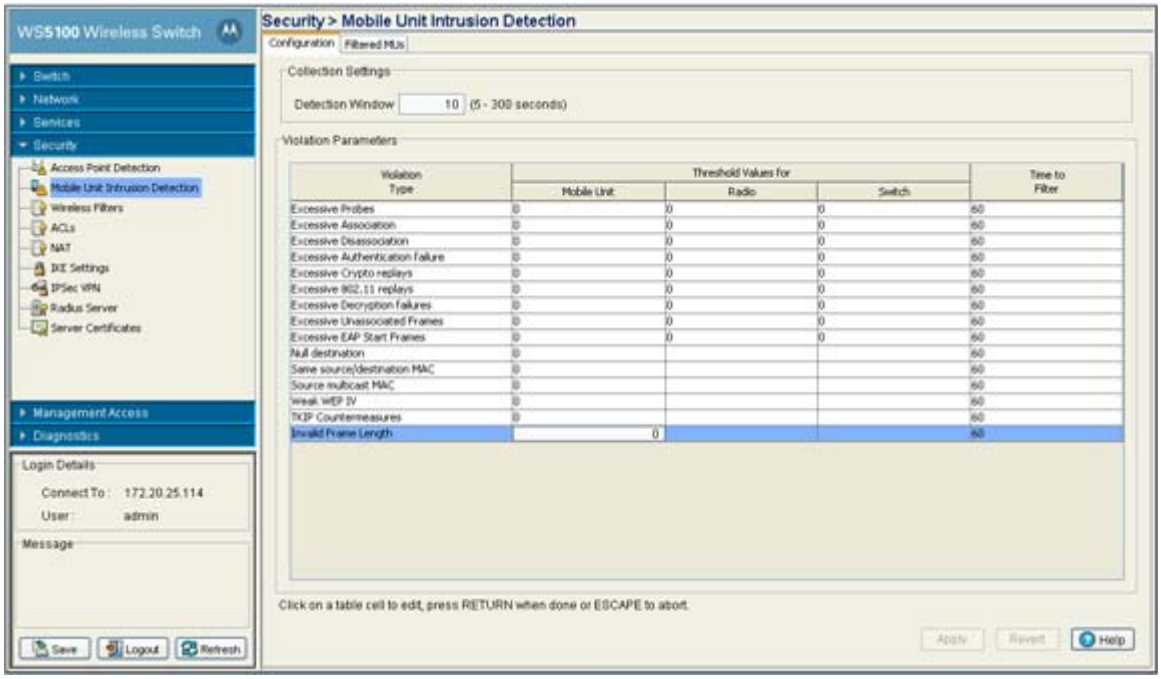
- *Configuring MU Intrusion Detection*
- *Viewing Filtered MUs*

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 mobile unit, 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. Set the values appropriately in respect to the number of MUs within the switch managed network and how often they will be associating/disassociating, and having their authentication and encryption credentials verified.
Radio	Set the radio threshold value for each violation type. If exceeded, the MU will be filtered and displayed within the Filtered MUs screen.
Switch	Set the switch's threshold value for each violation type. If exceeded, the offending MU will be filtered (from the switch) and displayed within the Filtered MUs screen.
Time to Filter	Set the Time to Filter interval (in seconds) the switch uses to filter out MUs that have been defined as committing a violation. Refer to *Viewing Filtered MUs on page 6-11* to review the contents of the MUs that have been filtered thus far.

CAUTION: Setting mobile unit threshold values too low can jeopardize MU performance or break the MU's connection.

5. Click on **Apply** button to save the configuration.

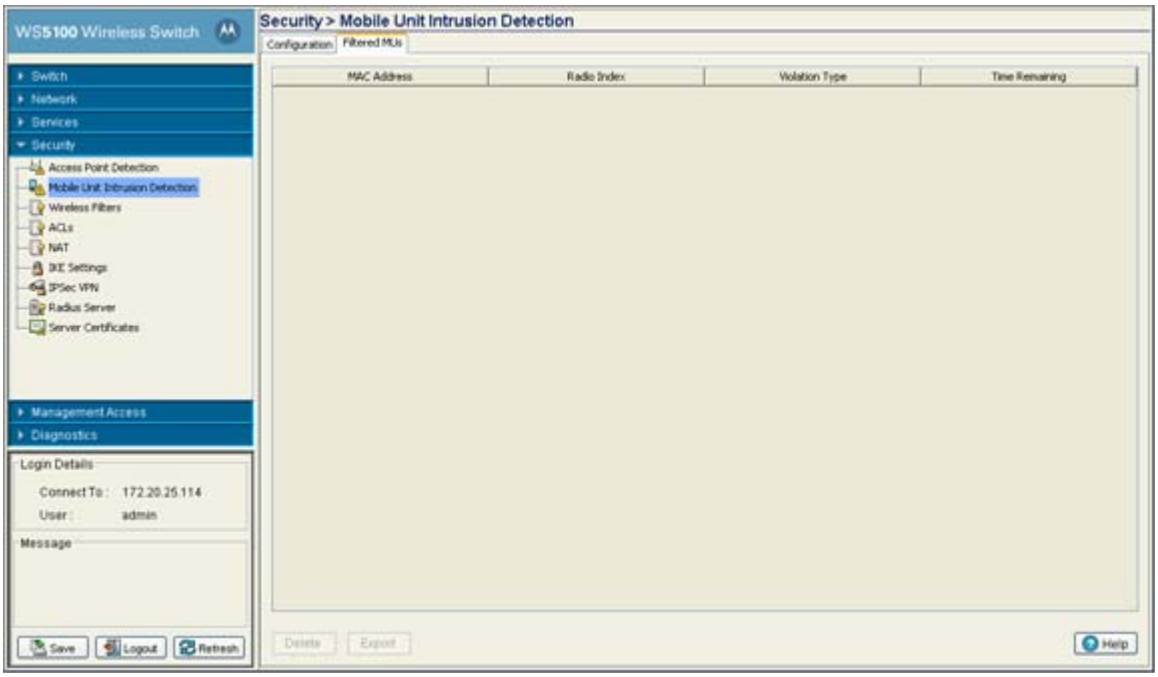
6. Click on **Revert** to rollback to the previous configuration.

6.3.2 Viewing Filtered MUs

Periodically check the **Filtered MUs** tab to review those MUs that have been 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. The following violation types are possible: • excessive probes • excessive associations • excessive disassocs • 802.11 replay failures • crypto replay failures • decryption failures • authentication failures • all 0's address • same source-dest address • multicast source address • use of weak WEP IV • TKIP countermeasures • excessive EAP/802.1x frames Use the Violation Type to discern whether the detested MU is truly a threat on the switch managed network (and must be removed) or can be interpreted as a non threat.
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.

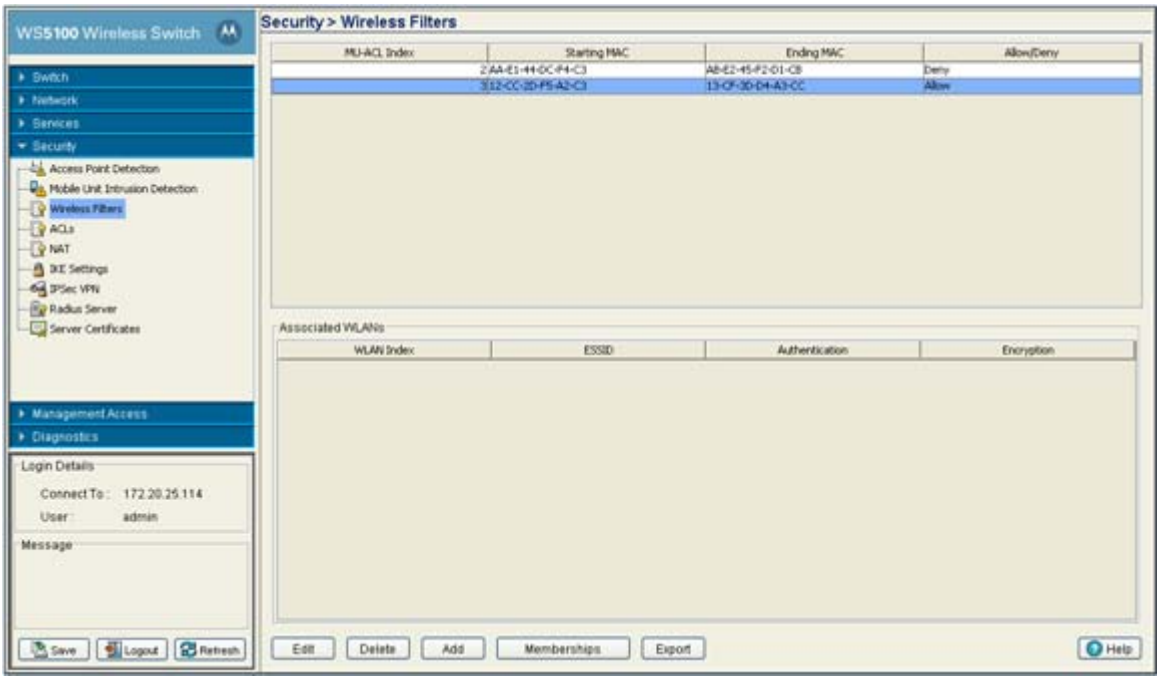
3. Select a detected MU and click the **Delete** button to remove it from the list of MUs you are tracking as potential threats within the switch managed network.

6.4 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 Filters** from the main menu tree.
2. The **Wireless Filters** tab is divided into 2 fields:
   - Filters
   - Associated WLANs



The **Filters** field 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.
Allow/Deny	States whether this particular ACL Index and MAC address range has been allowed or denied access to the switch managed network.

3. Refer to the **Associated WLANs** field for following

WLAN Index	Highlight an Index to display the name(s) of the WLANs currently associated with this particular Index. Click the **Membership** button to map available WLANs to this filter.
ESSID	Displays the SSID required by the devices comprising this WLAN.
Authentication	Displays the authentication scheme configured for the devices comprising this WLAN.
Encryption	Displays the encryption method configured for the devices comprising this WLAN.

4. If the properties of an existing filter are close 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 6-14*.
5. If an existing filter is now obsolete, select it from those listed and click the **Delete** button.
6. Click the **Add** button to create a new filter. For more information, see *Adding a new Wireless Filter on page 6-15*.

7. 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 WLAN on page 6-16*
8. Click on the **Export** button to export the contents of the table to a *Comma Separated Values* file (CSV).

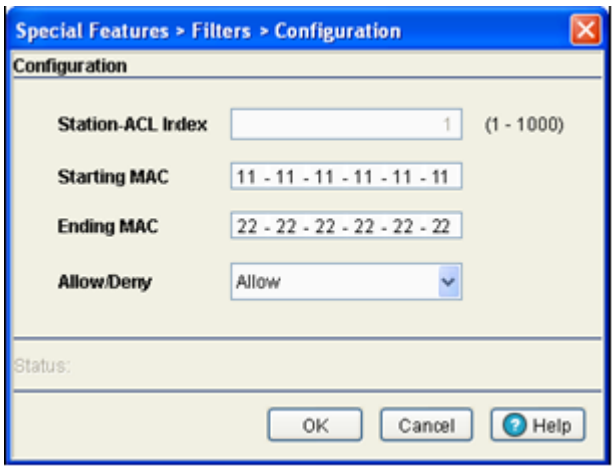
6.4.1 Editing an Existing Wireless Filter

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 **Special Features> Filters** from the main menu tree.
2. Select one of the existing ACLs from the filters list.
3. Click the **Edit** button at the bottom of the screen to launch a new dialogue used for editing an ACL.

   Within the screen 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.



4. The **Station-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.
5. 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.
6. 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.
7. Use the drop-down menu to select **Allow** or **Deny**.

   This rule applies to the 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.
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.

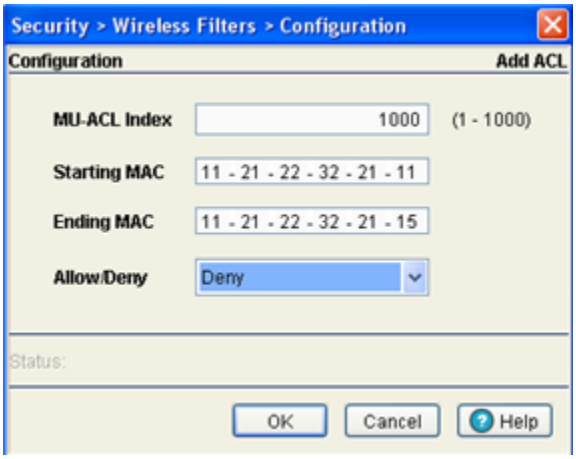
6.4.2 Adding a new Wireless Filter

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 Filters** from the main menu tree.
2. Click the **Add** button at the bottom of the screen to launch a new dialogue used for creating an ACL.

   Define an Index (numerical identifier) for the ACL and starting an ending MAC address range for the devices allowed or denied access to the switch managed network.



3. 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.

4. 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.

5. 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.
6. Use the drop-down menu to select **Allow** or **Deny**.

   This rule applies to the 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.

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.

6.4.3 Associating an ACL with 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 Filters** from the main menu tree.
2. Select one or more of the existing ACLs from the filters list.
3. Click the **Memberships** button.
4. Check the box below 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.
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.

6.5 Configuring ACLs

An *Access Control List* (ACL) is a sequential collection of permit and deny conditions that apply to switch data 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, then the packet is dropped.

Use the **ACL** 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 access rights for a user in relationship to the switch. When access is attempted, the operating system uses the ACL to determine whether the user has switch access permissions. It consists of the following tabs:

- *Configuring an ACL*
- *Attaching an ACL*
- *Attaching an ACL on a WLAN Interface/Port*
- *Reviewing ACL Statistics*

NOTE: For an overview of how the switch uses an ACL to filter permissions to the switch managed network, proceed to *ACL Overview on page 6-17*.

6.5.1 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 L2 ports.

For more information, see

- *Router ACLs*
- *Port ACLs*
- *Wireless LAN ACLs*
- *ACL Actions*
- *Precedence Order*

6.5.1.1 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 that gets routed through the switch. Whenever a packet is received from a Layer 3 interface, it is examined against all the 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 decide whether to accept it 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 the following:

- 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 can not 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

6.5.1.2 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–source and destination port 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 not stateful as compared to Router ACLs. Hence, it matches every packet against the configured ACL rules and takes action as defined by the ACL rules. 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.

6.5.1.3 Wireless LAN ACLs

Wireless LAN ACLs filter/mark packets based on the wireless LAN from which they arrive rather than filtering the packets arrived on L2 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 L2 port based ACL rather than a WLAN ACL.

Each WLAN is assumed to be a virtual L2 port. Configure one IP and one MAC ACL on the virtual WLAN port. In contrast to L2 ACLs, a WLAN ACL can be enforced on both the Inbound and Outbound direction.

6.5.1.4 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 matching criteria. The following types of actions are supported.

- deny— Instructs the ACL not to allow a packet to go to its destination.
- permit—Instructs the ACL to allows a packet to go to its destination.
- mark—Modifies certain fields inside the packet and then permits them. Hence mark is an action with an implicit permit.

NOTE: Only a Port ACL supports the mark action. For Router ACLs, the mark action is treated as a permit action and the packet is allowed without performing any modifications.

6.5.1.5 Precedence Order

The rules within an ACL are applied to packets based on their precedence values. Every rule has a unique precedence value which can be 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 which is 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 precedence value which is unique and 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 saying Rule with max precedence value exists. Either delete that 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 ascending order of precedence.

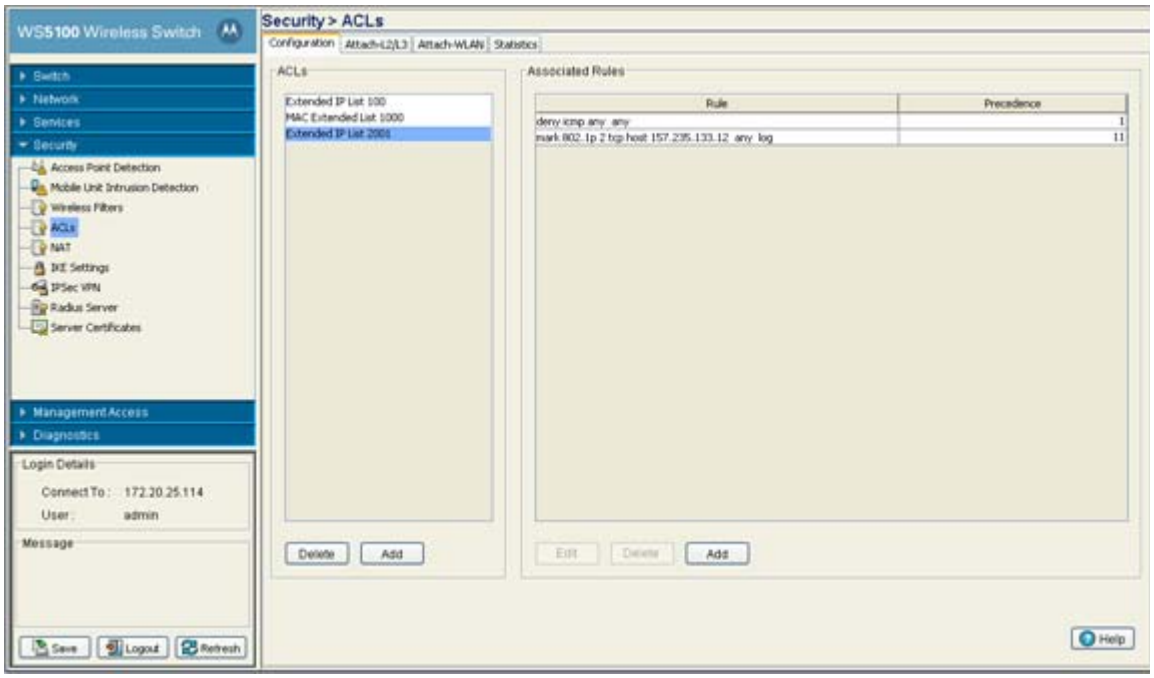
NOTE: ACEs with lower precedence are always applied first to packets. Hence, it is advised to add more specific entries in the ACL first then the general ones. While displaying the ACL, the entries are displayed in ascending order of precedence.

6.5.2 Configuring an ACL

Configure an ACL to enforce privilege separation and determine appropriate switch access permissions for groups and users.

To configure an ACL:

1. Select **Security** > **ACLs** from the main tree menu.
2. Click the **Configuration** tab.
3. 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 in order to match the ACE. Because the switch stops testing conditions after the first match, the order of conditions in the list is critical.

4. If an existing ACL no longer satisfies switch access control requirements, select it from amongst the existing ACLs and click the **Delete** button.
5. Use the **Add** button (within the ACLs field) to add an additional ACL. For more information, see *Adding a New ACL on page 6-20*.
6. 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 6-21*.

6.5.2.1 Adding a New ACL

When a packet is received by the switch, the switch compares the packet against the ACL to verify t the packet has the required permissions to be forwarded. Often, ACLs need to be added as client permissions change during switch operation.

To create a new ACL:

1. Select **Security** > **ACLs** from the main menu tree.
2. Click on the **Configuration t**ab to view the list of ACLs currently associated with the switch.
3. Click on the **Add** button.

4. 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 type information for matching operations
   - MAC Extended List – Uses source and destination MAC addresses, VLAN ID and optional protocol type information.
5. Enter a numeric index name for the ACL in the **ACL ID** field.
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.

6.5.2.2 Adding a New ACL Rule

To add a new rule:

1. Select **Security** > **ACLs** from the main menu tree.
2. Click the **Configuration** tab.

3. Click the **Add** button within the Associated Rules field.

4. 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.

---

5. 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.
6. Select the **Logging** checkbox to allow the log messages to be generated when a packet has been forwarded, denied or marked based on the criteria specified in the access lists.
7. If **mark** is selected from within the **Operations** drop-down menu, the **Attribute to mark** field becomes enabled. Select the **802.1p (0 - 7)** or **TOS(0 - 255)** checkbox and define the attribute receiving priority with this ACL mark designation.
8. From within the **Filters** field, select a **Source Wildcard/Mask** from the drop-down menu.

   The source is the source address of the network or host in dotted decimal format. The Source-mask is the network mask.
9. Use the **Source Address** field to enter the IP address from where the packets are sourced.
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.

6.5.2.3 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 the switch.

To modify an existing ACL rule:

1. Select **Security** > **ACLs** from the main menu tree.
2. Click on the **Configuration** tab.
3. Select an ACL from the ACLs field.

   The rules associated with the selected ACL display in the Associated Rules section.
4. Click the **Edit** button within the Associated Rules field.
5. Use the **Precedence** field to modify the 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 (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.
7. Select the **Logging** checkbox to allow the log messages to be generated 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 becomes enabled. If necessary, select the **802.1p (0 - 7)** or **TOS(0 - 255)** checkbox and define the attribute receiving priority with this ACL mark designation.
9. From within the **Filters** field, modify (if necessary) the **Source Wildcard/Mask** from the drop-down menu.

   The source is the source address of the network or host in dotted decimal format. The Source-mask is the network mask.
10. Use the **Source Address** field to edit (if necessary) the IP address from where the packets are sourced.

NOTE: If an Extended IP ACL type is used, a Destination Wildcard/Mask and Destination Address are also required.

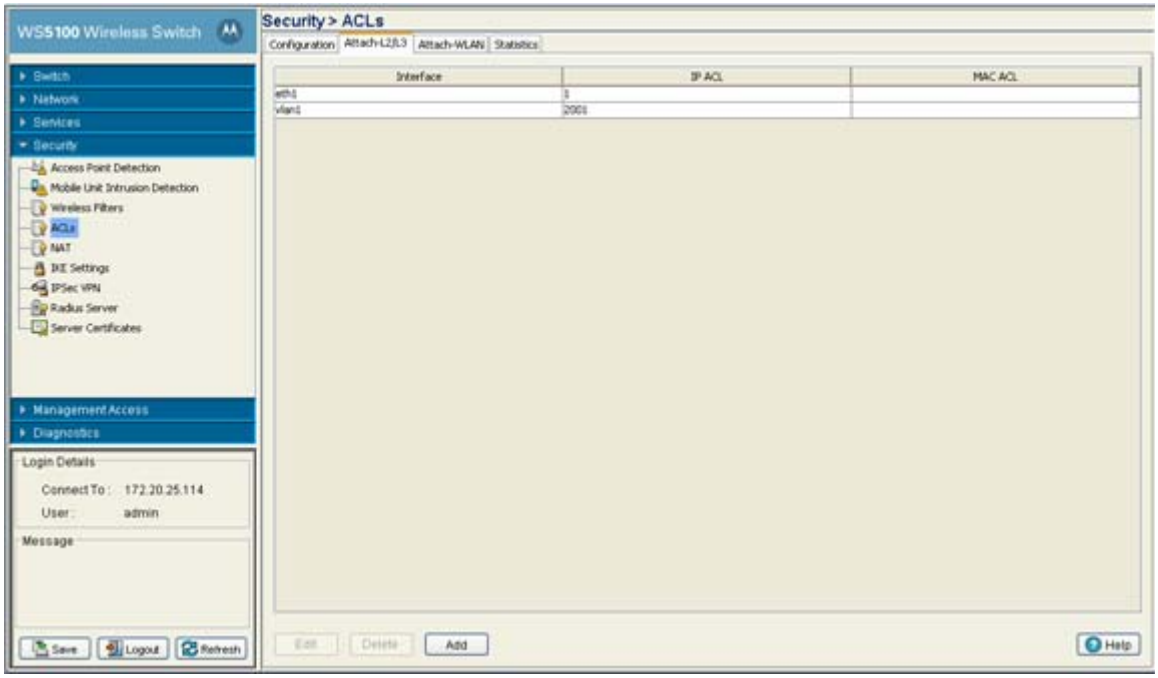
11. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
12. Click **OK** to use the changes to the running configuration and close the dialog.
13. Click **Cancel**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

6.5.3 Attaching an ACL

Use the **Attach-L2/L3** screen to view and assign the ACL to a physical interface or VLAN on the switch.

To attach an interface:

1. Select **Security** > **ACLs** from the main menu tree.
2. Click the **Attach-L2/L3** tab.



3. 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: • eth1 • eth2 • vlan1 (or any additional VLANs that have been created) • tunnel *n* (where *n* equals the name(s) of those tunnels created thus far).
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.

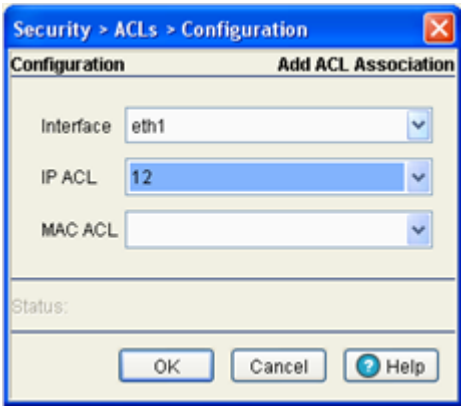
4. Select an interface and click on **Edit** to modify the ACL interface, IP ACL and MAC ACL values.
5. Select an interface and click the **Delete** button to delete the interface configuration from the switch.
6. Click on **Add** button to add an physical or VLAN interface to the switch. For more information, see *Adding a New ACL Configuration on page 6-24*.

6.5.3.1 Adding a New ACL Configuration

After creating an ACL, it can be applied to one or more interfaces. On a Layer 3 interface it can be applied in either an outbound or inbound direction, and only in inbound direction on a Layer 2 interface. To add an ACL interface to the switch:

1. Select **Security** > **ACLs** from the main menu tree.

2. Click on the **Attach** tab.
3. Click on the **Add** button.



4. Use the **Interface** drop-down menu to select the interface to configure on the switch. Available options include – Ethernet 1, Ethernet 2, VLAN 1 (plus those VLANs created thus far) and Tunnel *n* (where *n* equals the name(s) of those tunnels created thus far).
5. 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.
6. Use the **MAC ACL** drop-down menu to select an MAC ACL used as the MAC IP for the layer 2 interface.
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.

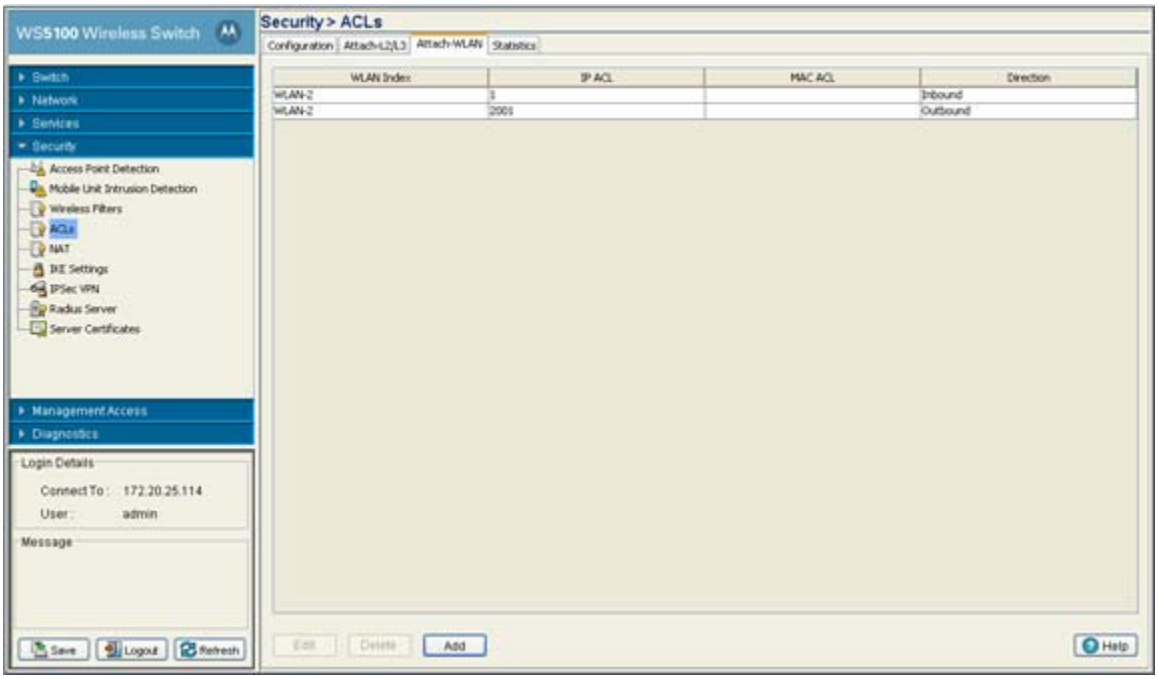
6.5.4 Attaching an ACL on a WLAN Interface/Port

Use the Attach- WLAN tab to view and assign an ACL to a WLAN on the switch. By default, arp is not supported. Create a MAC ACL to allow arp on the switch.

NOTE: WLAN based ACLs allows users to enforce rules/ACLs on both the inbound and outbound direction, as opposed to L2 ACLs, which just support the inbound direction.

To configure a WLAN ACL:

1. Select **Security** > **ACLs** from the main menu tree.
2. Click the **Attach-WLAN** tab.



3. Refer to the following information as displayed within the Attach -WLAN tab:

WLAN Index	The 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 the inbound or outbound direction.

4. Select a WLAN (by row) and click **Edit** to modify the WLAN Index, IP ACL and MAC ACL values.
5. Select a row and click the **Delete** button to delete the ACL from the list available (but not from the switch).
6. Click the **Add** button to add an ACL to a WLAN interface. For more information, see *Adding a New ACL WLAN Configuration on page 6-26*.

6.5.4.1 Adding 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 > ACLs from the main menu tree.
2. Click on the **Attach - WLAN** tab.
3. Click the **Add** button.

4. Define a **WLAN Index** between 1 and 32.
5. Use the **IP ACL** drop-down menu to select an IP ACL to configure for the WLAN interface.
6. Use the **MAC ACL** drop-down menu to select the MAC ACL to configure for the WLAN interface.
7. Select either the **Inbound** or **Outbound** radio button to define which direction the ACL applies.

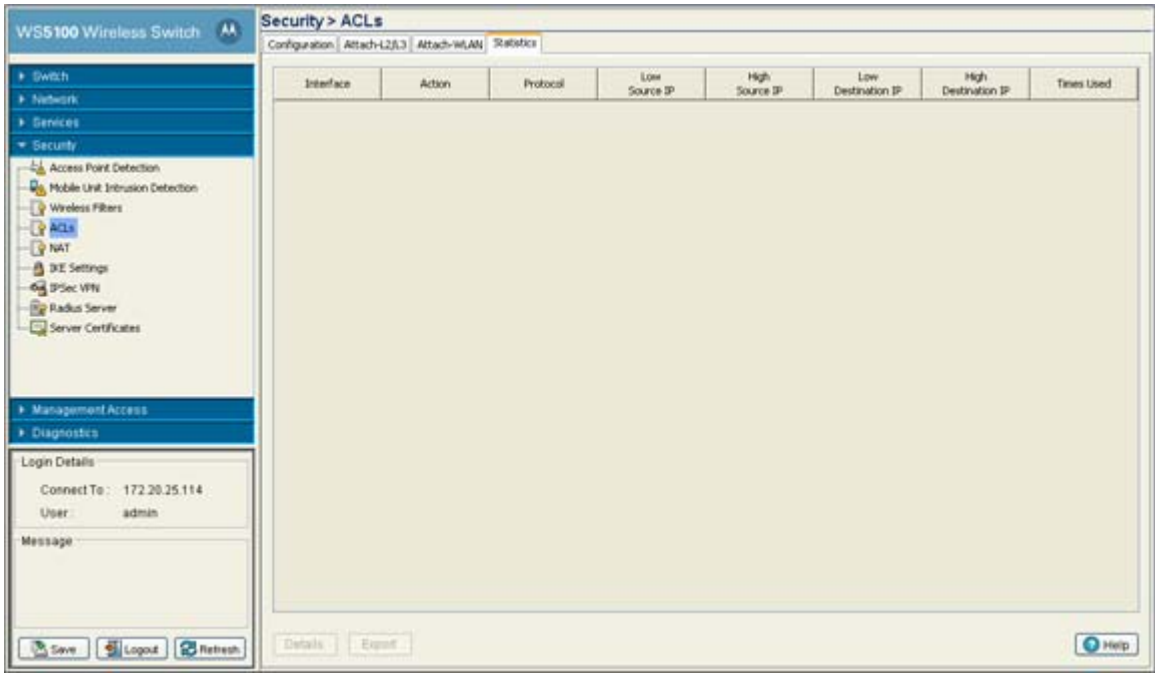
8. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
9. Click **OK** to use the changes to the running configuration and close the dialog.
10. Click **Cancel**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

6.5.5 Reviewing ACL Statistics

Use the **Statistics** screen to view set of statistics for those ACLs defined for use with the switch.

To review ACL statistics:

1. Select **Security** > **ACLs** from the main menu tree.
2. Click the **Statistics** tab.



3. Refer to the following information as displayed within the **Statistics** tab:

Interface	Displays the Ethernet 1, Ethernet 2 or VLAN 1 interface 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 protocol used with the ACL. Options available to the switch include icmp, ip, tcp and udp.
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.
Times Used	Displays the number of instances this ACL has been used. Periodically review this among ACLs to determine whether specific ACLs should be deleted or modified to make relevant.

4. Select an interface and click the **Delete** button to delete the ACL interface from the switch.
5. Click the **Export** to export the selected ACL attribute to a user specified location.

6.6 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 the private network, while the other is the 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 that is located on one of the LAN subnets but does not want to permit any other access, NAT is the appropriate solution.

NAT operates on the switch to connect two networks together. An inside network is addressed with 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 activities:

- *Defining Dynamic NAT Translations*
- *Defining Static NAT Translations*
- *Configuring NAT Interfaces*
- *Viewing NAT Status*

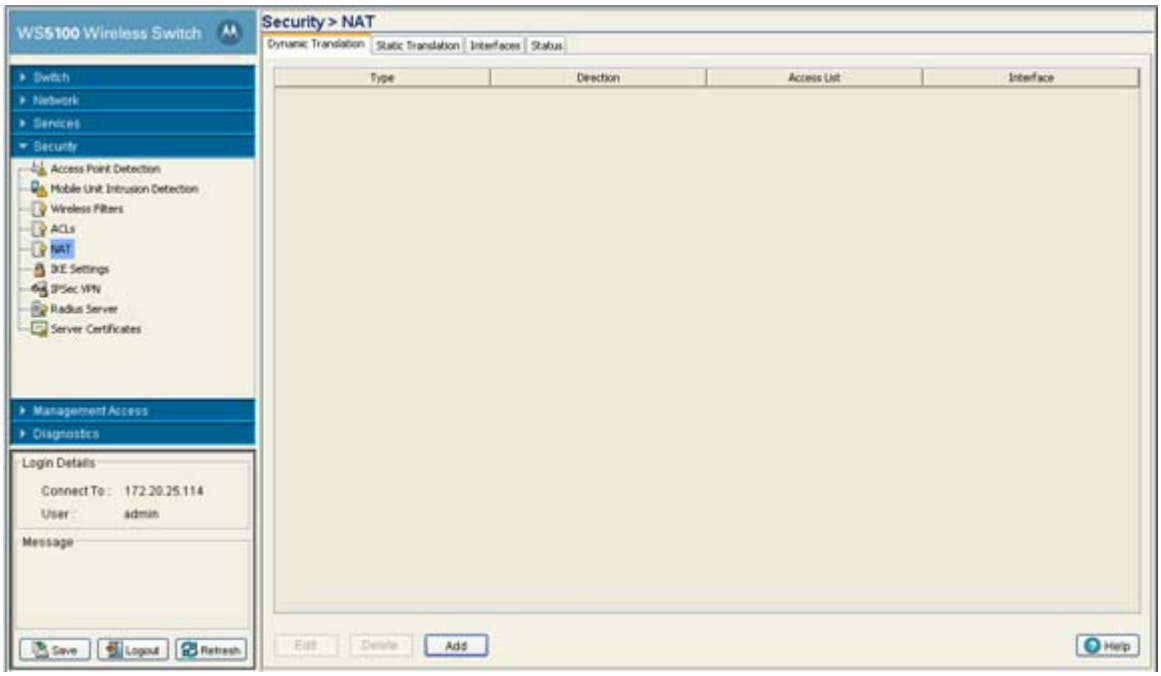
6.6.1 Defining Dynamic NAT Translations

The switch Dynamic NAT functionality creates active translation entries when a packet crosses from an IP NAT inside interface to an IP NAT outside interface, or vice versa. Dynamic NAT requires packets to be switched through the NAT router to generate translations in the switch's 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 coming in on interfaces marked as inside. These switch interfaces should be private networks which are 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 which are accessible from anywhere on the Internet.
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 in order 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 Standard IP and Extended IP Access List can be used.
Interface	Defines the interface through which packets get 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 display screen used 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.

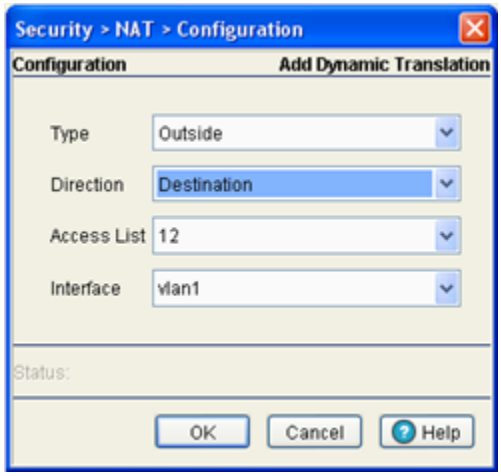
6. Click the **Add** button to display screen to create a new NAT configuration and add it to the list of available configurations. For more information, see *Adding a New Dynamic NAT Configuration on page 6-30*.

6.6.1.1 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 that are 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 to be used during the NAT translation process. 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 best represents the intended network traffic within the NAT supported configuration. vlan1 is available by default.
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.

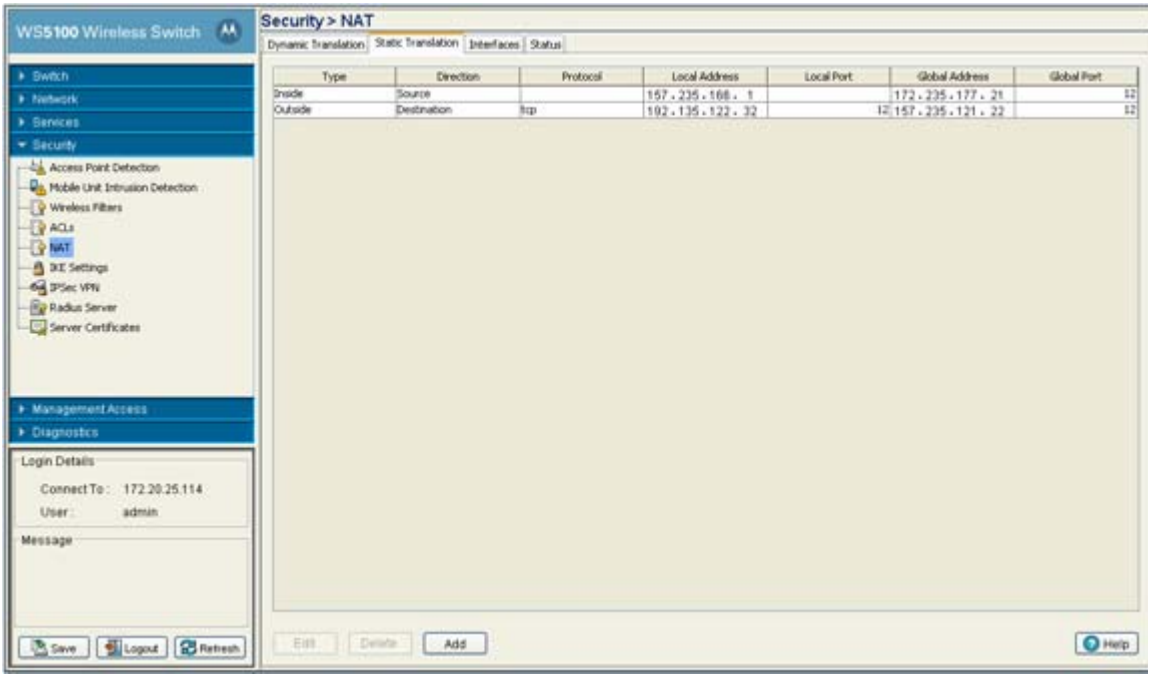
6.6.2 Defining Static NAT Translations

Static *Network Address Translation* (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 thus 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 that are 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.
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 in order to reach the LAN over the switch managed network.
Protocol	Displays the tcp or udp option selected for use with the static translation.
Local Address	Displays the Local Address used at the local (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**.
Global Address	Modifies the IP address of the matching packet to the specified value. The IP address to be 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 used 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 6-30*.

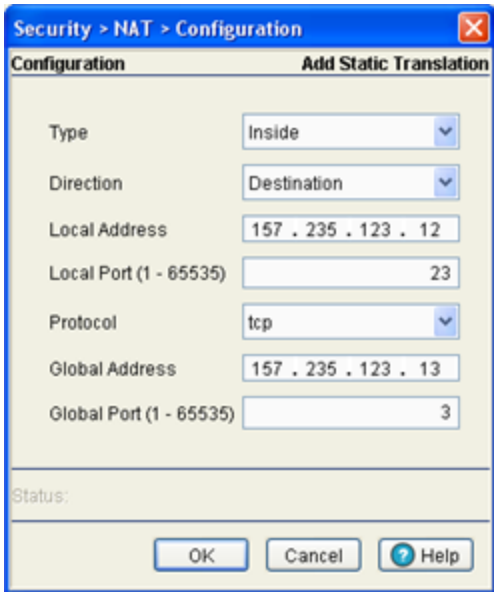
6.6.2.1 Adding a New Static NAT Configuration

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 **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 that are 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. Enter the **Local 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 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.

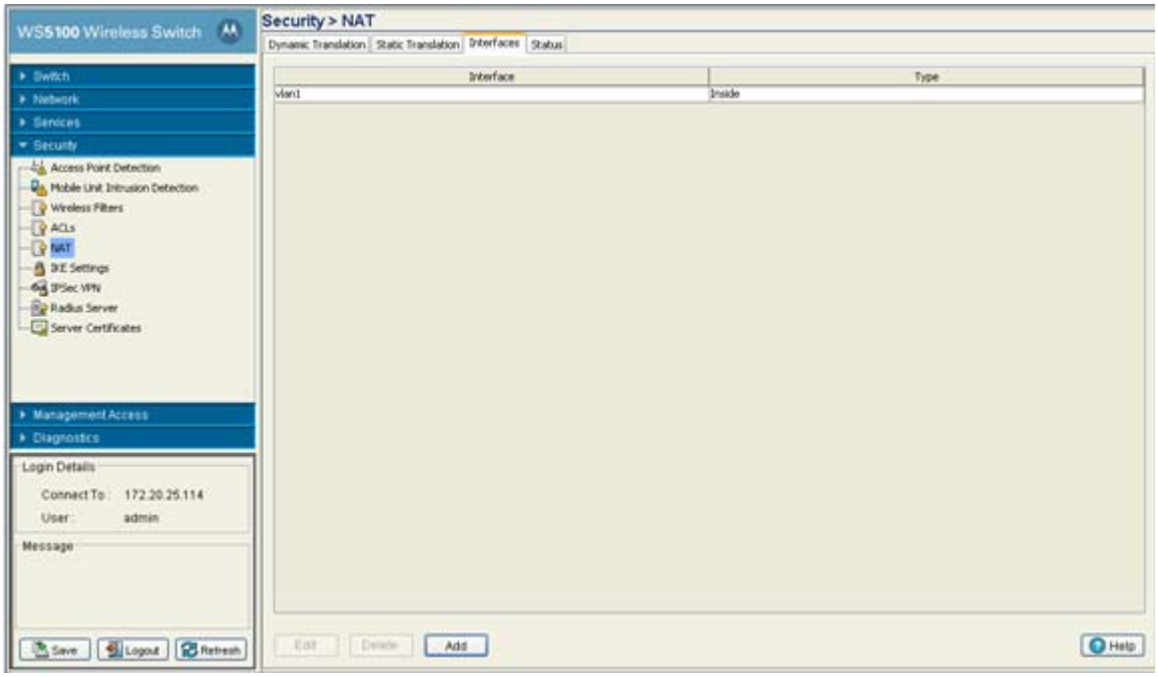
13.Click **Cancel** to close the dialog without committing updates to the running configuration.

6.6.3 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 you may have 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 particular 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.

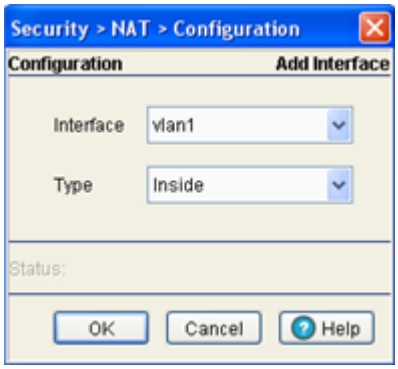
4. To Edit an existing interface, select it from the list of available interfaces and click the **Edit** button.

   An Edit Interface screen displays allowing the user to modify the VLAN and interface type (inside or outside) used.

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:

   d. 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.

   e. 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.

   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.

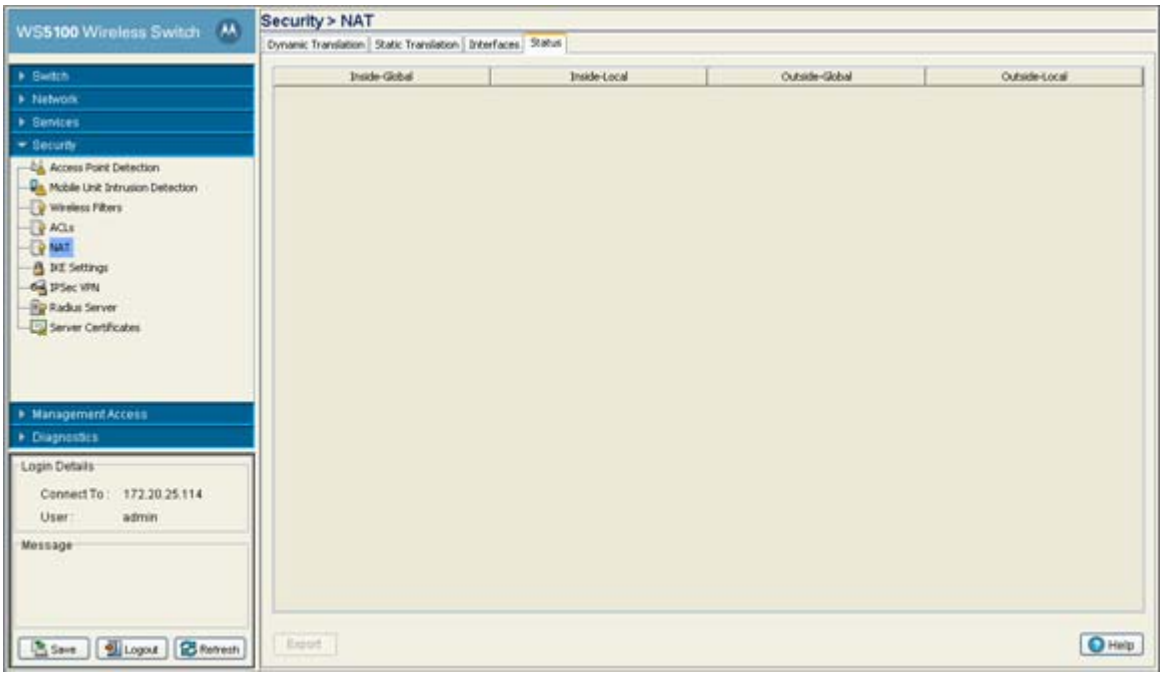
   h. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.6.4 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 information 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).

6.7 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 for the parties.

The switch IKE configuration process is decided into the following activities:

- *Defining the IKE Configuration*
- *Setting IKE Policies*
- *Viewing SA Statistics*

NOTE: By default, the IKE feature is enabled on the switch. Motorola does not support disabling the IKE server.

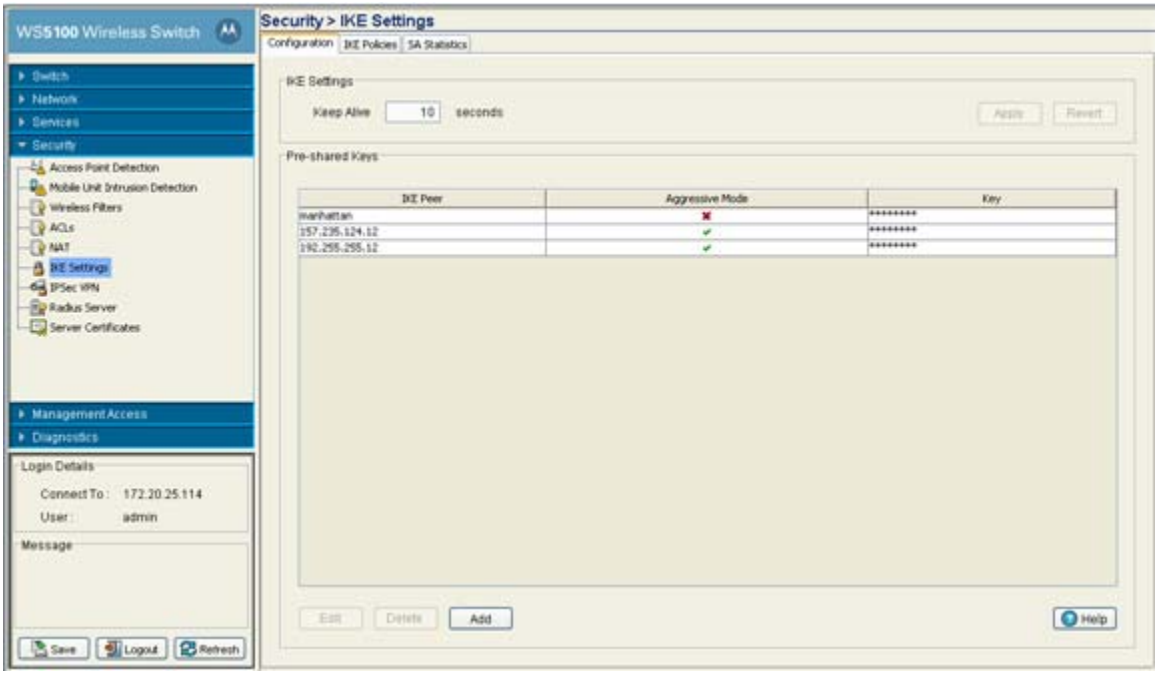
6.7.1 Defining the IKE Configuration

Refer to the **Configuration** tab to enable (or disable) IKE and define the IKE identity (for exchanging identities) and aggressive mode. Aggressive mode enables you to configure *Internet Key Exchange* (IKE) pre-shared keys as IPSec tunnel attributes for IP Security (IPSec) peers.

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 and stored on the Radius server. 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.



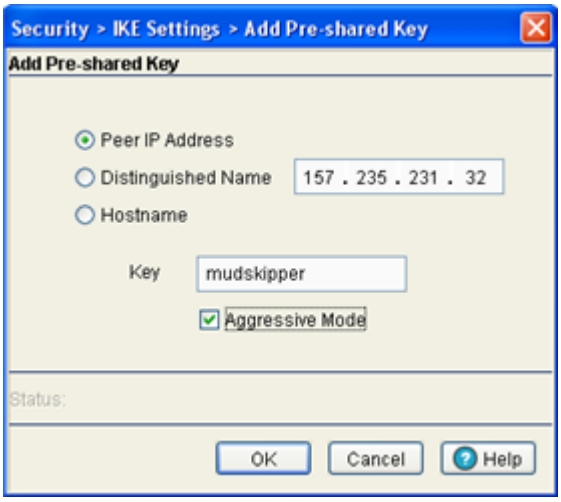
During IKE negotiations, peers must identify themselves to one another. Thus, the configuration you define is the identification medium for device recognition.

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 to the peer. The client notifies you when the peer is no longer present.
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:

Peer IP Address	Use the Peer IP 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.

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 within the table.
9. If the properties of an existing peer IP address, key and aggressive mode designation are no longer relevant and cannot be edited to be useful, 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 *Internet Key Exchange* (IKE) pre-shared keys as Radius tunnel attributes for IP Security (IPSec) peers.

   d. 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.

   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.

6.7.2 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, including the following:

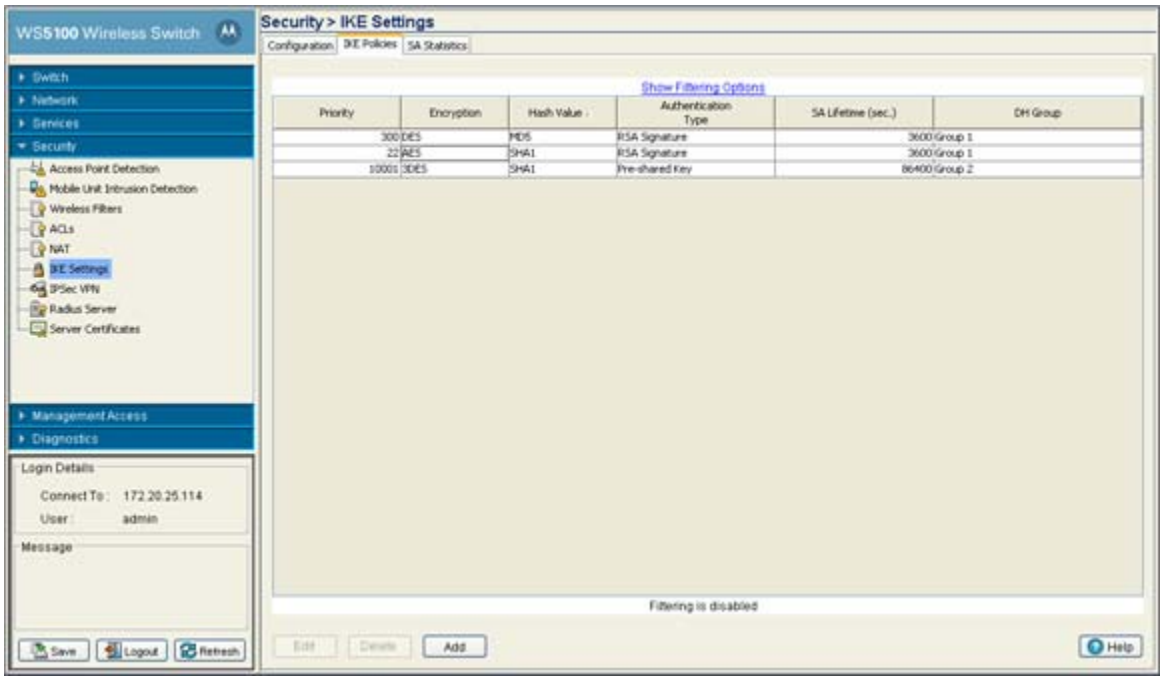
- A priority value (1 through 65,543, with 1 as highest priority permitted)
- An authentication scheme ensure the credentials of the peers
- An encryption scheme protecting the data
- A HMAC method ensuring the identity of the sender, and validating that the message has not been altered
- A Diffie-Hellman 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 (always set to the lowest priority) and contains the default values. When IKE negotiations start, 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 policies match 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.

Priority	Displays the priority for the IKE policy. The available range is from 1 to 65,543, with 1 being the highest priority value.
Encryption	Displays the encryption method protecting data transmitted between peers. Options include: • DES. 56-bit DES-CBC is less secure but faster than the alternatives. 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	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.

4. Highlight an existing policy and click the **Edit** button to revise the policy's existing priority, encryption scheme, hash value, authentication scheme, SA lifetime and DH group.
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:

Priority — Define the priority for the IKE policy. The available range is from 1 to 65,543, 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 is less secure but faster than the alternatives. 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 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 — 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 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.

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

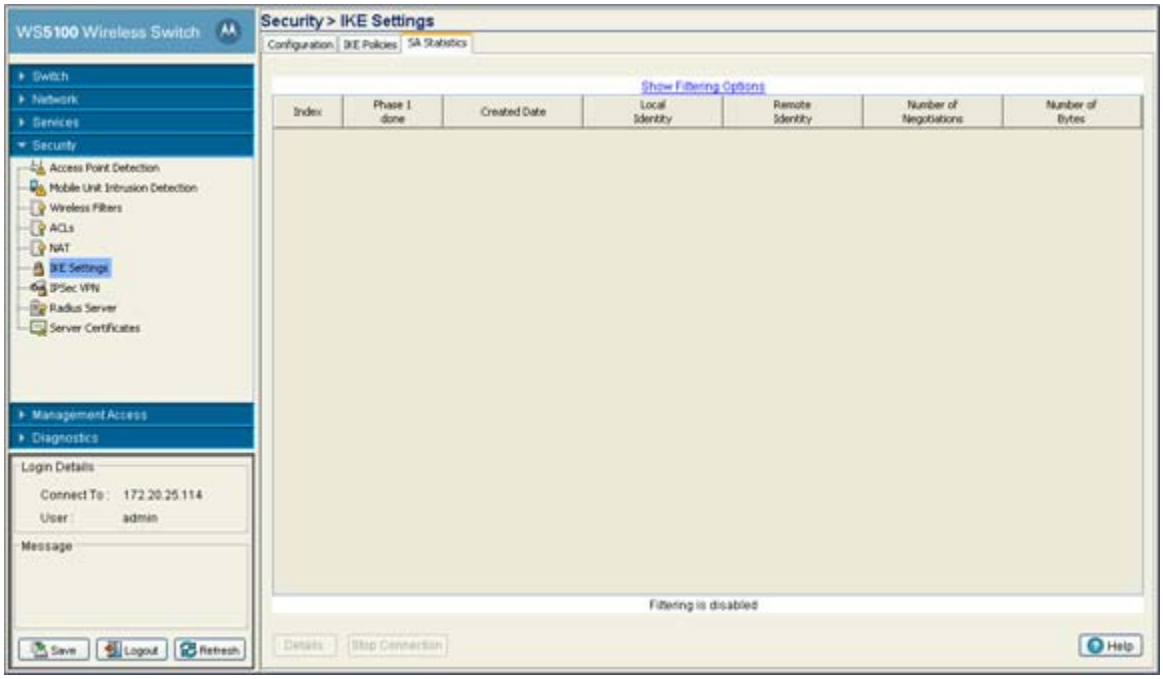
d. Click **Cancel** to close the dialog without committing updates to the running configuration.

6.7.3 Viewing SA Statistics

A *security association* (SA) is a description of how two peers employ a security technique 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:

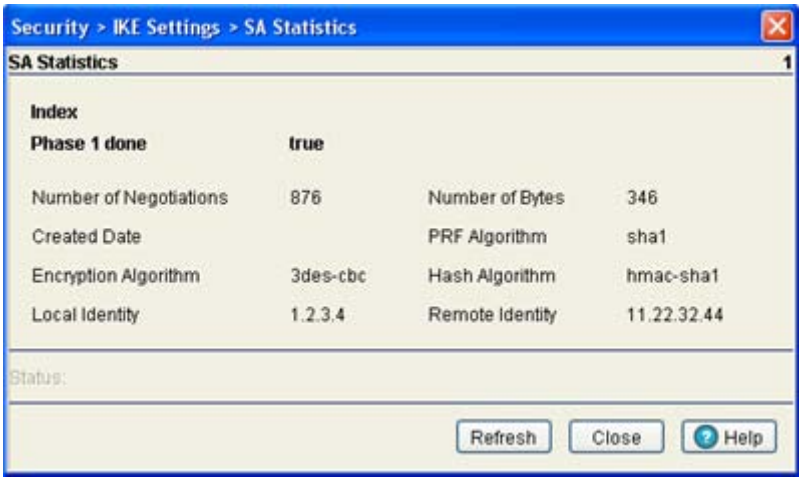
1. Select **Security** > **IKE Settings** from the main menu tree.
2. Click the **SA Statistics** tab.



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 exchange 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 use to identify itself to the remote peer.
Remote Identity	Specifies the address the remote IKE peer use 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.

6.8 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 these secure tunnels, and what should be used to protect these sensitive packets. Once configured, an IPsec peer creates the appropriate 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 which can be 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 give public IP address*

  An IPSec client needs to have an IP address before it can connect to the VPN Server and create an IPSec tunnel. Thus, 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. Permits *Certification Authority* (CA) support for a manageable, scalable IPSec implementation. Allows dynamic authentication of peers. If you do not want IKE to be used with your IPSec implementation, you can disable it for IPSec peers. You cannot have a mix of IKE-enabled and IKE-disabled peers within your IPSec network. Manually specify IPSec session keys.

- *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, so 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, so 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, you can specify lists (such as lists of acceptable transforms) within the Crypto Map entry.

- *Apply Crypto Map sets to Interfaces*

  You must 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 to 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 use of new sequence numbers and reassigning the Crypto Map does not tear down existing connections. With the WS5100 switch, a Crypto Map cannot get applied to more than one interface at a time.

- *Monitor and maintain IPSec tunnels*

  New configuration changes will only take effect when negotiating subsequent security associations. If you want the new settings to take immediate effect, you must clear the existing security associations so that 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.

  For more information on configuring IPSec VPN, refer to the following:

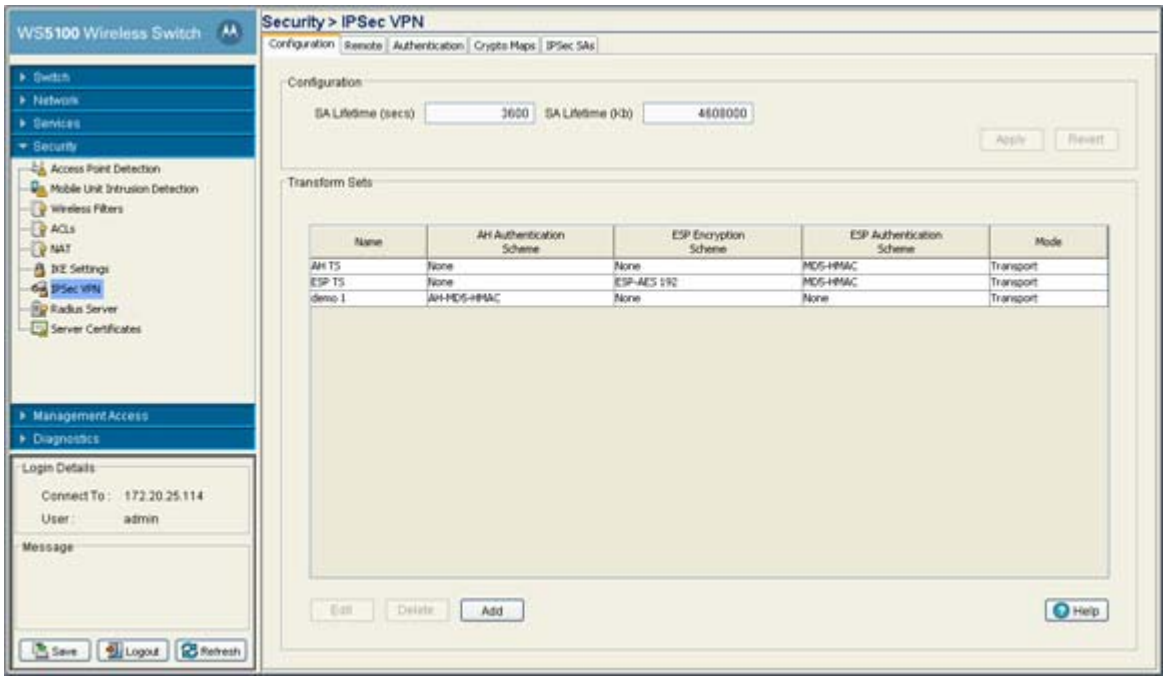
  - *Defining the IPSec Configuration*
  - *Defining the IPSec VPN Remote Configuration*
  - *Configuring IPSEC VPN Authentication*
  - *Configuring Crypto Maps*

- *Viewing IPSec Security Associations*

6.8.1 Defining the IPSec Configuration

Use the IPSec VPN Configuration screen to view the attributes of existing VPN tunnels and modify the security association lifetime and keep alive intervals used to maintain the routes between VPN peers. From the Configuration screen, 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 information.

SA Lifetime (secs)	For IKE based security associations, define a SA Lifetime (in seconds) forcing the periodically 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 a IPSec VPN transform set (by its index) and click the **Edit** button to modify its properties.
6. s only recommended if the existing index is no longer relevant in its current state. For more information, see *Editing an Existing Transform Set on page 6-46*.
7. Select an index and click the **Delete** button to remove it from the table.
8. If none of the transform sets displayed appear useful, click on the Add button to create a new one. For more information, see *Adding a New Transform Set on page 6-47*.

6.8.1.1 Editing an Existing Transform Set

If the attributes of an existing transform set no longer lend themselves as 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 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.

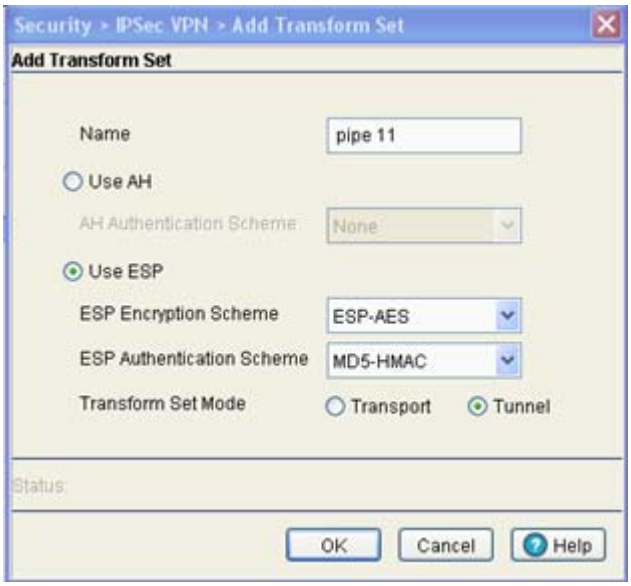
6.8.1.2 Adding a New Transform Set

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 as 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.

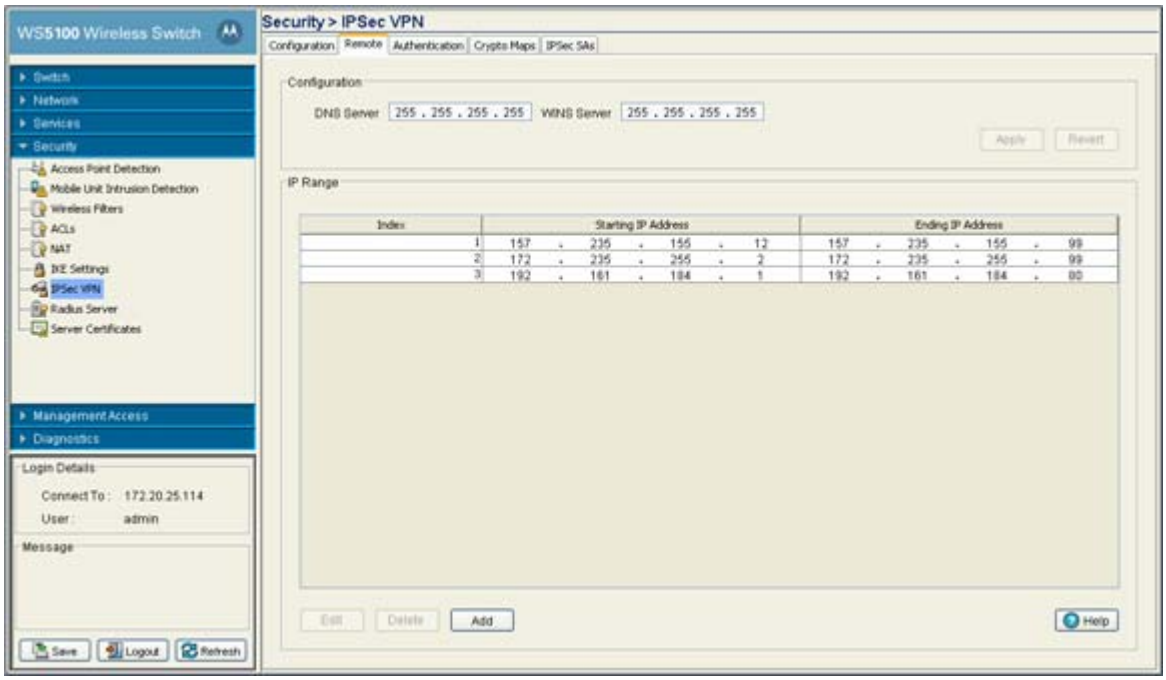
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch.
6. Click **OK** to use the changes to the running configuration and close the dialog.
7. Click **Cancel**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

6.8.2 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 is also used for defining the IP address range used within the IPSec VPN tunnel and configuring the user authentication scheme for user permissions within the IPSec VPN tunnel.

To define the IPSEc VPN 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 information.

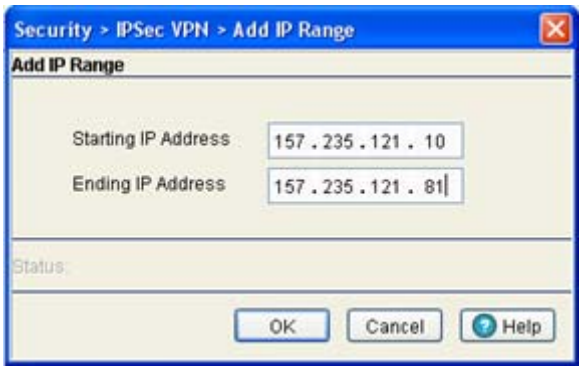
DNS Server	Enter the numerical IP address of the DNS Server used to route information to the remote destination of the IPSec VPN.
WINS Server	Enter the numerical IP address of the WINS Server used to route information to the remote destination of the IPSec VPN.
Apply	Click **Apply** to save any updates 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. Click the **IP Range** tab to view the following information.

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, then 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, then 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 specific 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.



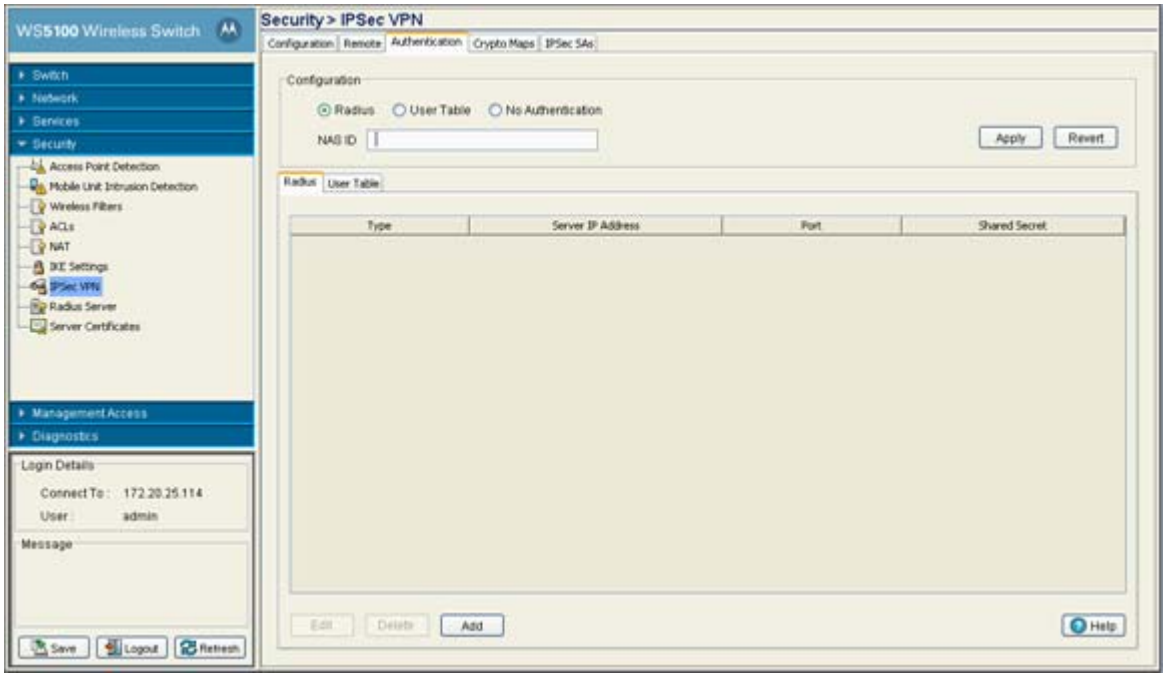
6.8.3 Configuring IPSEC VPN Authentication

If IKE is not used for establishing security associations, there is no negotiation of security associations, so the configuration information in both systems must be the same for traffic to be processed successfully by IPSec. 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. Click the **Authentication** tab.



3. Define whether the 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 physical *network access server* (NAS) port connected. Every profile contains a profile 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.

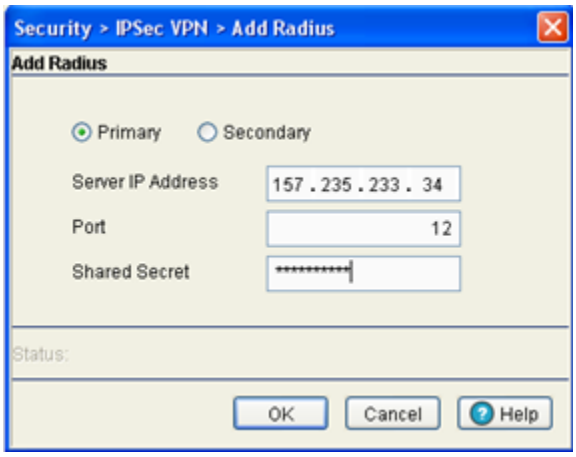
5. If the **Radius Server** radio button was selected, the following server information displays when the Radius tab is selected:

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 389.
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 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 for the remote VPN connection. 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 **User Table** 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 the 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.

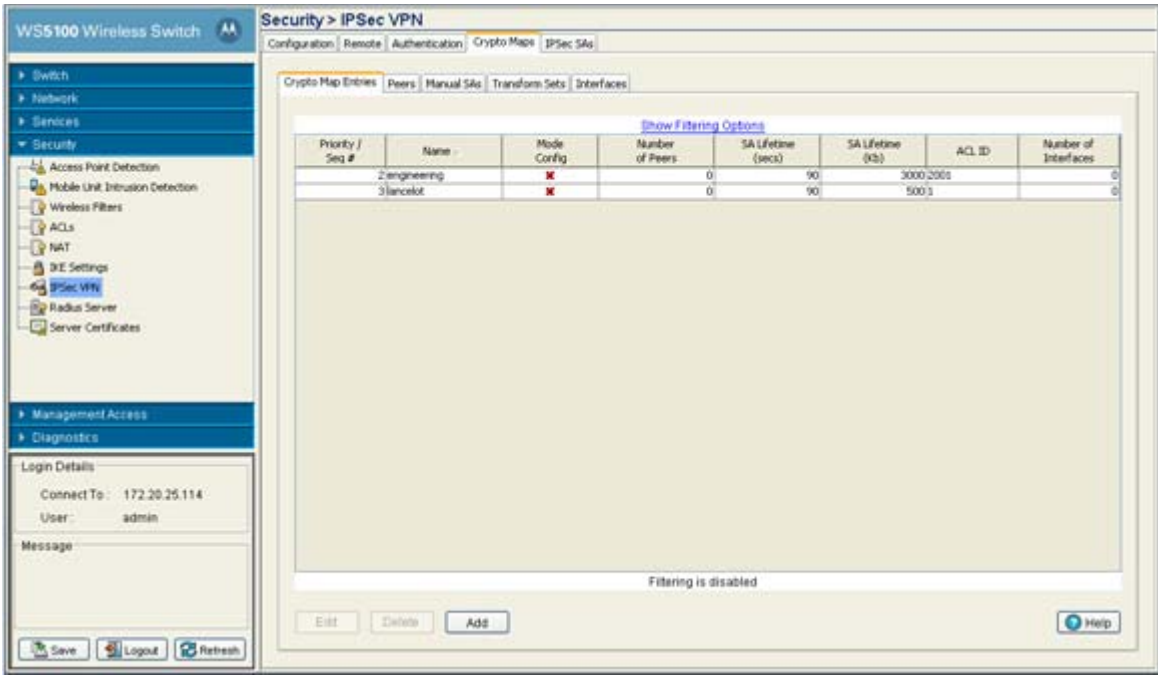
6.8.4 Configuring Crypto Maps

The Crypto Maps feature allows you to configure the switch to restrict access to selected encrypted interfaces for those peers with specific certificates, especially certificates with particular *Distinguished Names* (DNs). 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 different 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*

6.8.4.1 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.

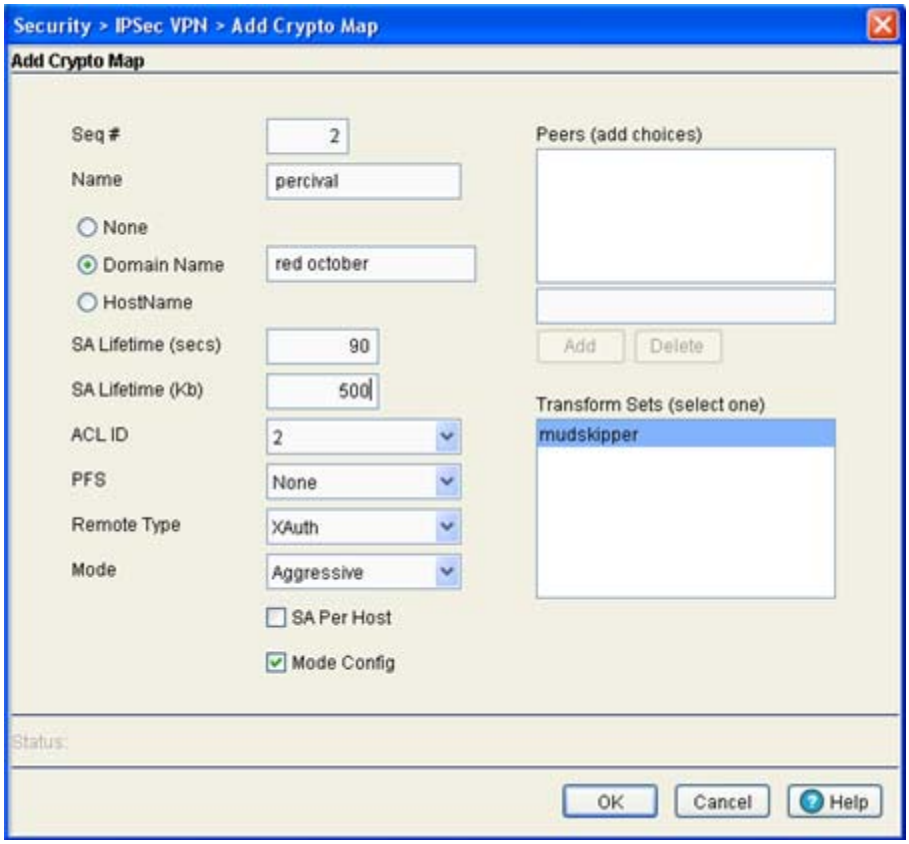
Mode Config	This columns displays a green checkmark for the Crypto Map used with the current interface. A "X" is displayed next to other Crypto Maps not currently being used.
Number of Peers	Displays the number of peers used by each Crypto Map displayed.
SA Lifetime (secs)	Displays a SA Lifetime (in 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 *Access Control List* (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 Crypto Maps within the screen.

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. The sequence number determines its priority among the other Crypto Maps. The lower the number, the higher the priority.

b. Assign the Crypto Map a **Name** to differentiate from others with similar configurations.

c. Use the **None, Domain Name** or **Host Name r**adio buttons to select and enter the fully qualified domain 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 amount of 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 of 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 to select and use the Add and Delete buttons as necessary to add or remove existing peers to the Crypto Map. For information on adding or modifying peers, see *Crypto Map Peers on page 6-55*.

m. Refer to the **Transform Sets (select one)** field to select and assign a transform set for use with the 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.

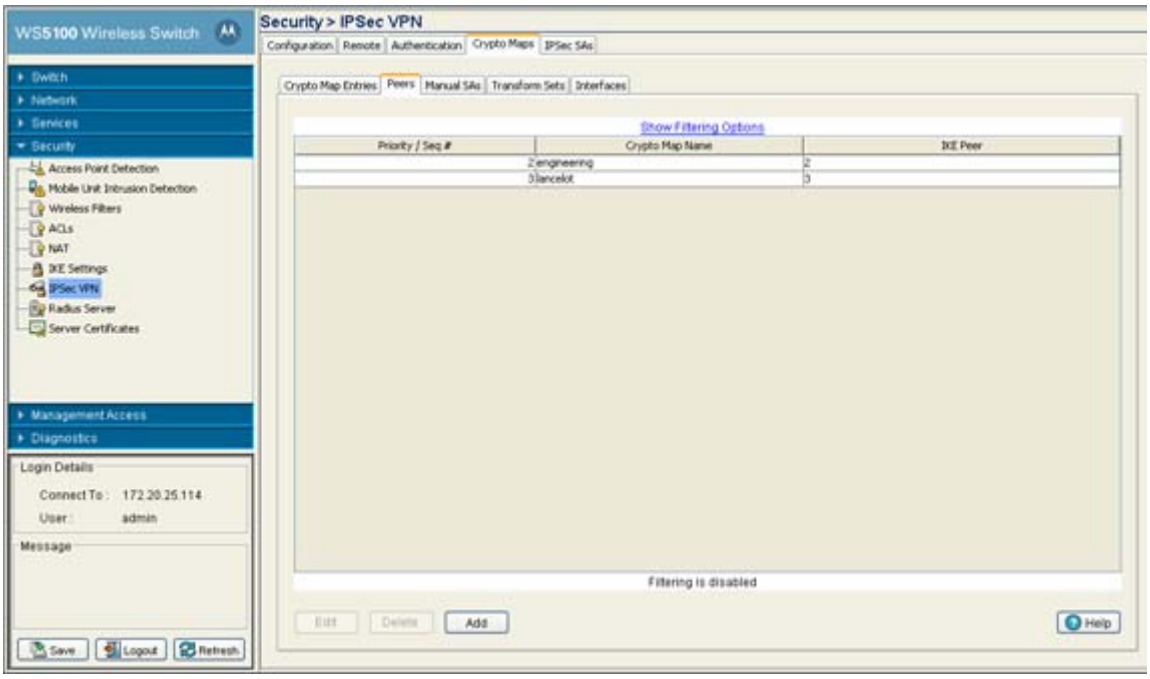
7. Click **OK** to save the new Crypto Map and display it within the Crypto Map tab.

6.8.4.2 Crypto Map Peers

To review, revise or add Crypto Map peers:

1. Select **Security** > **IPSec VPN** from the main menu tree.

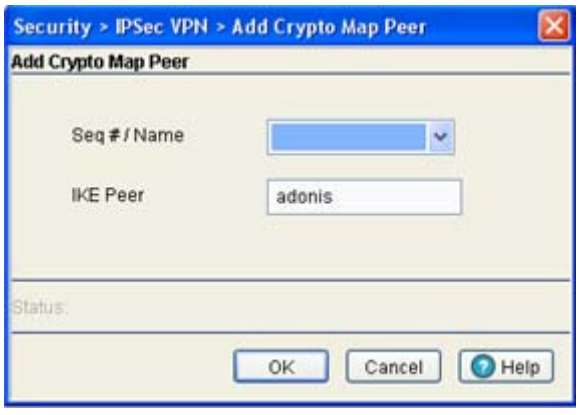
2. Click the **Crypto Maps** tab and select **Peers**.



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) in order to distinguish one from the other. The sequence number determines its priority among Crypto Maps. The lower the number, the higher the priority.
Peer 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 to revise its configuration.
5. Select an existing Crypto Map and click the **Delete** button to remove 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. The lower the number, the higher the priority among Crypto Maps.

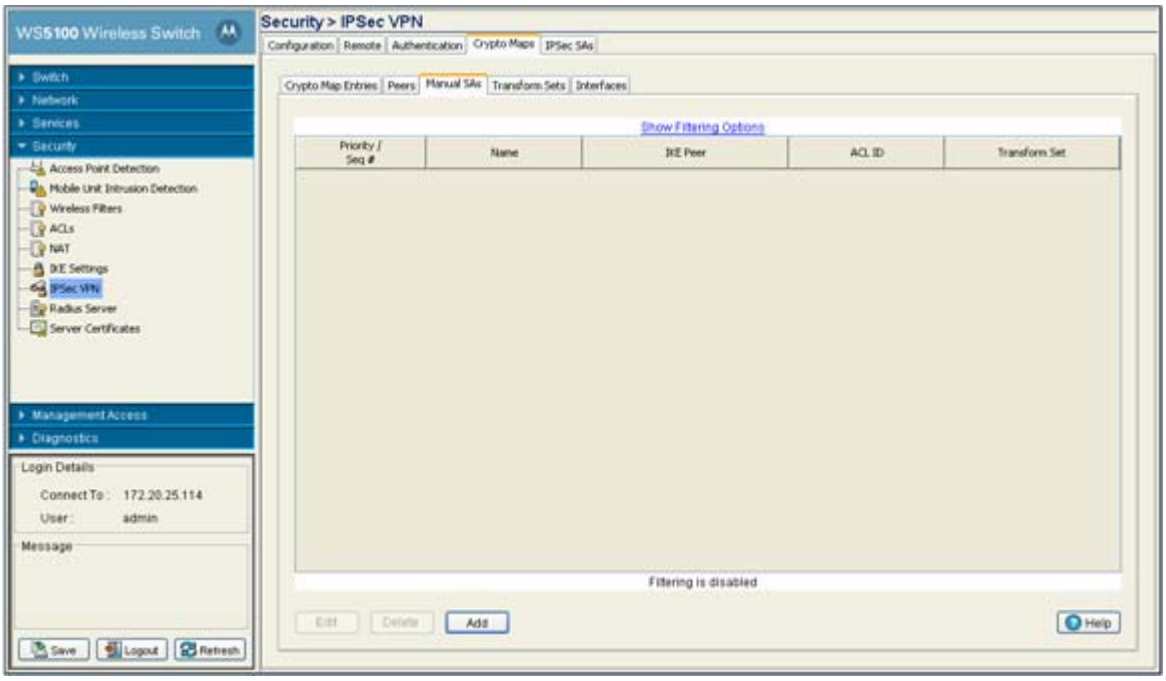
b. Enter the name of the **IKE Peer** used with the Crypto Map to build an IPSec security association.

7. Click **OK** when completed to save the configuration of the new Crypto Map peer.

6.8.4.3 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**.

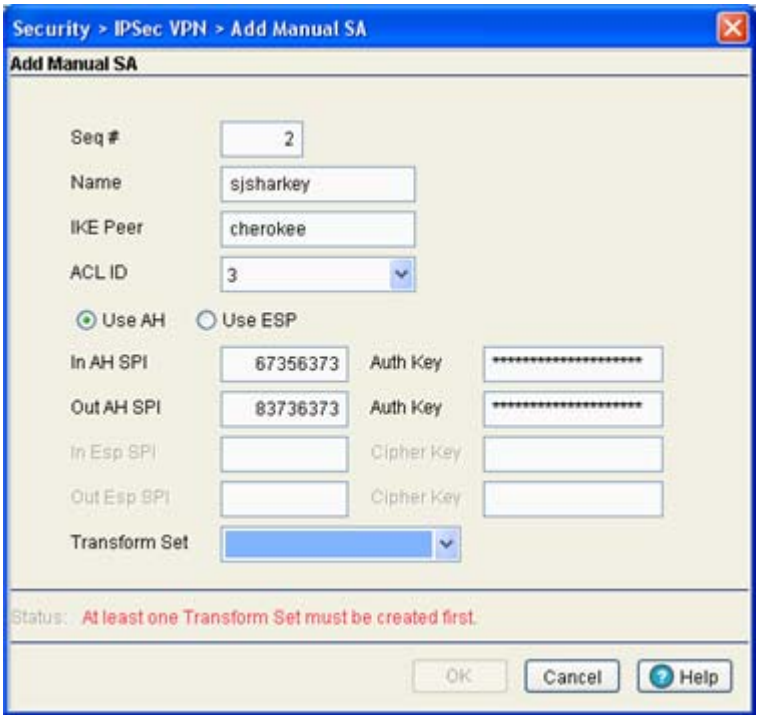


3. Refer to the read-only information displayed within the **Manual SAs** tab to determine whether a Crypto Map with a manually defined security association requires modification or a new one requires creation.

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 is using to establish access permissions.
Transform Set	Displays the transform set representing a combination of security protocols and algorithms. During the IPSec 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 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 with the manual security association 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 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 and key fields become enabled depending on which radio button is 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.

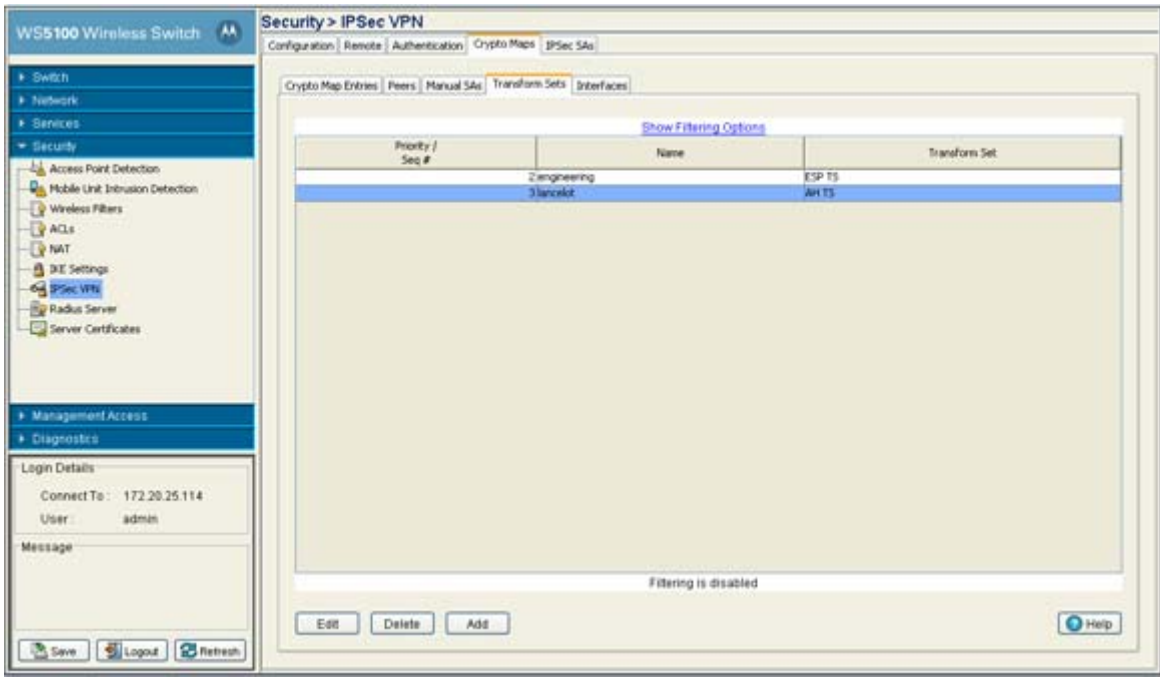
7. Click **OK** when completed to save the configuration of the Crypto Map security association.

6.8.4.4 Crypto Map Transform Sets

A transform set is a combination of security protocols and algorithms that define how the switch protects data.

To review, revise or add a Crypto Map transform set:

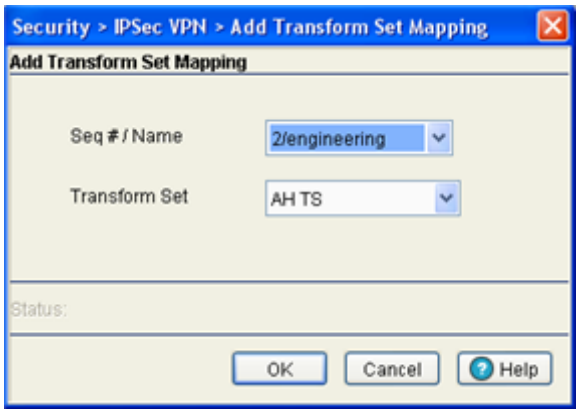
1. Select **Security** > **IPSec VPN** from the main menu tree.
2. Click the **Crypto Maps** tab and select **Transform Sets**.



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. The lower the number, the higher the priority.
Name	Displays the name assigned Crypto Map 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 from list.
6. If a new Crypto Map transform set requires creation, click the **Add** button.



a. Define the **Seq #/Name**. The lower the number, the higher the priority among Crypto Maps.

b. Enter the name of the **Transform set** used with the Crypto Map.

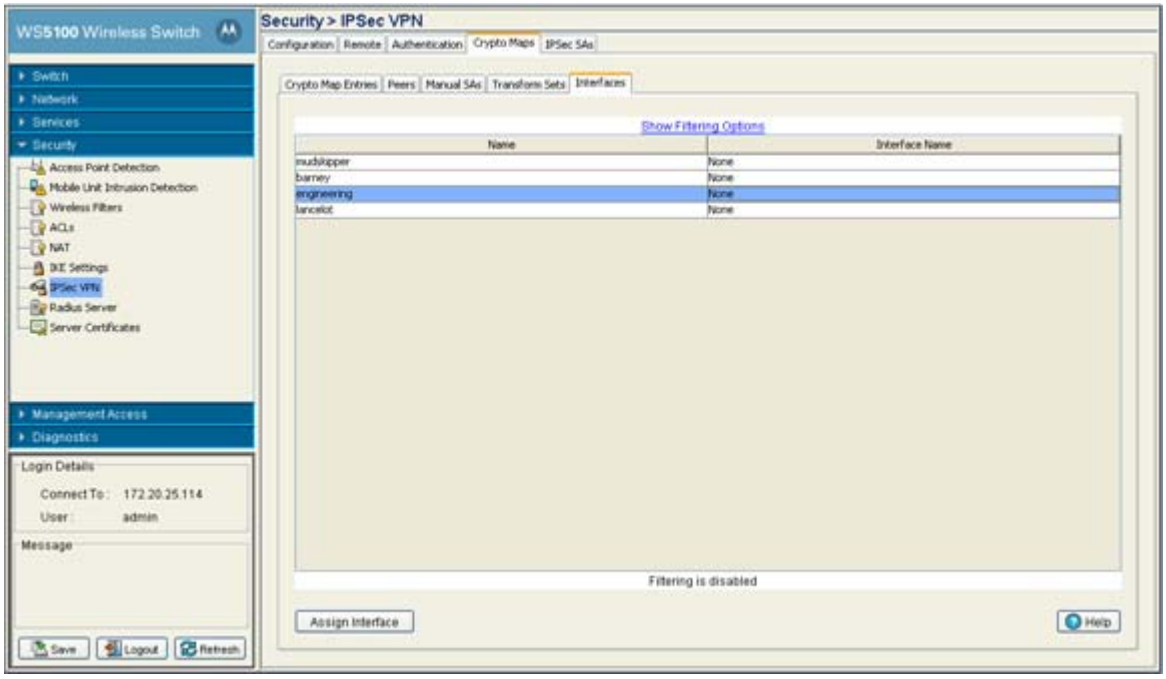
7. Click **OK** when completed to save the configuration of the Crypto Map transform set.

6.8.4.5 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.

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	Displays the name of the Crypto Maps available for interface.
Interface Name	Displays the name of the interface through which IPSec traffic will flow. 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 to be 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.

   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 to 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

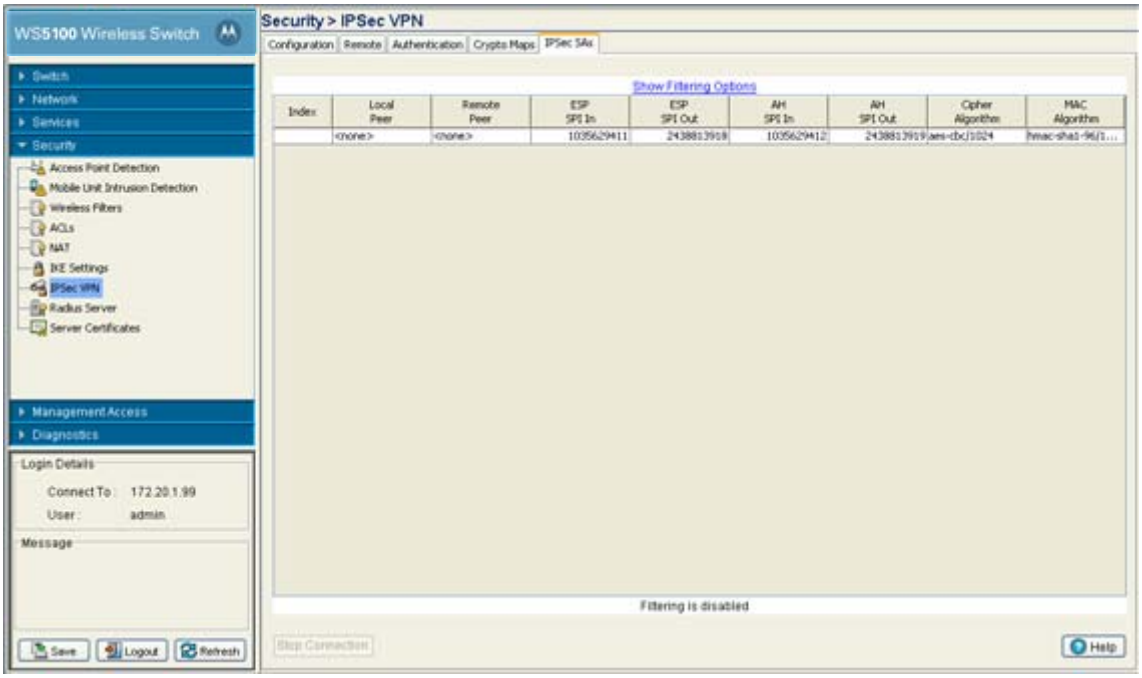
Crypto Map configuration. Also, adding new peers through the use of new sequence numbers and reassigning the Crypto Map does not tear down existing connections.

6.8.5 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 also 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) 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. If necessary, select a security association from those displayed and click the **Delete** button to remove it.

6.9 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 6-62*.

Setting up Radius on the switch entails the following:

- *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. For information on configuring the Radius server, see *Configuring the Radius Server on page 6-62*.

6.9.1 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 communication 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 makes is an excellent choice for performing accounting. Radius can significantly increase security by centralizing password management.

The switch can be configured to use its own local Radius server or an external Radius server you define and configure within the switch managed network. 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 6-64*.

NOTE: When restarting or rebooting the switch, the Radius server will also be restarted regardless of its state before the reboot.

The Radius server is used to define 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 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 enforcement of User based policies. User based policies include dynamic VLAN assignment and access based on time of day.

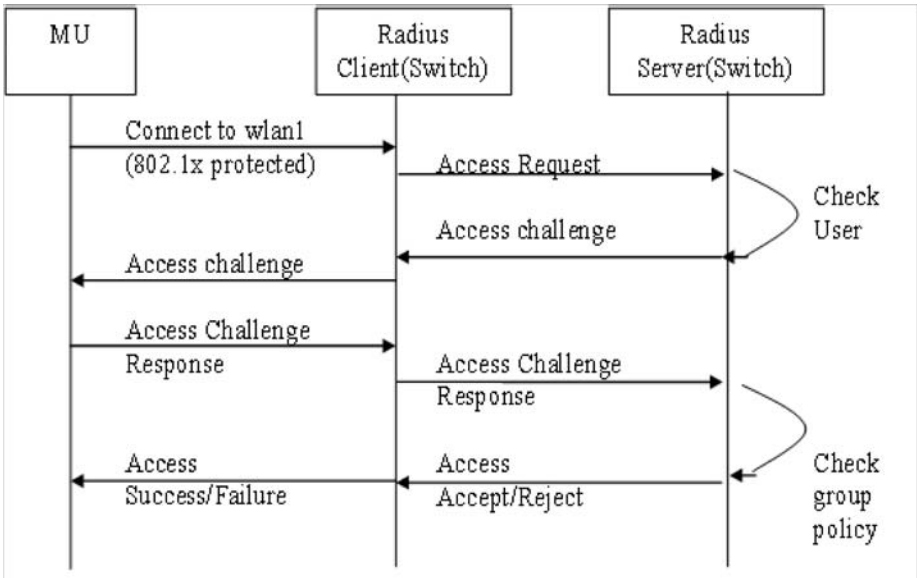
The switch uses a default trustpoint. A certificate is required for EAP TTLS,PEAP and TLS Radius authentication (configured with the Radius service).

Dynamic VLAN assignment is achieved based on 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 4-22*.

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 the challenge information received in the Radius access request frames. If the user is authorized and authenticated, the wireless client is granted access by sending a Radius access accept frame. This is transmitted to the wireless client in an EAPoL frame format.



6.9.1.1 User Database

The User Group names and the 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 on its local database. Each group can have a maximum of 500 users configured.

6.9.1.2 Authentication of Terminal/Management User(s)

The local Radius server can be used to authenticate users. A normal user (with password) should be created in the local database. These users should not be a part of any group.

6.9.1.3 Access Policy

Access policies are defined for a group created in 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 by using a "Time of the day" access policy. Consider User1 who's a part of Group1, 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.

6.9.1.4 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.

6.9.1.5 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 the users. The switch supports two LDAP server configurations.

6.9.1.6 Accounting

Accounting should be initiated by the Radius client. Once the Local/Onboard Radius server is started, it will listen for both authentication and accounting records.

6.9.2 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 user 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 4-36*. To continue to instructions on how to configure the switch's local Radius Server, see *Defining the Radius Configuration on page 6-65*.

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 the external Radius Server is unreachable, the switch reverts to the local Server's user database to authenticate a user. However, if the external Radius server is reachable but rejects the user Using the Switch's Radius Server Versus an External Radius Server 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.

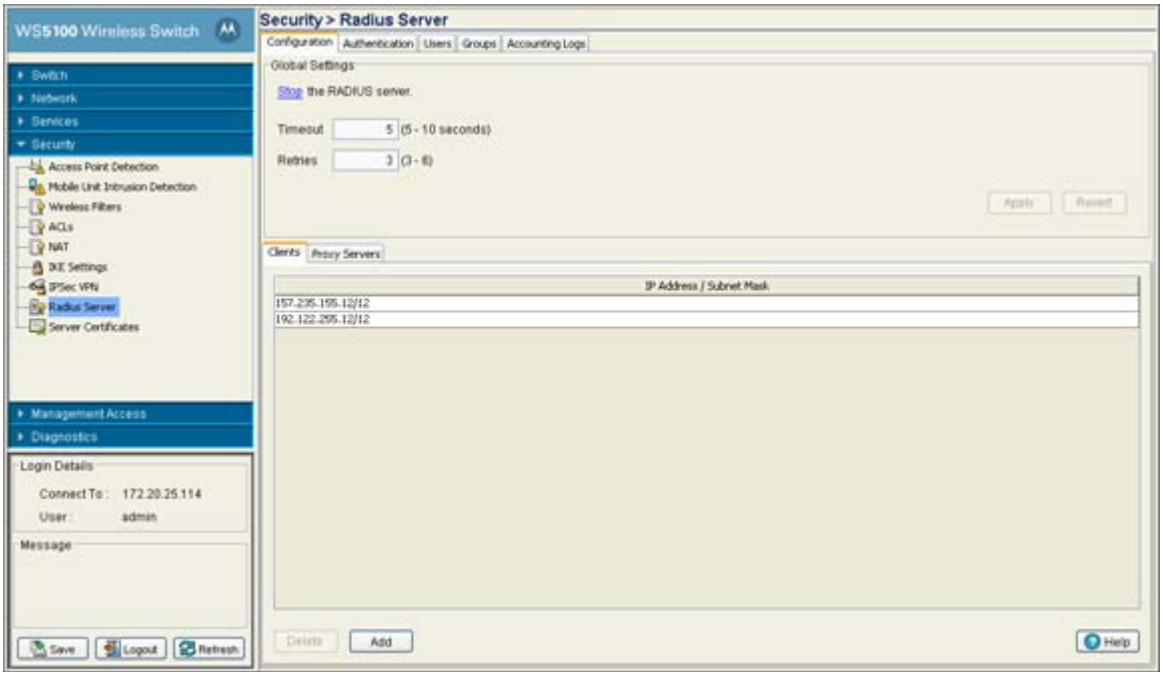
If the switch's local Radius Server is configured as the primary authentication method and an external Radius Server is configured as an alternate method, the alternate external Radius Server will not be used a

authentication source if a user does not exist in the local Server's database, since the primary method has rejected the authentication attempt.

6.9.3 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.
4. Set a **Timeout** value (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 6-66*. 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 6-66*.

6.9.3.1 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 their 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:

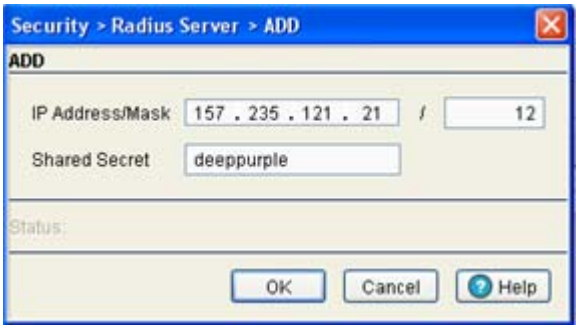
1. Select **Security** > **Radius Server** from the main menu.
2. Ensure the **Configuration** tab is selected.
3. Select the **Clients** tab from the bottom portion of the Configuration tab.

The Clients tab displays the IP address and subnet mask of the switch's 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 the 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 are 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 22 characters long to protect the Radius server from brute-force attacks. The max length of the shared secret is 31 characters.

   c. 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.

   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

6.9.3.2 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 portion 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. To create a new Radius proxy server configuration, click the **Add** button at the bottom of the screen.

   a. Create a new **User ID Suffix** serving as an abbreviation for the configuration to differentiate it from other configurations with similar attributes.

   b. Specify the **IP Address** of the new Radius proxy server.

   c. Enter the TCP/IP port number to be used by the proxy Radius server.

   d. Specify a Radius **Shared Secret** for authenticating the Radius client.

   e. Shared secrets are 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 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.

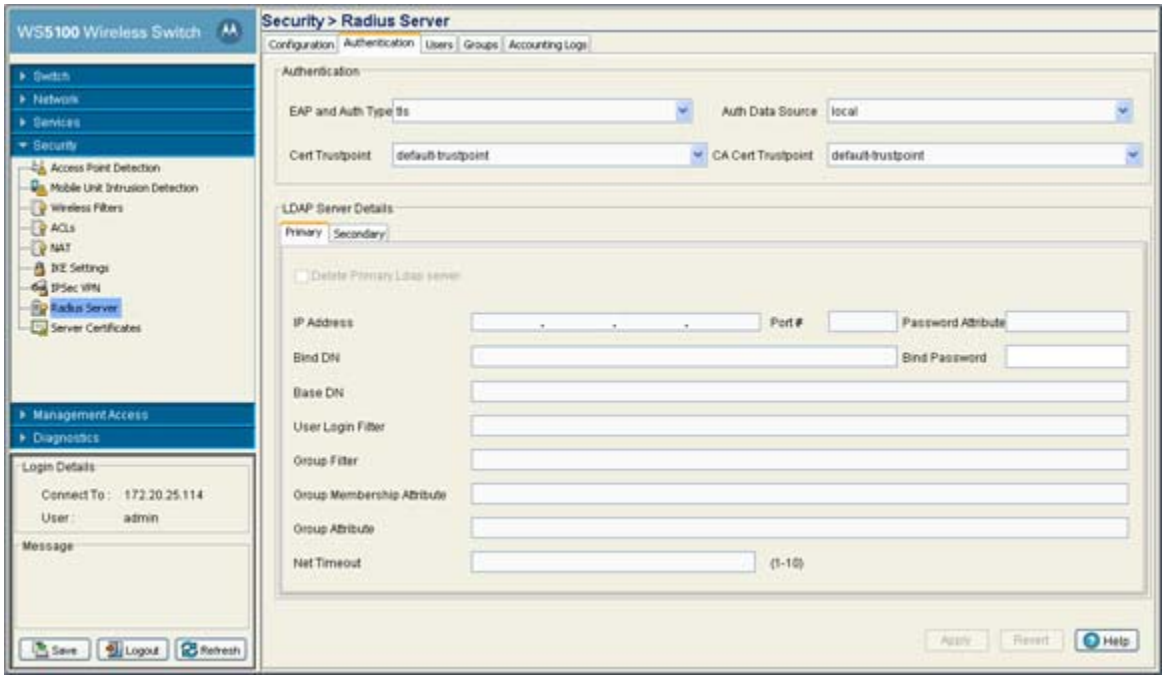
   h. Click **Cancel** to close the dialog without committing updates to the running configuration

6.9.4 Configuring Radius Authentication and Accounting

Deploy one or more Radius servers to manage security and retrieve accounting information within 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 will be 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 itself will be 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 use with the switch, see *Creating Server Certificates on page 6-74*.

4. Refer to the **LDAP Server Details** field to define the attributes of the primary and secondary Radius LDAP servers providing access to external databes to be used with local Radius servers.

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 subnet on the switch.
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 your LDAP server.
Group Membership Attribute	Specify the Group Member Attribute to be sent to the LDAP server when authenticating the users.
Group Attribute	Specify the group attribute used by the LDAP server.
Net Timeout	Enter a timeout value the system uses to terminate the connection to the Radius Server if no activity is detected.

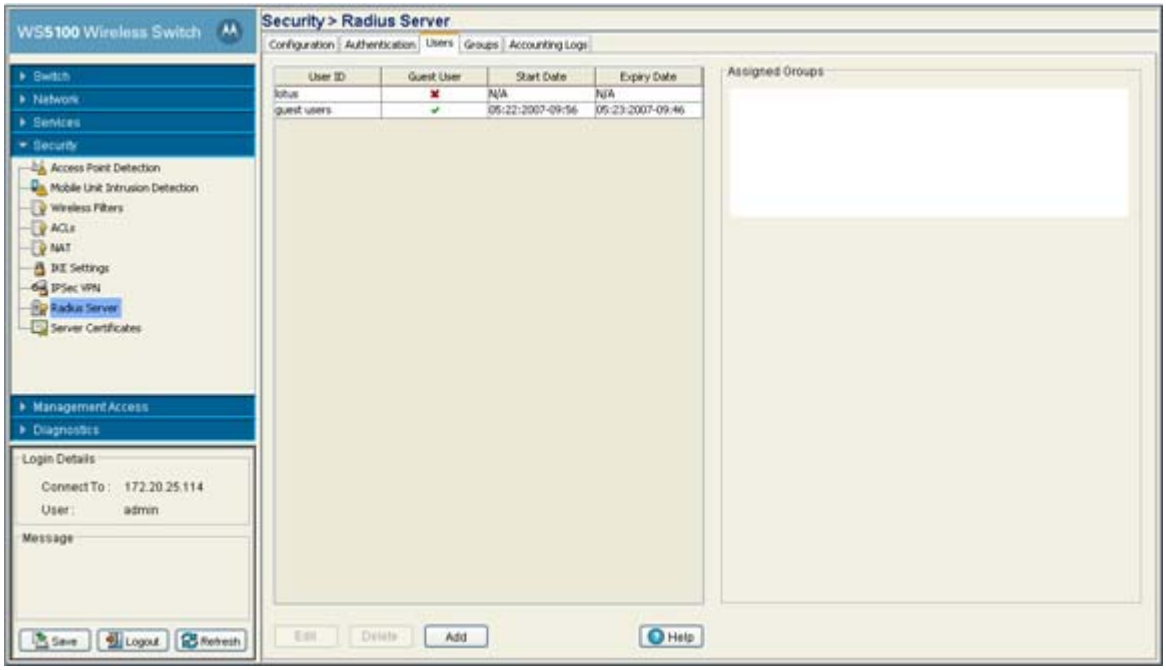
5. Click the **Apply** button to save the changes made to within the screen.
6. Click the **Revert** button to cancel any changes made within the screen and revert back to the last saved configuration.

6.9.5 Configuring Radius Users

Refer to the **Users** tab to view the current set of users and assigned groups for the Radius server. The Users tab is used 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 user 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 user information 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 Radius server access.
Start Date	Defines the time when the User's privileges commence.
Expiry Date	If the user has been assigned guest privileges, then they were also assigned a date when their Radius privileges expire.

4. Refer to the **Assigned Groups** field to view the memberships for the existing users displayed within the Users tab.

   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.

5. To modify the attributes of an existing user, select the user from the list of users displayed 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.

6. If an existing user is no longer needed, select the user from those displayed and click the **Delete** button to permanently remove the user from the list available.

7. To create a new user for use with the local Radius server, click the **Add** button and provide the following information.

CAUTION: Radius user passwords will be stored in the running configuration file in clear text if password encryption is not enabled. The user passwords will be shown as encrypted if the global password encryption is enabled. The maximum for the file is 500 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 only temporary access to the local Radius server, thus restricting their authentication period to a user defined interval.
Password	Enter the password used to add 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 Time	Displays the read only switch time. This is the switch time used for the expiry data and time.
Start Date & Time	Defines the start date and time (in dd:MM:yyyy-hh:mm format) to login guest users defined with temporary permissions.
Expiry Date & Time	Defines the date and time (in dd:MM:yyyy-hh:mm format) to timeout guest users defined with temporary permissions.
Available Groups	Use the Available Groups **Add ->** and **Remove <-** functions to map groups (for inclusion) for this specific user.
Configured Group	Select the **Configured Group** checkbox to

   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

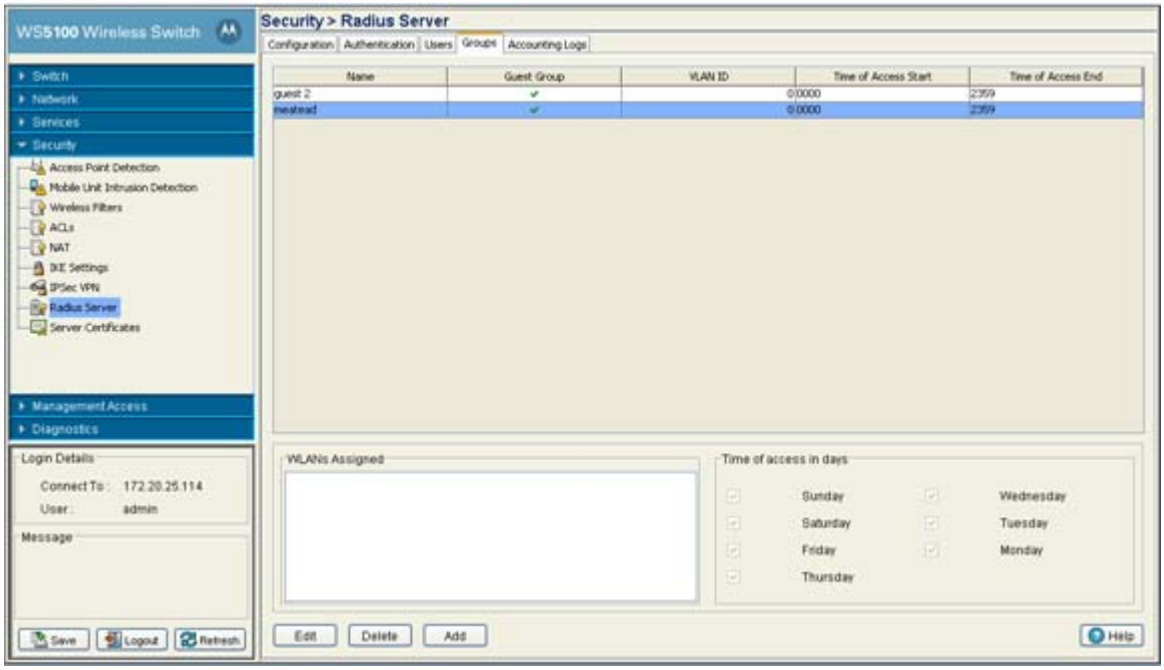
6.9.6 Configuring Radius User Groups

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 fro each group is displayed to provide the administrator then option of using a group as is, modifying an existing group's properties or creating a new group.

To assess the configuration of existing user groups:

1. Select **Security** > **Radius Server** from the main menu.

2. Select the **Groups** tab.



3. Refer to the displayed user groups to assess the following read-only attributes for each group listed:

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 (with a red X) or has been configured as permanent group. Guest users have temporary Radius server access.
VLAN ID	Display the VLAN ID(s) used by each group listed. 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 was (will be) authenticated to interoperate within the switch managed network. Each user within the group will be authenticated with the local Radius server. Those group members successfully authenticated are allowed access to the switch managed network using the restrictions defined for the group.
Time of Access End	Displays 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, then the user may still interoperate with the switch (remain authenticated) as part of that group.

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 to be selected.

   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 and WLAN assignment.

7. If an existing group is no longer needed (perhaps obsolete in function), select the group from those displayed and click the **Delete** button to permanently remove the group from the list of available groups.

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 with one another 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 within the switch managed network. Each user within the group will be authenticated with the local Radius server. Those group members successfully authenticated are allowed access to the switch managed network 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, then the user may still interoperate with the switch (remain authenticated) as part of that group.
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 using the WLANs configured. Of course, the user base within the group still needs to be authenticated by the local Radius server first.

   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.

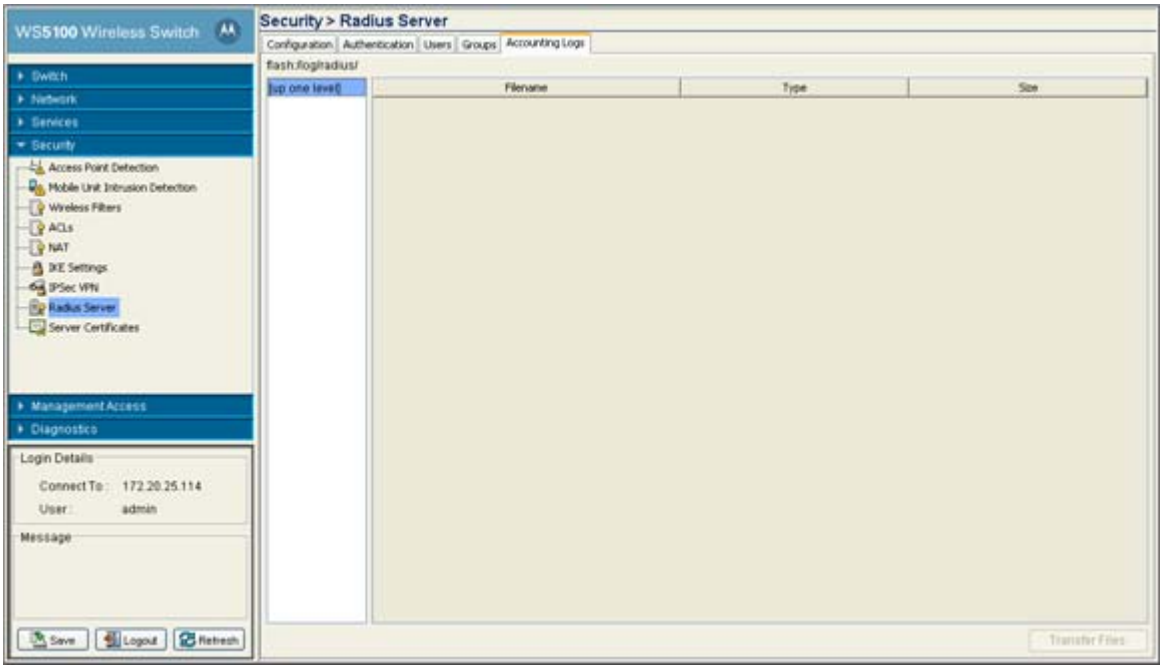
6.9.7 Viewing Radius Accounting Logs

Accounting logs contain information about the use of remote access services by users.

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.

6.10 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)
- import the certificate.
- 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 Web browsers while establishing a *Secure Socket Layer* (SSL) connection.

The **Server Certificates** screen contains the following two tabs:

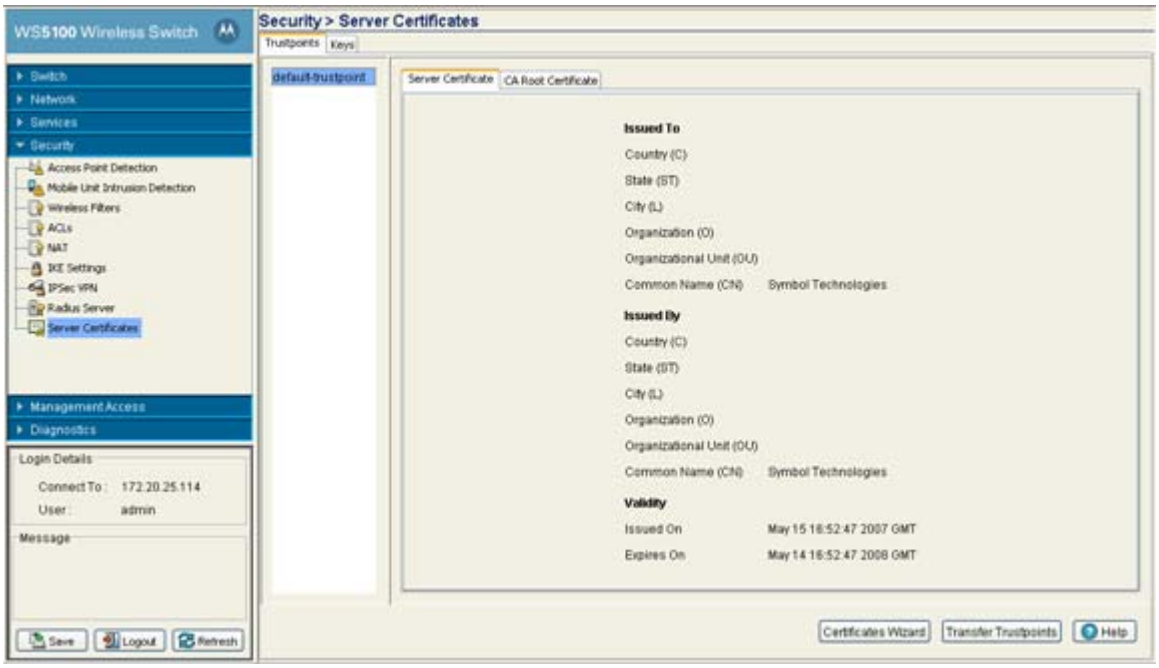
- *Using Trustpoints to Configure Certificates*
- *Configuring Trustpoint Associated Keys*

6.10.1 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 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.

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 the currently enrolled trustpoints.

The **Server Certificate** and **CA Root Certificate** tabs display read-only credentials for the certificates currently 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.

Org. 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) and 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 6-77*.

6.10.1.1 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. The Certificate Wizard displays.

   Use this wizard to:

   - Create a new certificate
   - Upload 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 send to a *Certificate Authority* (CA).

   For more information, see *Using the Wizard to Create a New Certificate on page 6-77*.
5. Select the **Upload an external certificate** radio button to upload an existing Server Certificate or CA Root Certificate.

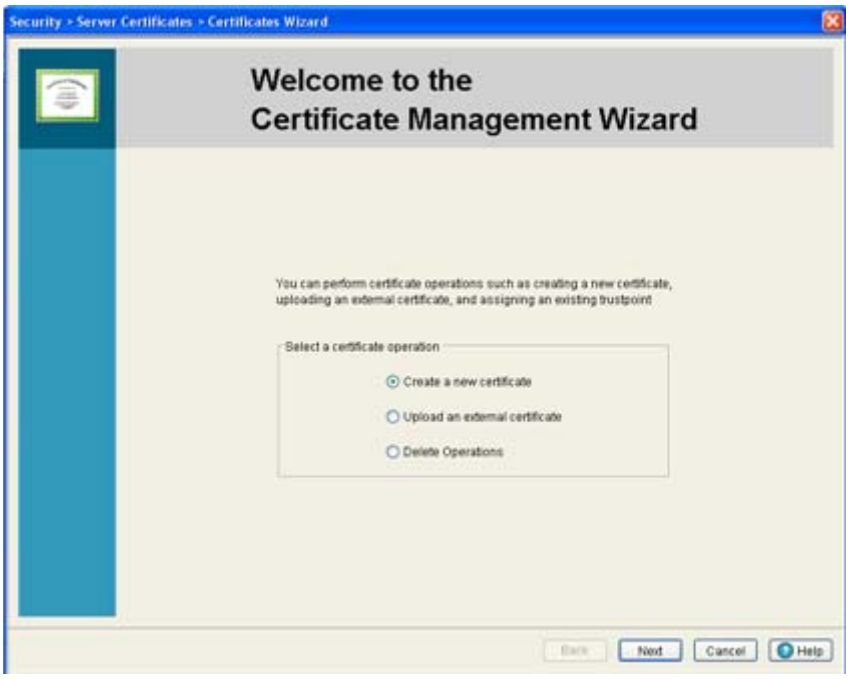
   For more information, see *Using the Wizard Delete Operation on page 6-80*.
6. Select the **Delete Operations** radio button to delete trustpoints and all related keys.

   For more information, see *Using the Wizard Delete Operation on page 6-80*.

Using the Wizard to Create a New Certificate

To generate a new self-signed certificate or prepare a certificate request which can be send to a *Certificate Authority* (CA):

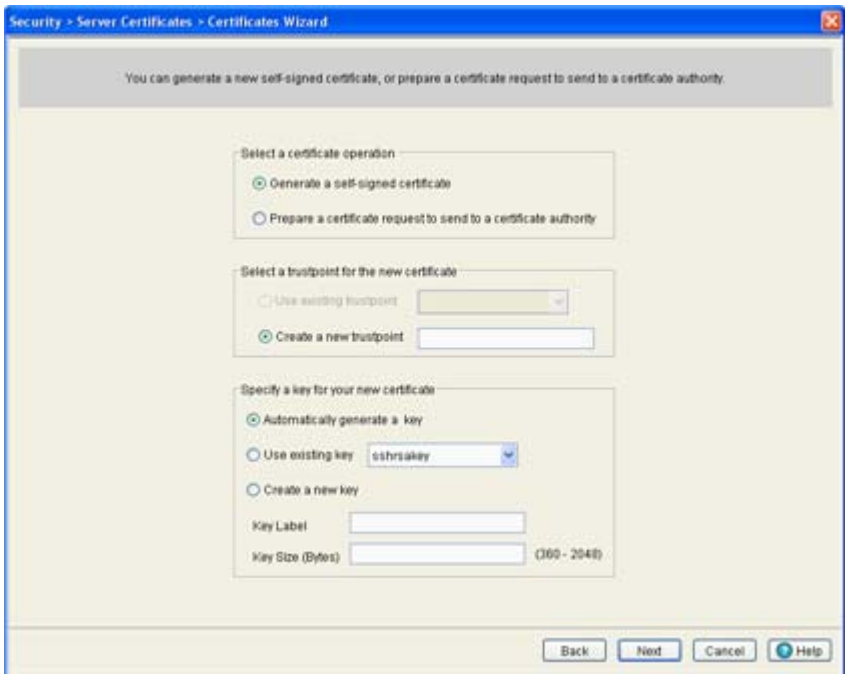
1. Select the **Create new certificate** radio button in the wizard and click the **Next** button.



   The second page of the wizard contains two editable fields, **Select Certificate Operation** and **Specify a key for you new certificate**.

2. Use the second page to create either a self signed certificate or prepare for a certificate request. For certificate operation, 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 create and install the certificate.



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 the key for the new certificate, select one of the following options:

- *Automatically generate a key* — Select this option to automatically generate a key for the trustpoint.
- *Use existing key* — Select 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 Label 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 a new certificate.

3. Select the **Configure the trustpoint** checkbox to enable the new self signed certificate to be configured as a trustpoint.
4. 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 Province. 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 City. This is a required field.
Organization	Define an Organization for the organization used in the Self-Signed Certificate. By default, it is Company Name. 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 Department Name. This is a required field.
Common Name	Define a Common Name for the URL of the switch. This is a required value. The Common Name must match the URL used in the browser when invoking the switch Web UI.
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 that can be used as the switch destination for certificate requests.
Password	Enter an alphanumeric password used to access the certificate configuration.
Company	Provide a Company name to be used on behalf of the certificate.

5. Select the **Enroll the trustpoint** checkbox to enroll the certificate request with the CA.
6. Click **Next** to proceed with the certificate creation.

   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.
7. Use the **Enter trustpoint name** parameter to assign a name to the trustpoint.
8. Provide Certificate Credential information for the following:

Country	Define the **Country** used in the Self-Signed Certificate. By default, this 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 Province. 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 City. This is a required field.
Organization	Define an Organization for the organization used in the Self-Signed Certificate. By default, it is Company Name. 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 Department Name. This is a required field.
Common Name	Define a Common Name for the switch URL. This is a required value. The Common Name must match the URL used in your browser when invoking the switch applet.
Password	Provide the password required to access the URL.
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 that can be used as the switch destination for certificate requests.

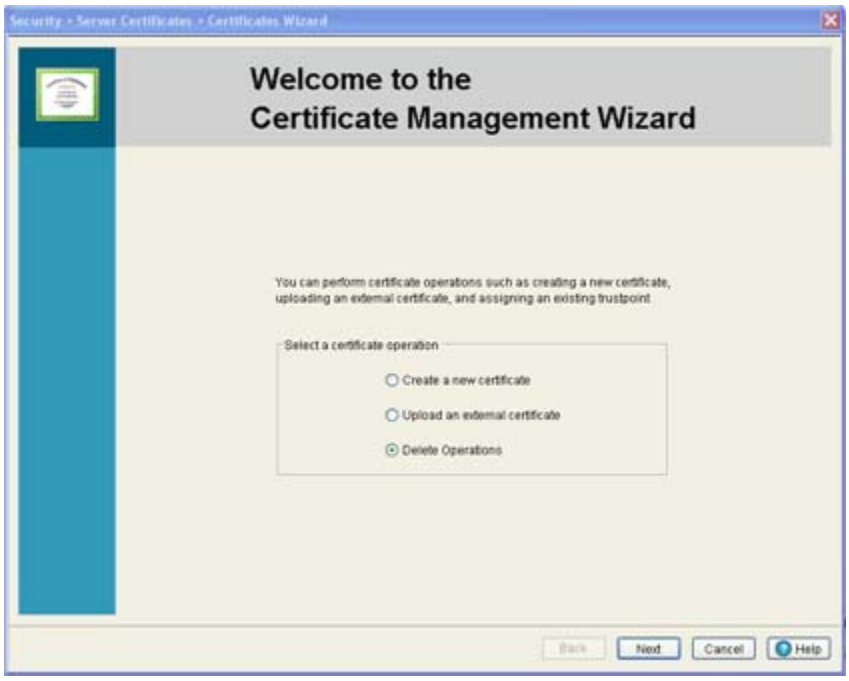
9. Click the **Next** button to continue preparing the certificate request.

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 the 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 in the wizard and click the **Next** button.



   The next page of the wizard is used to delete a trustpoint.

2. Select the **Delete the following for trustpoint** checkbox and select the trustpoint to delete from the drop-down menu associated with it. This enables the following options:

Delete entire trustpoint	Select the checkbox and select a certificate to remove. If selected, the **Delete the following trustpoint** option is disabled.
Delete the following for trustpoint	Select this option to delete the trustpoint for the selected Server Certificate or CA Root Certificate.
Delete all the keys from the switch	Select this option to remove all of the keys that have previously been configured for the deleted trustpoints. Once removed, the keys cannot be restored.

3. Click the Next button to complete the trustpoint removal.

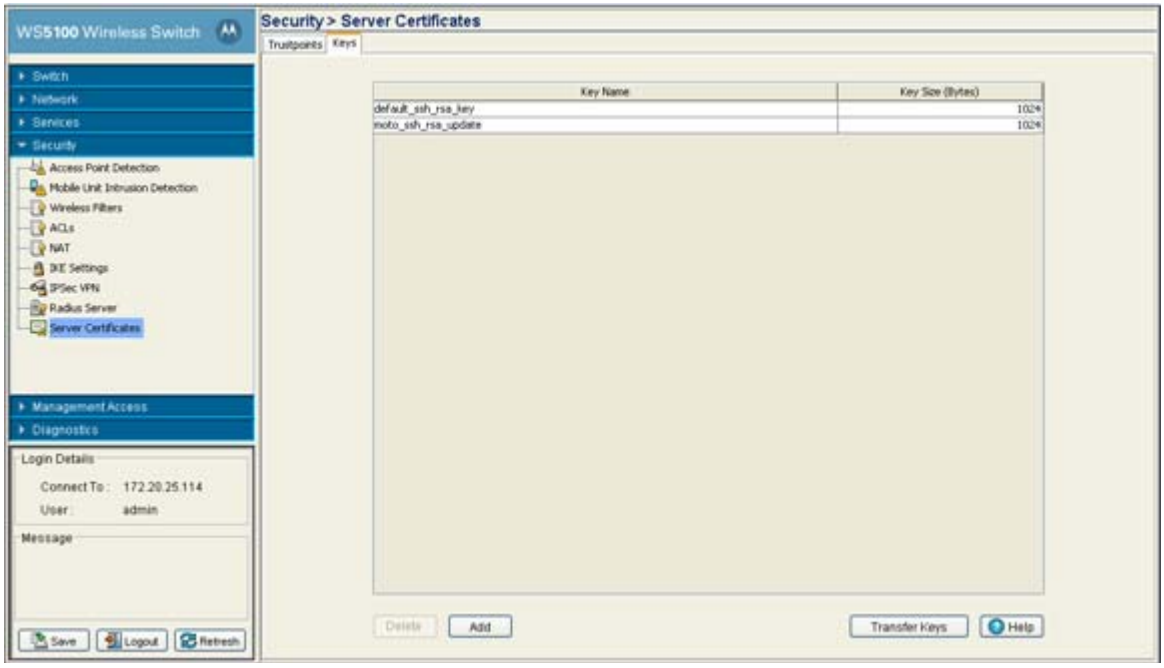
6.10.2 Configuring Trustpoint Associated Keys

Trustpoint keys allow a user to configure the switch to use different *Rivest, Shamir, an Adelman* (RSA) key pairs. Therefore, the switch can maintain a different key pair for each certificate.

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 Label	The Key Label is the name of the key pair that can be automatically generated separately, or automatically when selecting a certificate. Specify your option within the wizard.
Key Sizes	The size of the desired key. If not specified, a key size of 1024 is used.

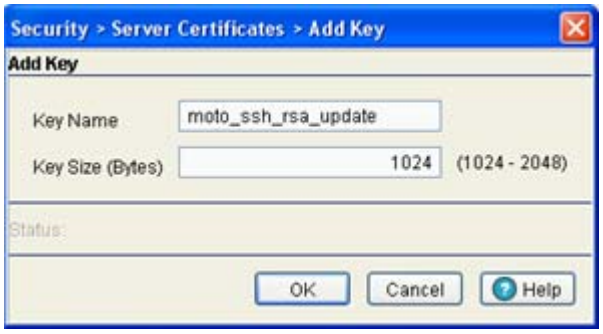
3. Highlight a Key from the table and click the **Delete** button to delete it from the switch.
4. Click on **Add** button to add a new key label to the list of keys available to the switch. For more information, see *Adding a New Key on page 6-82*.
5. Click on **Transfer Keys** to archive the keys to a user-specified location. For more information, see *Transferring Keys on page 6-83*.

6.10.2.1 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 in the space provided.
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.

6.10.2.2 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 this data needs to be retreived.

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 will be 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 **Close** button to exit the screen after a transfer. There are no changes to save or apply.

7

Switch Management

This chapter describes the Management Access main menu items used to configure the switch. This chapter contains following content:

NOTE: HTTPS must be enabled to access the switch applet. Ensure that 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 Motorola Website for a newer version) of 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.

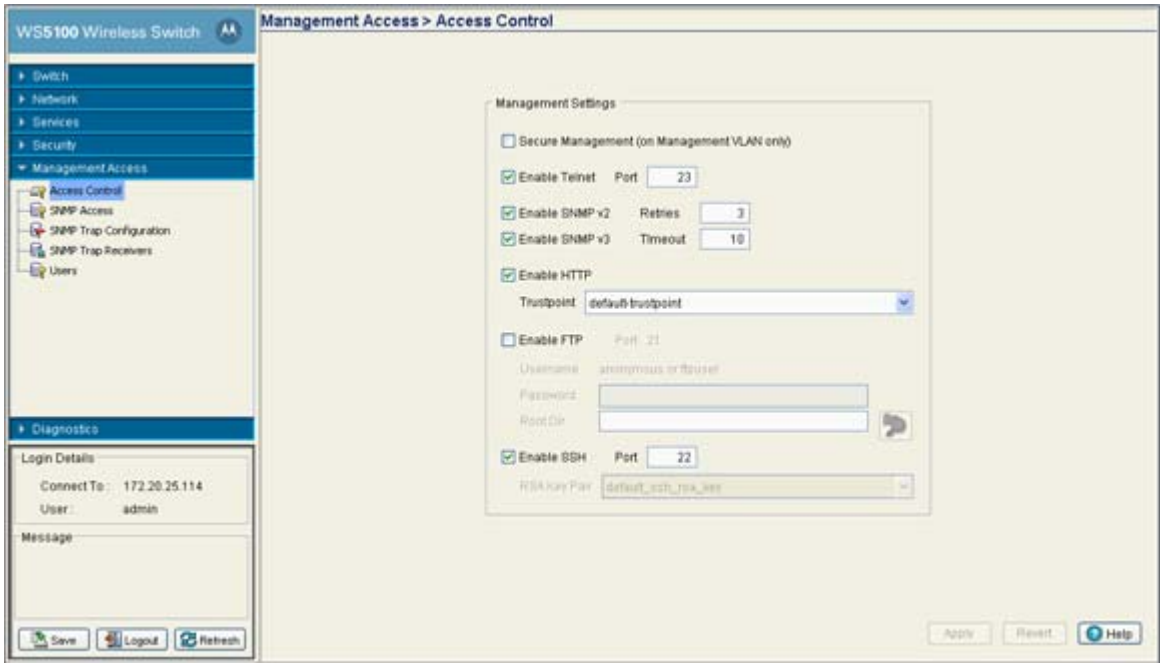
NOTE: The **Apply** and **Revert** functions are greyed out within this screen, as this screen is read-only with no configurable parameters for the user to update and save.

7.2 Configuring Access Control

Refer to the **Access Control** screen to allow/deny management access to the switch using different protocols such as HTTP, HTTPS, Telnet, SSH or SNMP. The access options are either enabled or disabled. 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 on the switch:

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 telnet session access 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.
Enable SNMP v2	Select this checkbox to enable SNMPv2 access to the switch and configuration activities over the SNMPv2 interface. This setting is enabled by default.
Enable SNMP v3	Select this checkbox to enable SNMPv3 access to the switch and configuration activities 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 their 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.
Trustpoint	Use the Trustpoint drop-down menu to select the local or default trustpoint or used with the HTTPS session with the switch. For information on creating a new certificate for use with the switch, see *Creating Server Certificates on page 6-74*.

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 SSH	Select this checkbox to enable SSH 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

The SNMP Access menu allows you to view and configure existing SNMP v1/v2 and SNMP v3 details 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*
- *Accessing SNMP v2/v3 Statistics*

CAUTION: Your system must be running Sun JRE version 1.5.x (or higher) or Mozilla in order 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. You must first deposit the configuration file to a computer, then FTP the file to the switch.

7.3.1 Configuring SNMP v1/v2 Access

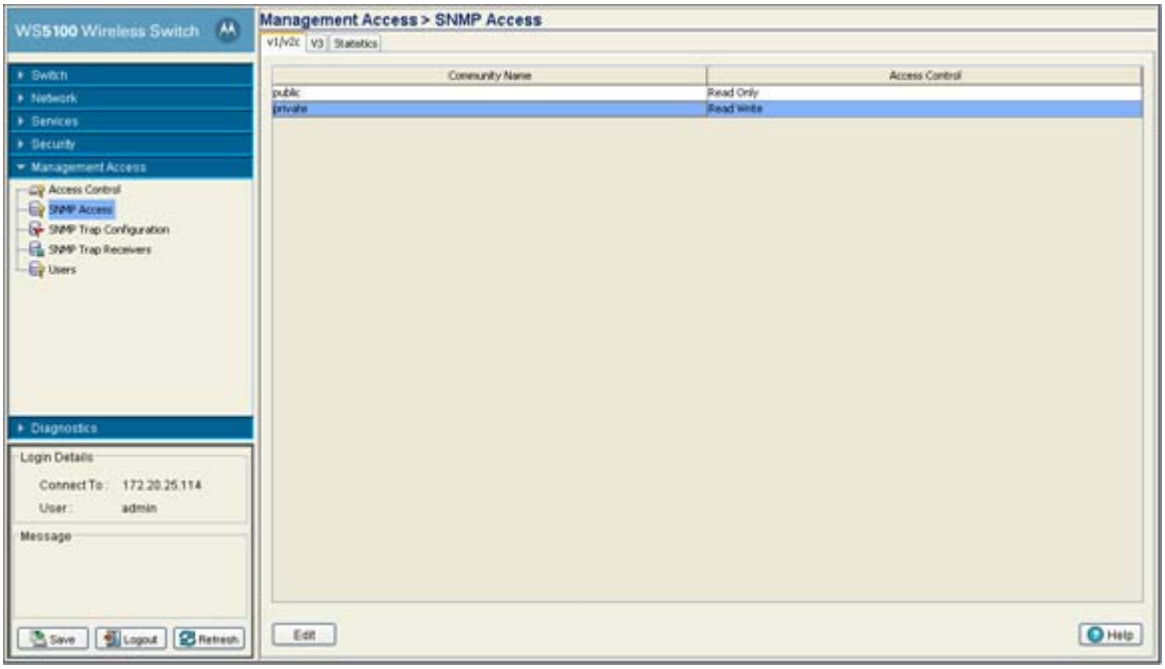
SNMP version 2 (SNMPv2) is an evolution of the SNMPv1. The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv2. However, SNMPv2 adds and enhances some protocol operations. The SNMPv2 Trap operation, for example, serves the same function used in SNMPv1, but it 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** fields 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.

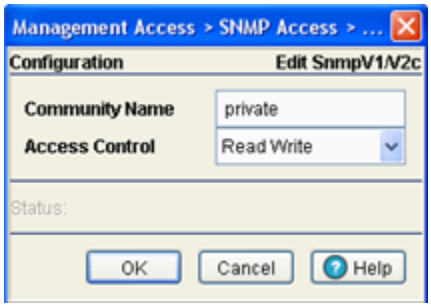
3. Highlight an existing entry and click the **Edit** button to modify the properties of an existing SNMP V1/v2 community and access control definition. For more information, see *Editing an Existing SNMP v1/v2 Community Name on page 7-6*.

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 models.

Refer to the **v3** screen to review the current SNMP v3 configuration. An Existing User Name can be selected and edited, enabled or disabled. .

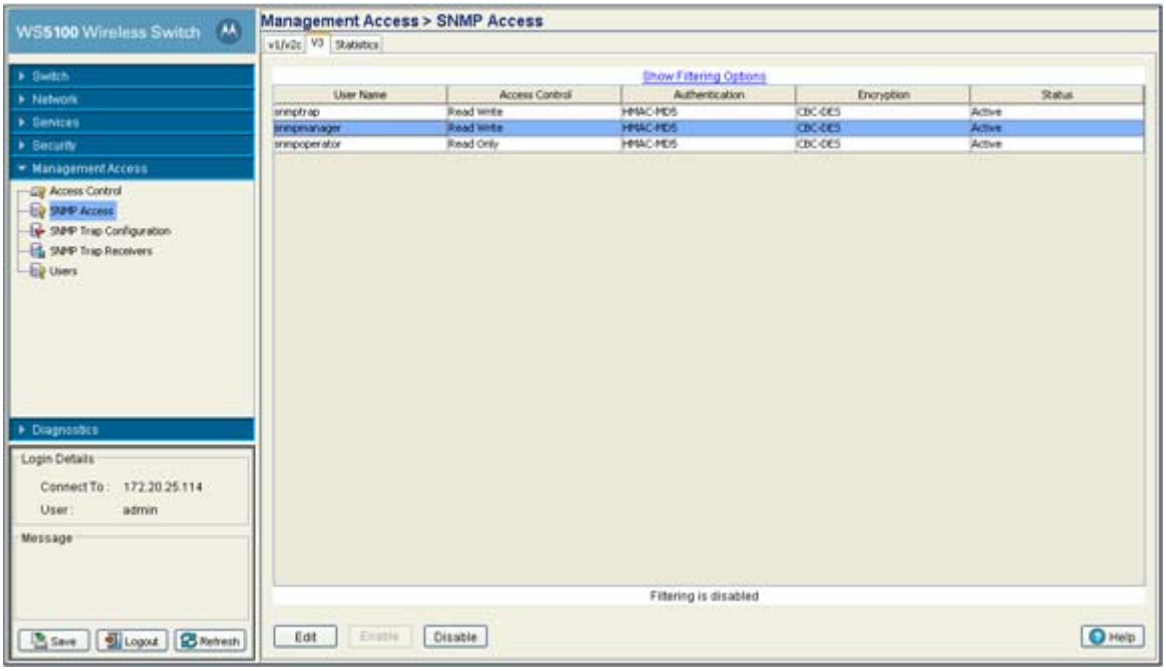
NOTE: The SNMP undo feature is not supported in this product.

CAUTION: The 3.x version WS5100 switch uses 3 unique (default) SNMPv3 user names and passwords for MD5 authentication and DES privacy. If upgrading your configuration from a 1.4.x or 2.x baseline, you will need to change your SNMPv3 usernames and passwords to ensure SNMPv3 interoperation.
The unique SNMPv3 usernames and passwords include:

username = snmpoperator/password = operator
username = snmpmanager/password = symboladmin
username = snmptrap/password = symboladmin

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. Operator typically has an Access Control of read-only and 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 the authentication keys.
Encryption	Displays the current *Encryption Standard* (DES) protocol the user must adhere to for SNMP v3 access to the switch. Click the **Edit** button to modify the password required to change the encryption keys.
Status	Displays whether this specific SNMP v3 User Name is currently 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.

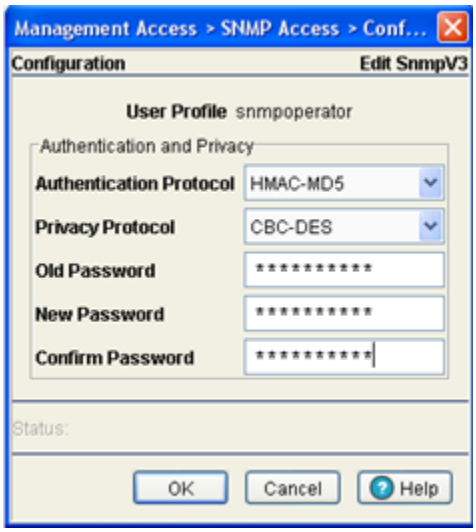
   For additional information, see *Editing an Existing SNMP v1/v2 Community Name on page 7-6*

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.

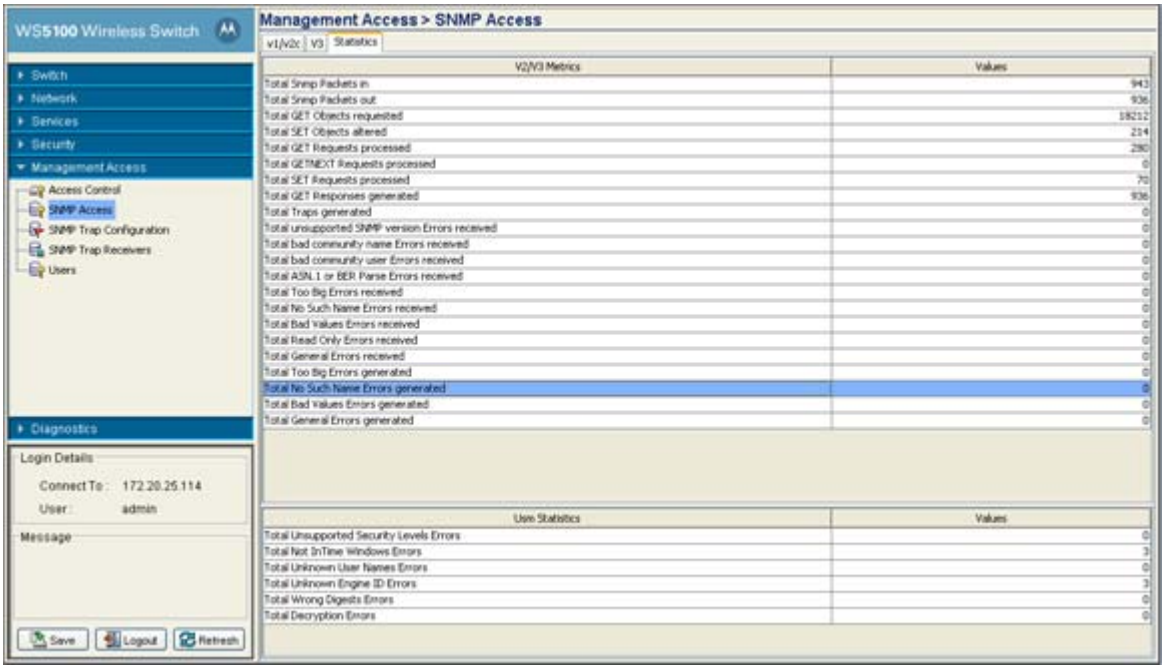
4. Enter the **Old Password** used to grant Authentication Protocol and Privacy Protocol permissions for the User Profile.
5. Enter the **New Password**, then verify the new password within the **Confirm New Password** area.
6. Click **OK** to save and add the changes to the running configuration and 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 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 trap generation individually or by functional group. It is also used for modifying the existing threshold conditions values for individual trap descriptions. The SNMP Trap Configuration window consists of the following tabs:

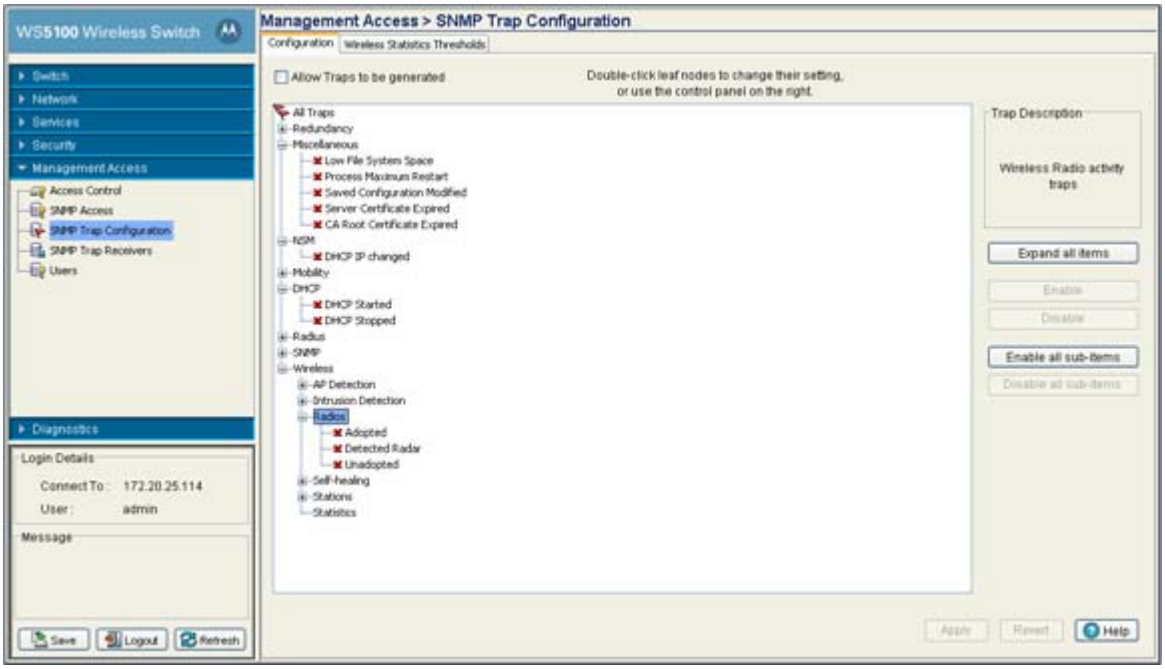
- *Enabling Trap Configuration*
- *Configuring Trap Thresholds*

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 traps within the screen. Leaving the checkbox unselected renders the trap selection un-configurable.
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 "Redundnacy" 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.
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.

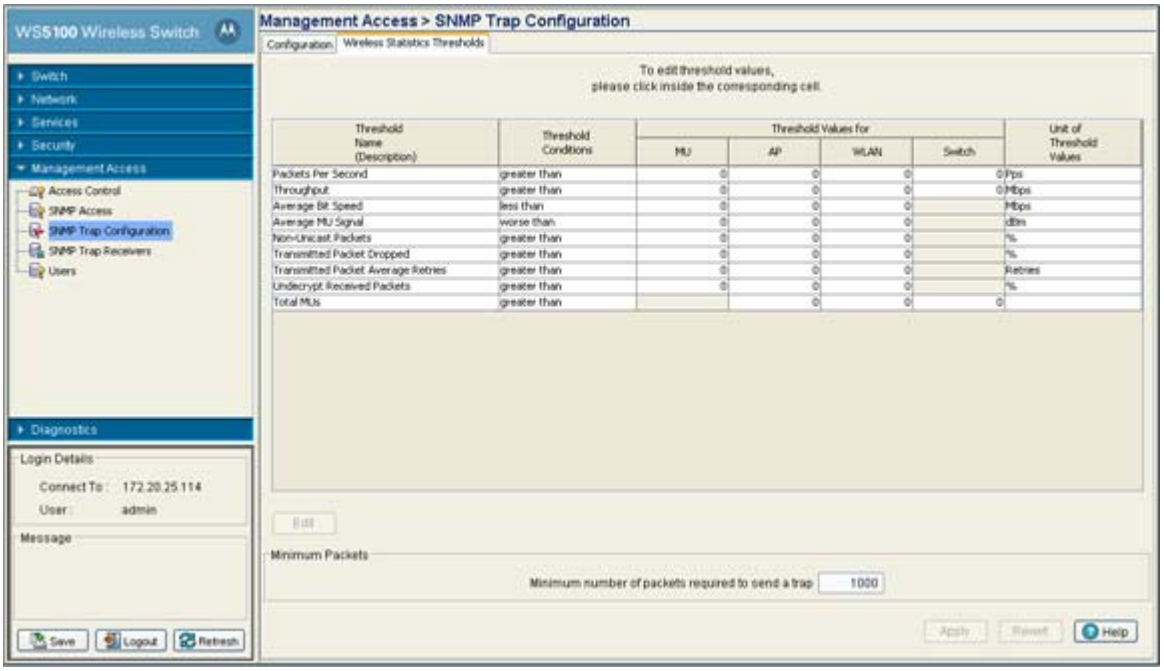
11. Click **Revert** to discard any updates and revert back to its last saved configuration.

7.4.2 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, 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.

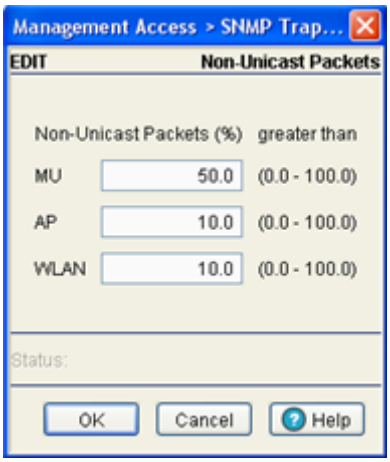


3. Refer to the following information for thresholds descriptions, conditions, editable threshold values and units of measurement.

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 7-15*.
Threshold values for: AP	Set a threshold value for associated radios. Use the **Threshold Name** and **Threshold Conditions** as input criteria to define an appropriate Threshold Value unique to the radios within the network. For information on specific values, see *Wireless Trap Threshold Values on page 7-15*.
Threshold values for: WLAN	Define a threshold value for associated WLANs. Use the **Threshold Name** and **Threshold Conditions** as input criteria to define an appropriate Threshold Value unique to the WLANs within the network. For information on specific values, see *Wireless Trap Threshold Values on page 7-15*.
Threshold values for: Switch	Use the **Threshold Name** and **Threshold Conditions** as input criteria to define an appropriate Threshold Value unique to the module. For information on specific values, see *Wireless Trap Threshold Values on page 7-15*.
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 7-15*.

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 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 7-15* 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:

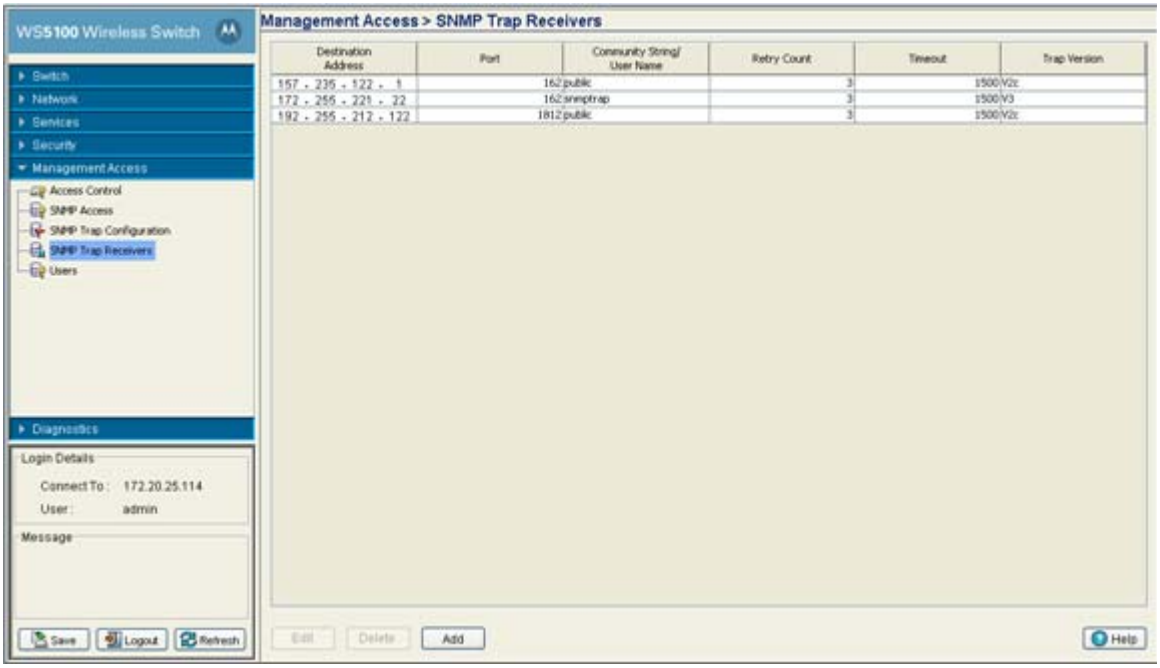
#	***Threshold Name***	***Condition***	***Station Range***	***Radio Range***	***WLAN Range***	***Wireless Service Range***	***Units***
1	Packets per Second	Greater than	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 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, retry count, timeout 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 the traps sent by the SNMP agent.
Port	The **Port** specifies a destination User Datagram Protocol receiving traps.
Community	Enter a Community name specific to the SNMP-capable client that receives the traps. The community name is public.
Retry Count	The Retry Count specifies the maximum number of retries attempted (to reach the destination address) before the session times out.
Timeout	The Timeout value specifies the time (in seconds) for the retransmission of packets. If this time is exceeded, the session is terminated. The deafult (and permanent value is 1500).
Trap Version	The Trap Version defines the kind of trap that will be made by the SNMP-capable client that is 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 the 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 7-17*.

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 7-17*.

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 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 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** window to view the administrative privileges assigned to different types of switch users. You can configure the associated roles and access modes assigned to each user. This window also allows you to configure the authentication methods used by the switch. This window consists of the following tabs:

- *Configuring Local Users*
- *Configuring Switch Authentication*

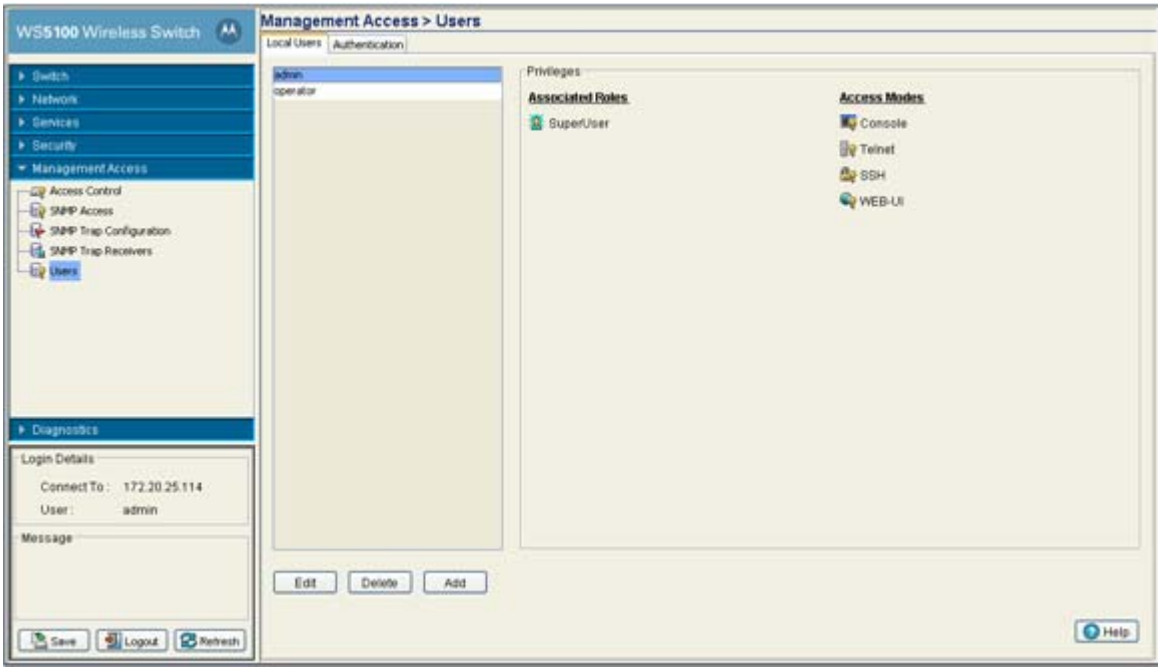
Additionally, the switch Web UI has the facility for creating guest administrators for the purpose of creating guest users with defined login periods to specific guest groups. For more information, see *Creating a Guest Admin and Guest User on page 7-22*.

7.6.1 Configuring Local Users

Refer to the Local User tab to view the administrative privileges assigned to different types of switch 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 sections:

- Users – This frame displays the users authorized to use the switch. By default the switch has two default users, Admin and Operator.

- Privileges – This frame displays the privileges assigned to different type of user.

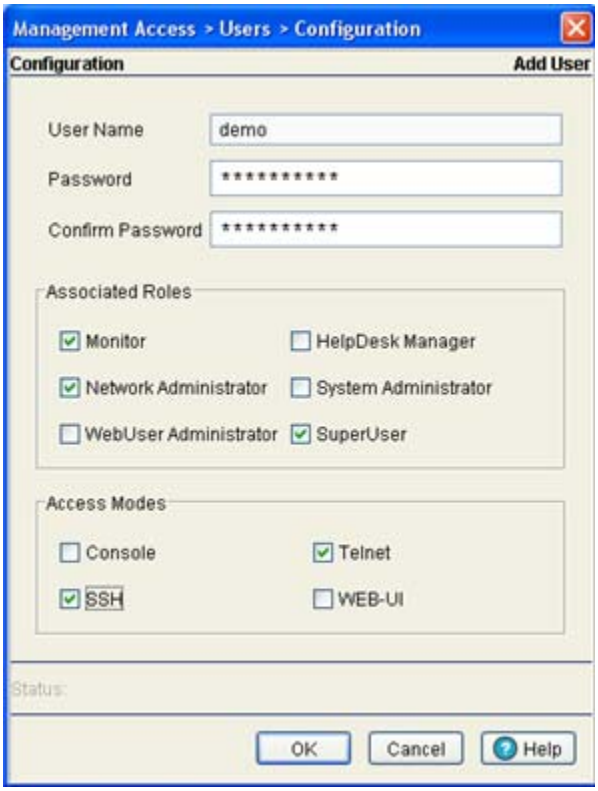
3. Select the user (Admin, Operator or user defined) from the **Users** frame and the **Privilege** frame displays the rights authorized to the user.
4. Click on the **Edit** button to modify the associated roles and access modes of the selected user. By default, the switch has two default users – Admin 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.



3. Enter the login name for the user in the **Username** field.
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** provides configures all wired and wireless parameters like IP config, VLANs, L2/L3 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 like exit, logout, help available to all the 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 applet 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).

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 log name of the user.
4. Enter the new authentication password for the user in the **Password** field and reconfirm the same again in the **Confirm Password** field.

5. Select the role to assign to the user 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, L2/L3 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 the 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	This option provides the new user access to the switch using the console (applet).
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 Telnet
Applet	This option provides the new user access to the switch the Web UI (applet).

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 the purpose of 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:

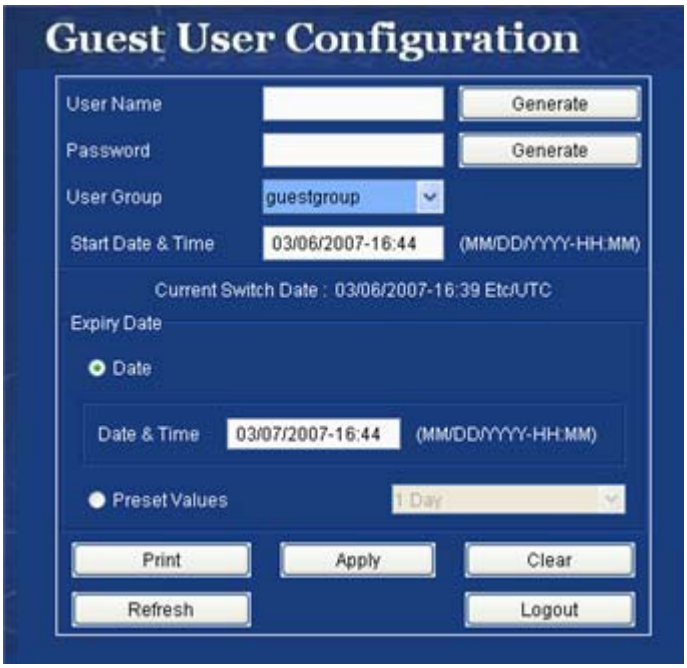
1. Select **Management Access** > **Users** from the main menu tree.
2. Click the **Add** button.

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 be able to create guest users, a guest administrator must be assigned a **WebUser Administrator** access mode. None of the other modes will 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.

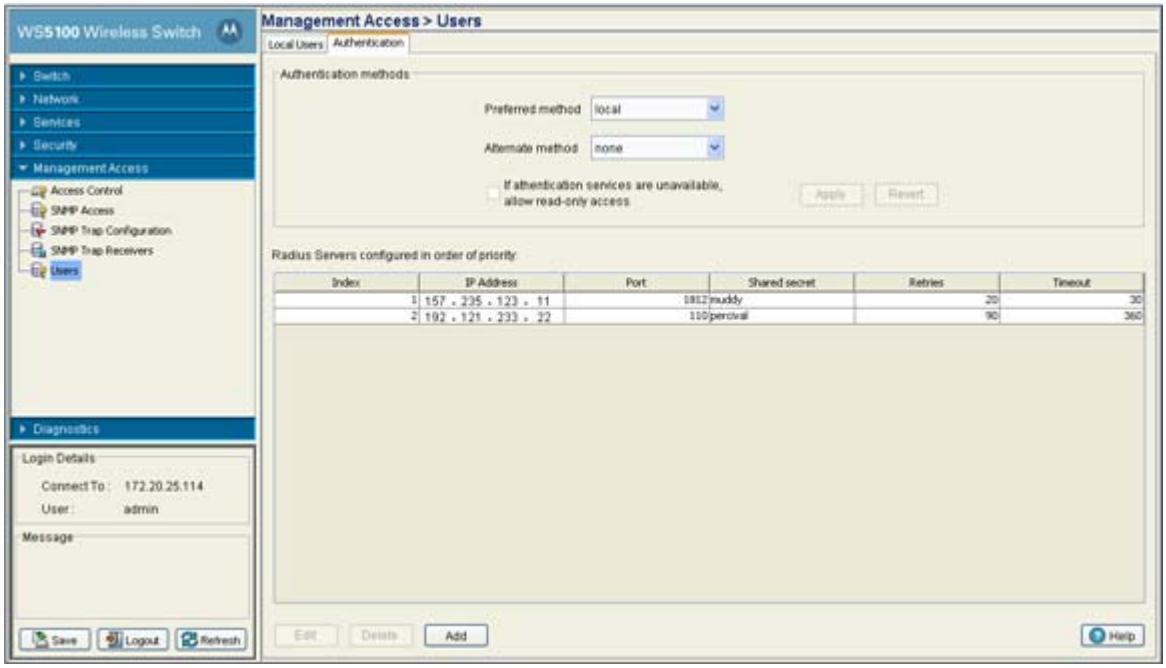
7.6.2 Configuring Switch Authentication

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 activities 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. Click on 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** value 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 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 for the switch to retransmit a Radius Server frame before it times out 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 7-25*.
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 a New Radius Server on page 7-26*.

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 WS5100 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	Revise the numerical **Index** value for the Radius Server to help distinguish this Radius Server from other servers with a similar configuration (if necessary). The maximum number that can be assigned is 32.
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 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	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 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 modification of the Radius Server.
7. Click **Cancel** to revert back to the last saved configuration without saving any of your changes.

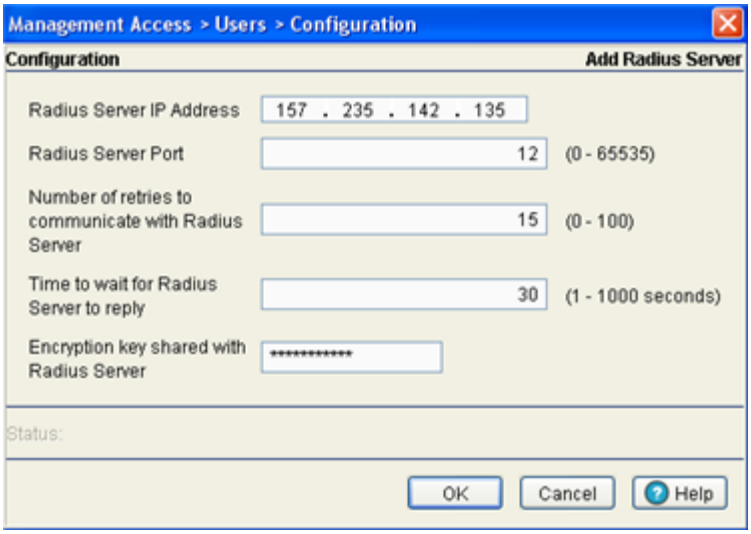
7.6.2.2 Adding a New Radius Server

The attributes of a new Radius Server can be defined by the WS5100 to provide a new user authentication server. Once the Radius 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	Define 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 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.

8

Diagnostics

This chapter describes the various diagnostic features available to monitor switch performance. It consists of the following sections:

- *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

Use the main diagnostic screen to configure and monitor the following switch features:

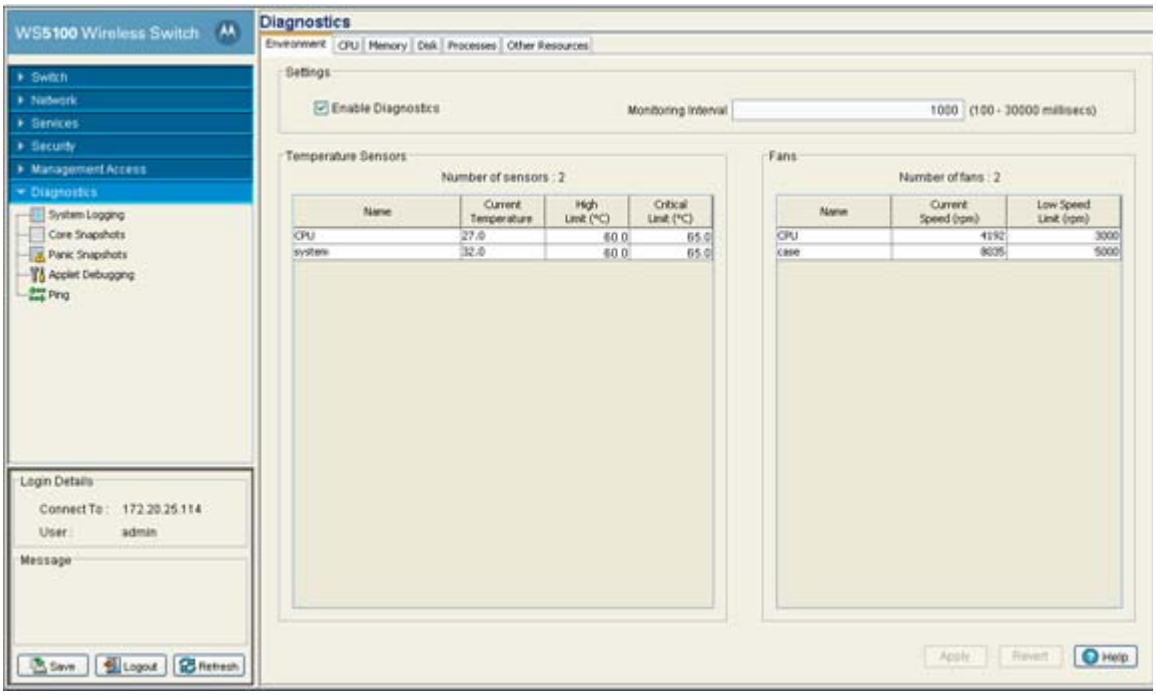
- *Switch Environment*
- *CPU Performance*
- *Switch Memory Allocation*
- *Switch Disk Allocation*
- *Switch Memory Processes*
- *Other Switch Resources*

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** screen 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.



3. The Environment tab has 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.

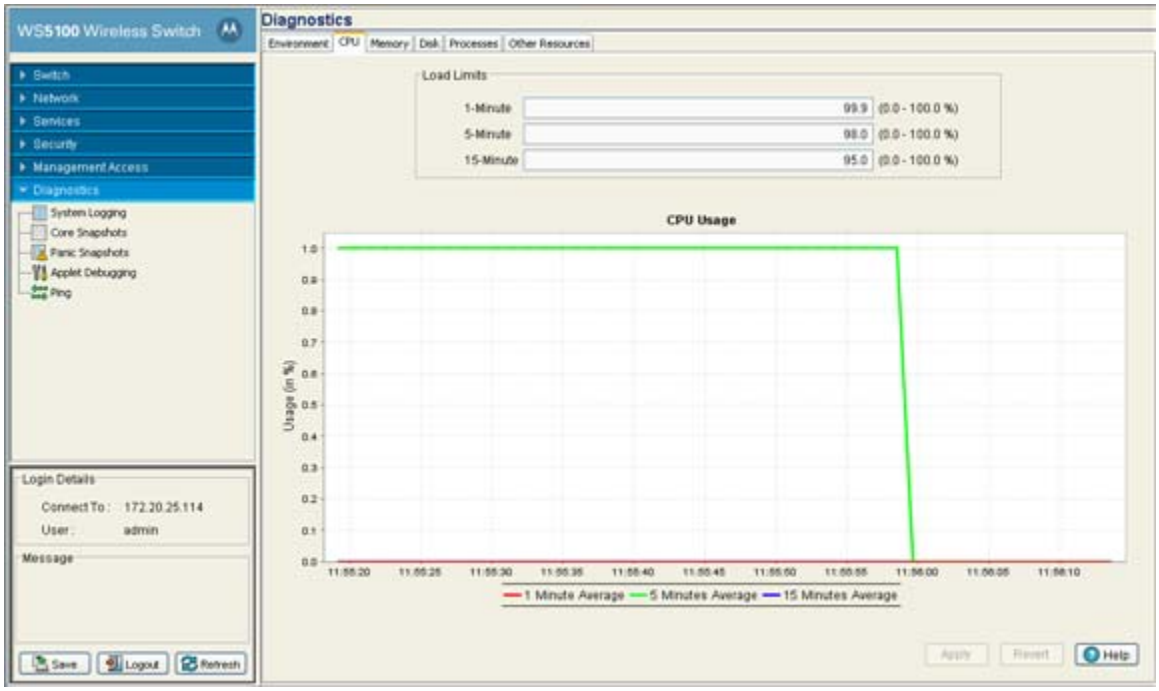
NOTE: Enabling switch diagnostics is recommended, as the diagnostics facilities provide detailed information on the physical performance of the switch and may provide indicators in advance of actual problems. Enabling diagnostics also assists in the troubleshooting problems associated with data transfers 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.
6. Refer to the **Fans** field to monitor the CPU and system fan speeds. Unlike a RFS7000 model switch, a WS5100 has two fans.
7. Click on 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** screen to view and modify the CPUs load statistics in terms of last 1, 5, and 15 minutes.

1. Select **Diagnostics** from the main tree menu.
2. Select the **CPU** tab.

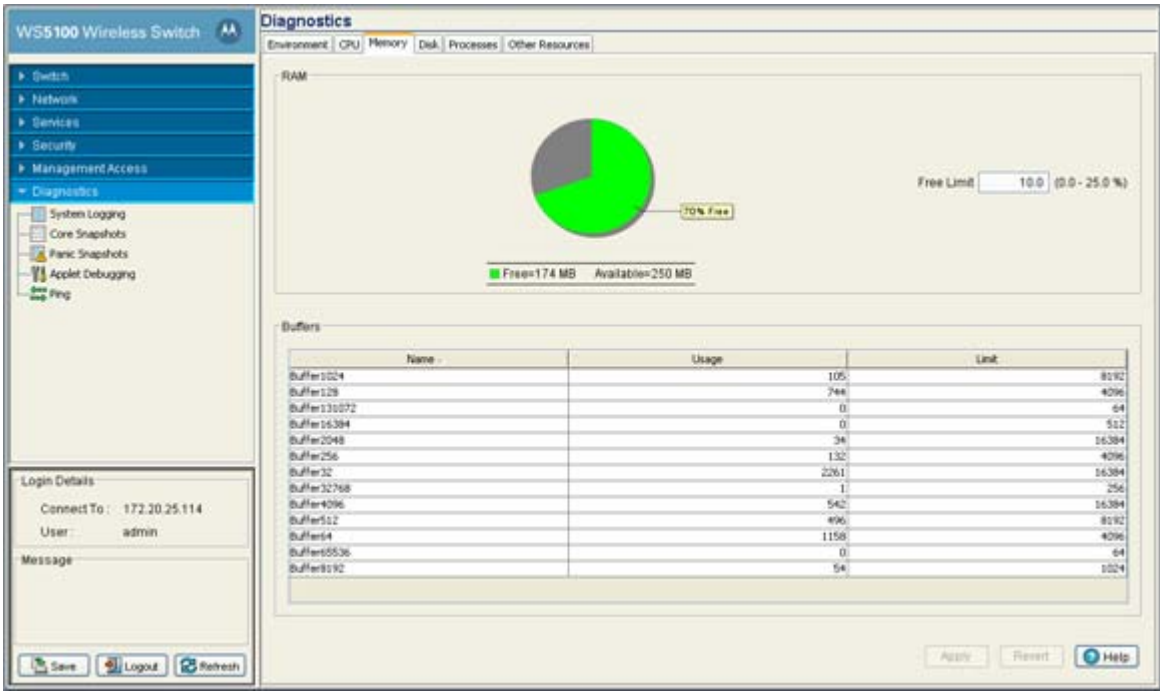


3. The CPU screen has 2 fields:
   - Load Limits
   - CPU Usage
4. The **Load Limit** field displays the CPU load statistics in terms of last 1, 5, and 15 minutes. The limits displayed coincide with periods of increased or decreased switch activity.
5. The **CPU Usage** field displays the real time CPU consumption values from the switch. Use this information to periodically determine if performance is negatively impacted by the overusage of switch CPU resources. If the 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** screen to assess the CPU's load over the last 1, 5, and 15 minutes.

1. Select **Diagnostics** from the main tree menu.
2. Select the **Memory** tab.



The Memory tab has 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. Use the **Free Limit** field to change the CPUs memory allocation limits. The Free Limit field should be configured in respect to high bandwidth and increased load anticipated over the switch managed network.
4. The **Buffers** field displays buffer usage information. It consists of a table with the following information:

Name	The name of the buffer.
Usage	Buffers current usage
Limit	The buffer limit.

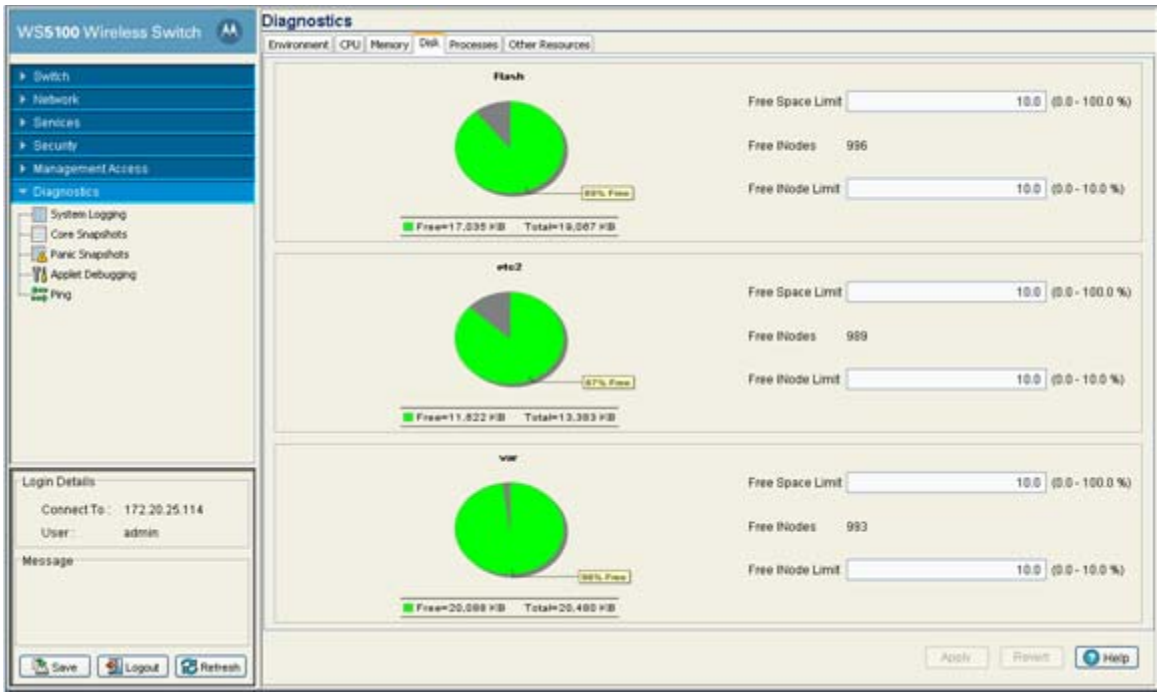
5. Click the **Apply** button to commit and apply the changes.
6. Click the **Revert b**utton to revert back to the last saved configuration.

8.1.4 Switch Disk Allocation

The Disk tab contains all parameters related to the various disk partitions on the switch. It also displays available space in the external drives (such as USB drive or compact flash etc).

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

2. Select the **Disk** tab.



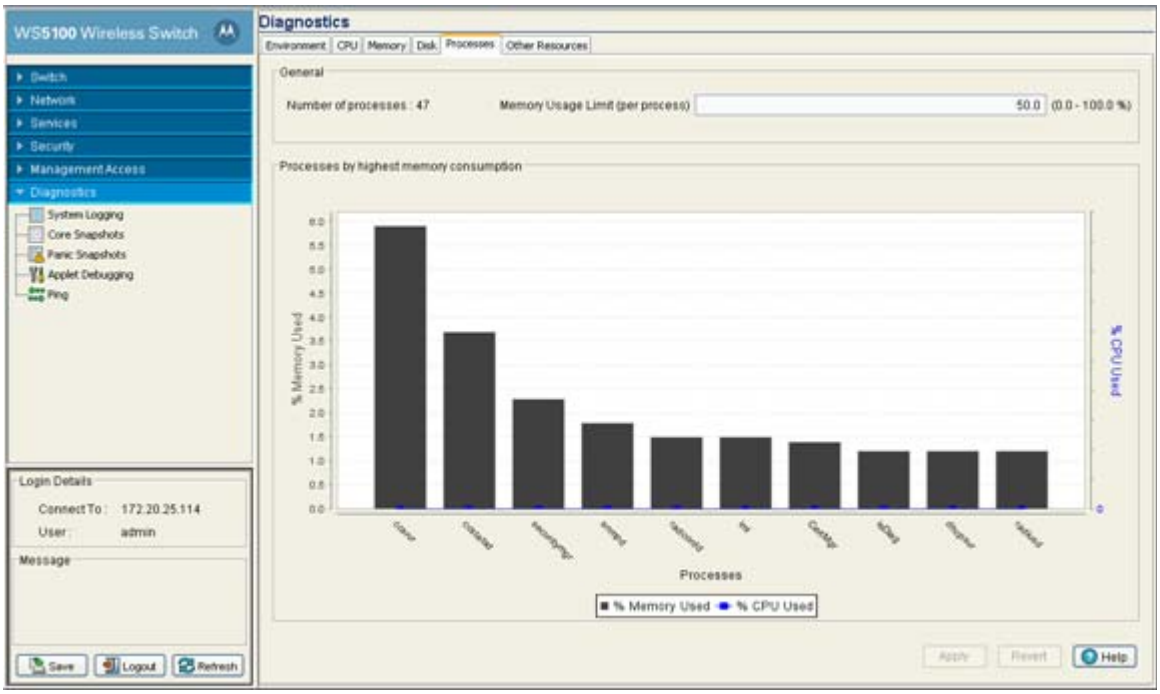
3. This Disk tab displays the status of the various disks on the switch. Each section displays the following information:
   - Maximum Limit
   - Free INodes
   - Free INode Limit
4. Use the **Free Limit Space** variable carefully, as disk space may be required during periods of high bandwidth traffic 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



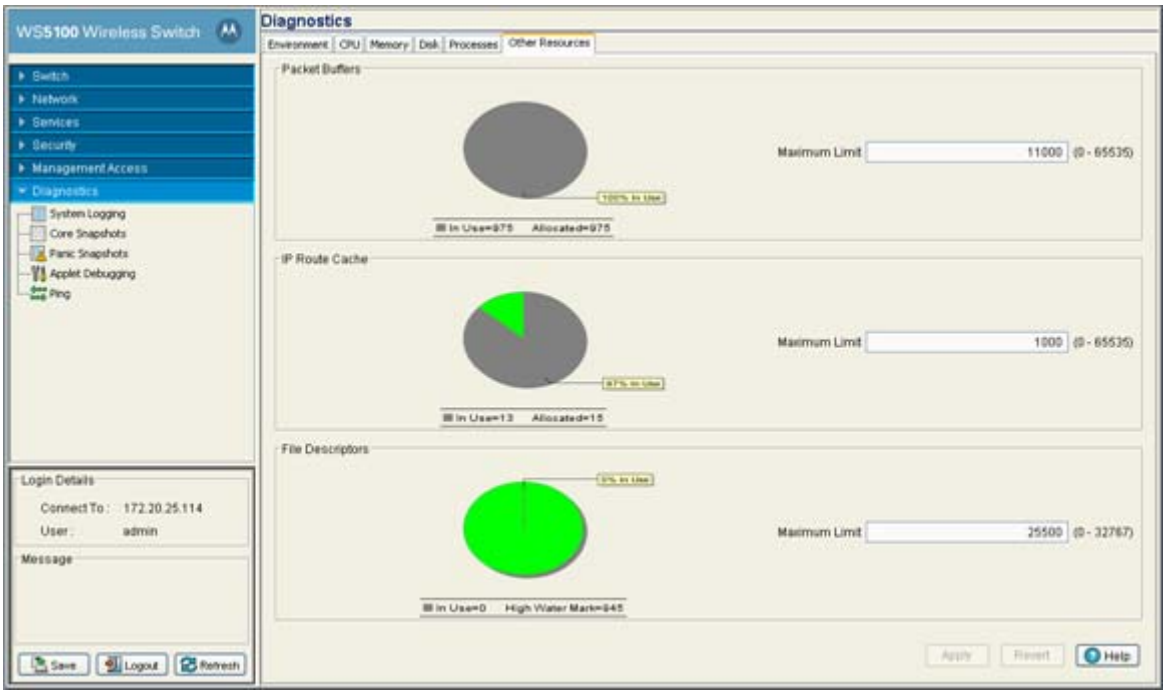
3. The Processes tab has 2 fields:
   - General
   - Processes by highest memory consumption
4. Refer to the **General** field for the number of processes in use and percentage of memory usage per process. The value defined is the maximum limit per process during periods of increased and network activity 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 the changes.
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.



The Other Resources tab displays the memory allocation of Packet Buffer, IP Route Cache and File Descriptors. Keep the Cache allocation in line with cache expectations required within the switch managed network.

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 natively impacting switch performance. The System Logging screen consist of the following tabs:

- *Log Options*
- *File Management*

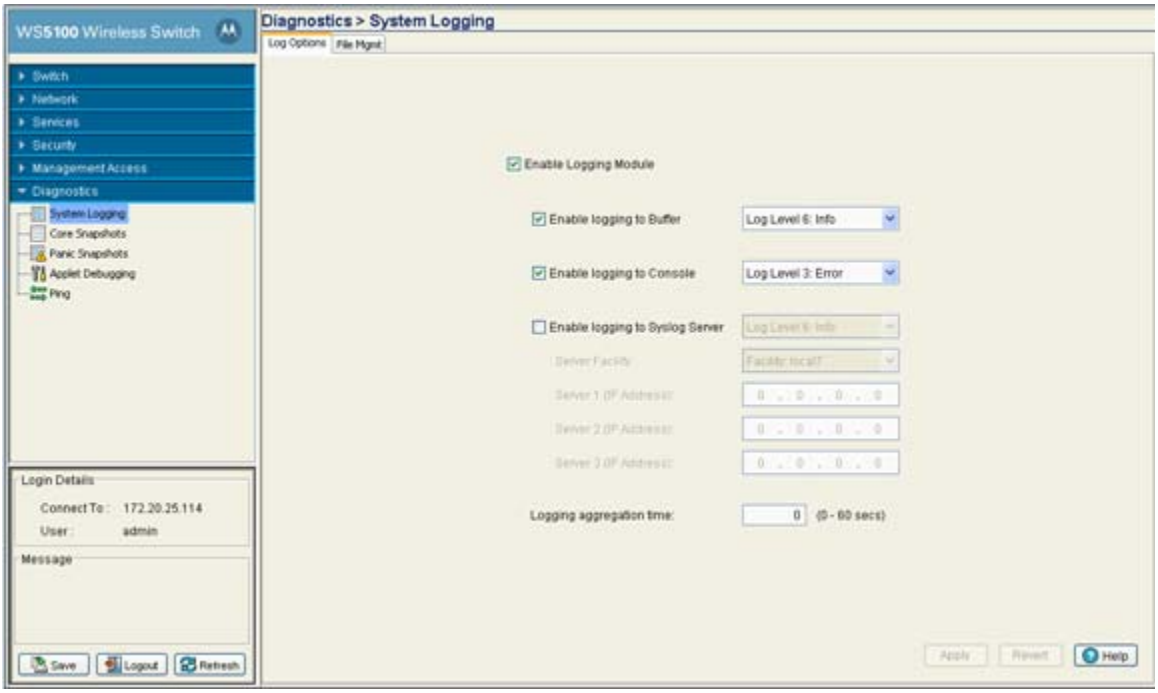
8.2.1 Log Options

Use the Log Options screen 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:

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 local 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. Use the drop-down menu to select the desired log level for tracking system events to a local log file.
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.
6. Select the **Enable Logging to Syslog Server** checkbox to enable the switch to log system events for tracking system events and sending 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 in 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.

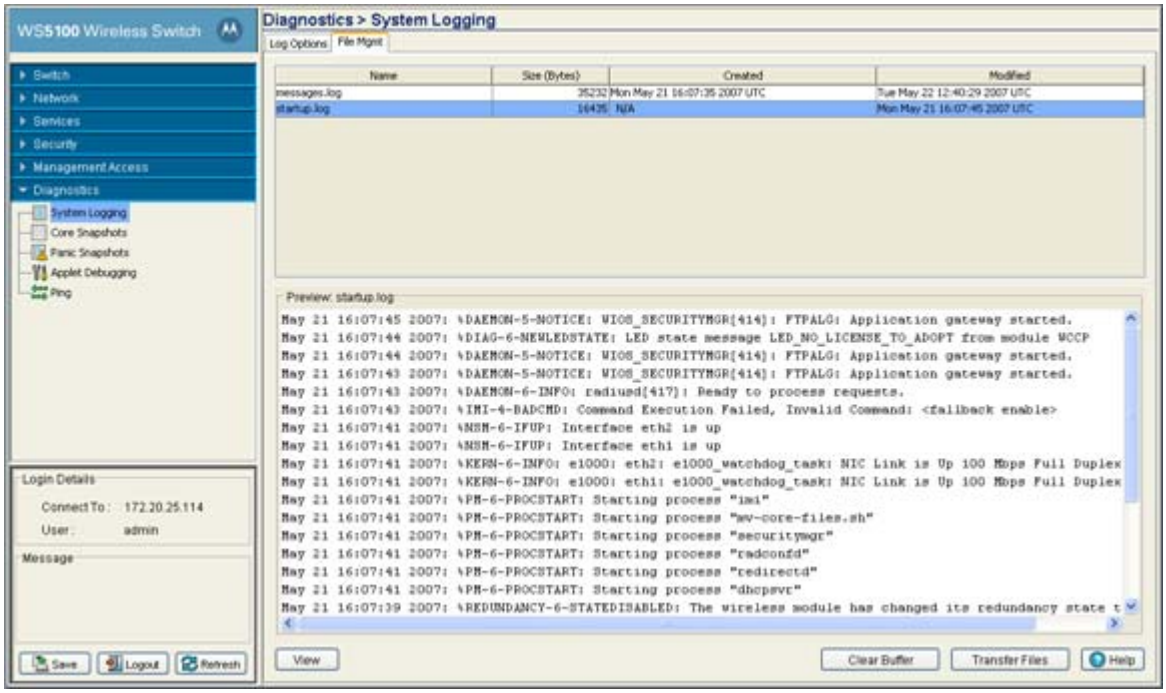
9. Click the **Revert** button to move the display back to the last saved configuration.

8.2.2 File Management

Use the **File Mgt** screen 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 **System Logging** screen displays existing log files. Refer to the following for log file details:

Name	Displays a read-only list of the log files 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.

   The time, module, severity, mnemonic and description of the file are displayed. For a more detailed description of the entire log file click the **View** button.

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 to be cleared.

7. Click the **Transfer Files** button to display a sub-screen wherein log files can be sent to an external location (as defined by you) via a user-defined file transfer medium.

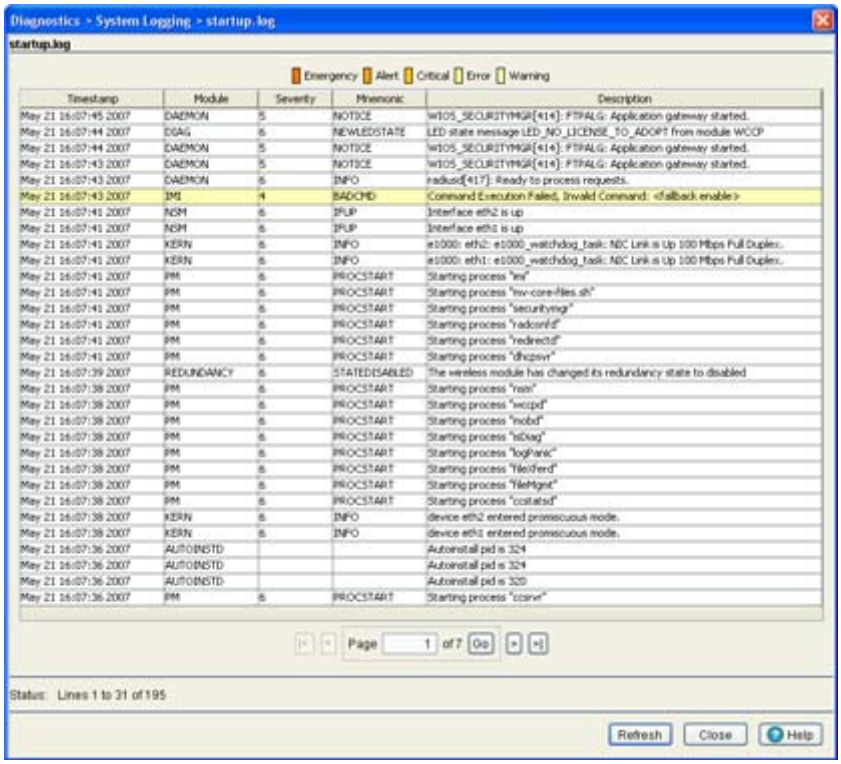
   Transferring files is recommended when the log file is frequently cleared, but an archive of the log files is required in a safe location. For more information on transferring individual log files, see *Transferring Log Files on page 8-11*.

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** > **File Mgt** from the main menu tree.
2. Select an individual log file whose properties you wish to display in detail and click the **View** button.



3. 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.
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 purposes or for metric collection.

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 the **Refresh** button to update the contents of the screen to the latest values.
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 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** > **File Mgt** from the main menu tree.

2. Select a target log file to transfer and click the **Transfer File** button.

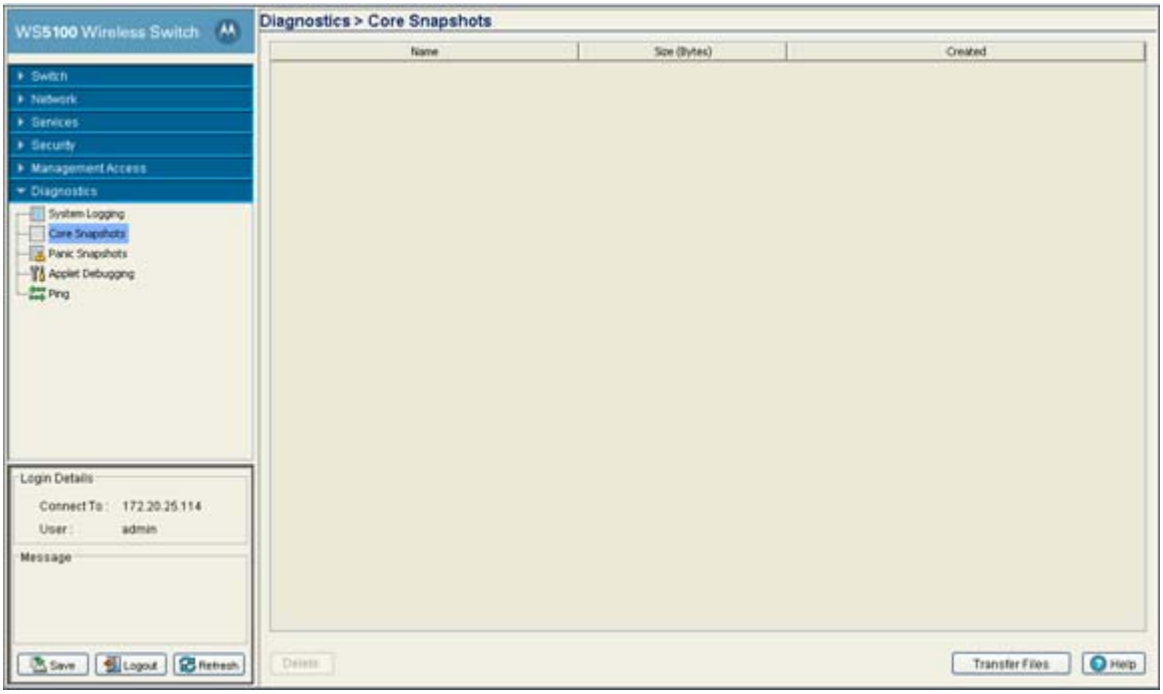
3. Use the **From** drop-down menu (within the Source field) to specify the location from which the log file is sent. If only the applet is available as a transfer location, use the default switch option.
4. Select a target file for transfer from the **File** drop-down menu. The drop-down menu contains the log 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 within the **File** parameter. Ensure the file name is correct.
7. If Server has been selected as the source, use the **Using** drop down-menu to configure whether the log 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 log file. Ensure the IP address is valid or risk jeopardizing the success of the log file transfer.
9. If Server has been selected as the source, enter the **User ID** credentials required to send the log file to the target location.
10. 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.
11. 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.
12. 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.
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 **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 .core extension) logged by the system impacting the switch core (or distribution layer) events. Once reviewed, core files can be deleted or transferred for potential archive.

To view the 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 8-13*.

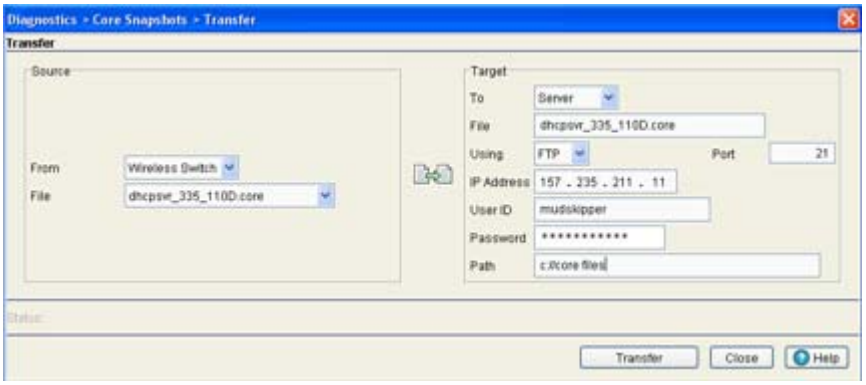
8.3.1 Transferring Core Snapshots

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 will be 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** name 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.

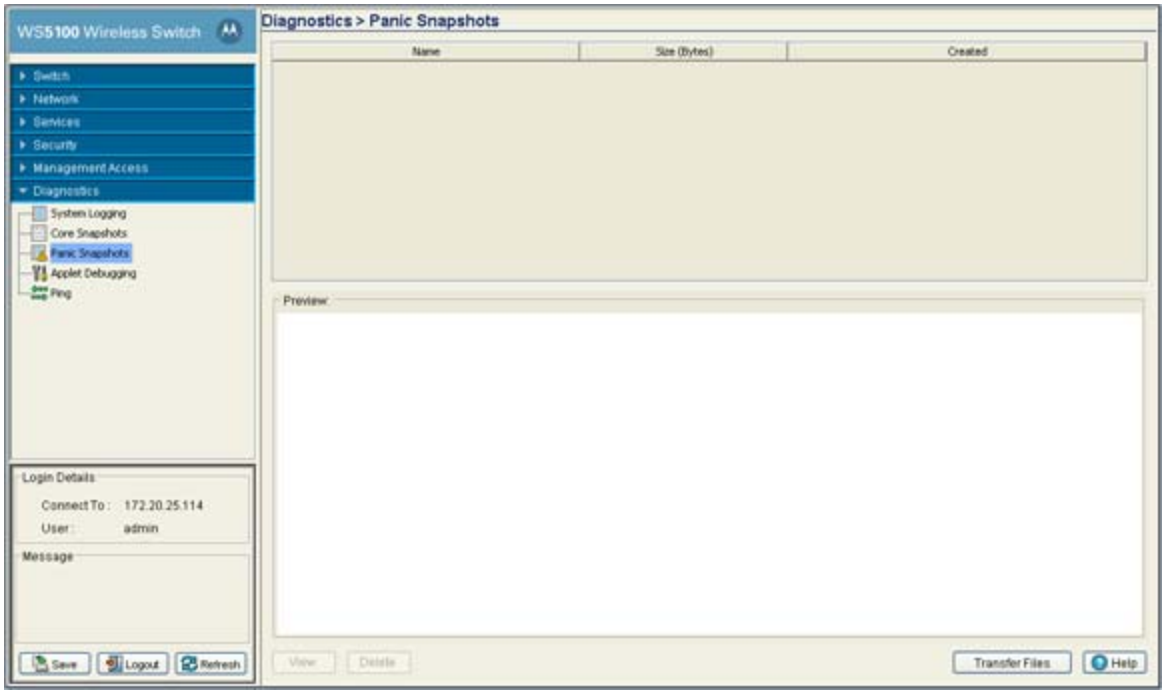
14. Click the **Close** button to exit the screen after a transfer. There are no changes to save or apply.

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 you can 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. 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:

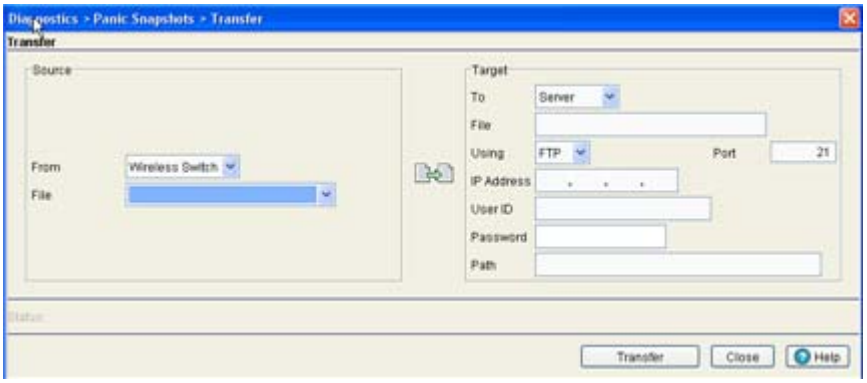
Main	The **Main** parameter displays detailed panic information for the selected kernel.
Page	Panic information may be spread across multiple pages. The Page value allows the user to view complete information on the panic. Use the < and > options to navigate through the contents of the file.
Refresh	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 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.



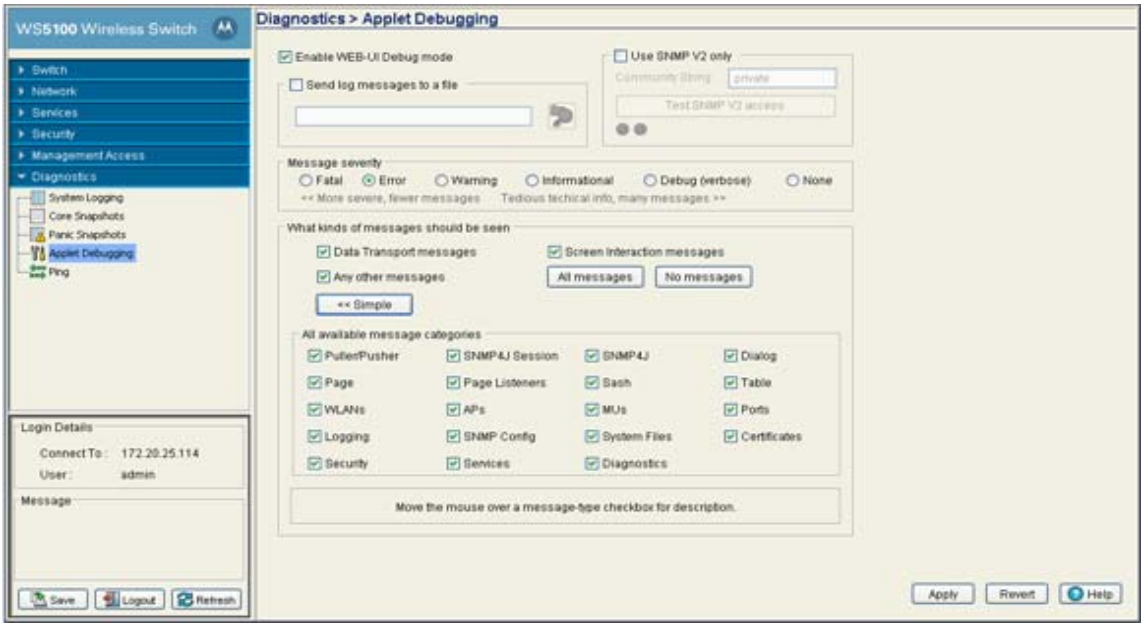
3. Use the **From** drop-down menu to specify the location from which the file is sent. If only the applet is available as a transfer location, use the default switch option.
4. Select a file for the file transfer from the **File** drop-down menu. The drop-down menu contains the panic files listed within 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 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 **Make 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. 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 Applet Debug Mode** checkbox.
3. The Applet Debugging window has the following sections:
   - Send log message to a file.
   - Use SNMP v2 only.
   - Message Severity.

- What kinds of message should be seen.

4. 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.

5. 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.

6. Select the severity of the message that 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.

7. Select the message when a bug is raised.

   The **What Kind of message should be seen** field allows you to select a range of parameters for which you can see a message while you debug. Place your mouse pointer over the message type check box for the message description.

   a. Click the **Advanced** button to display the entire list of message categories for when switch 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.

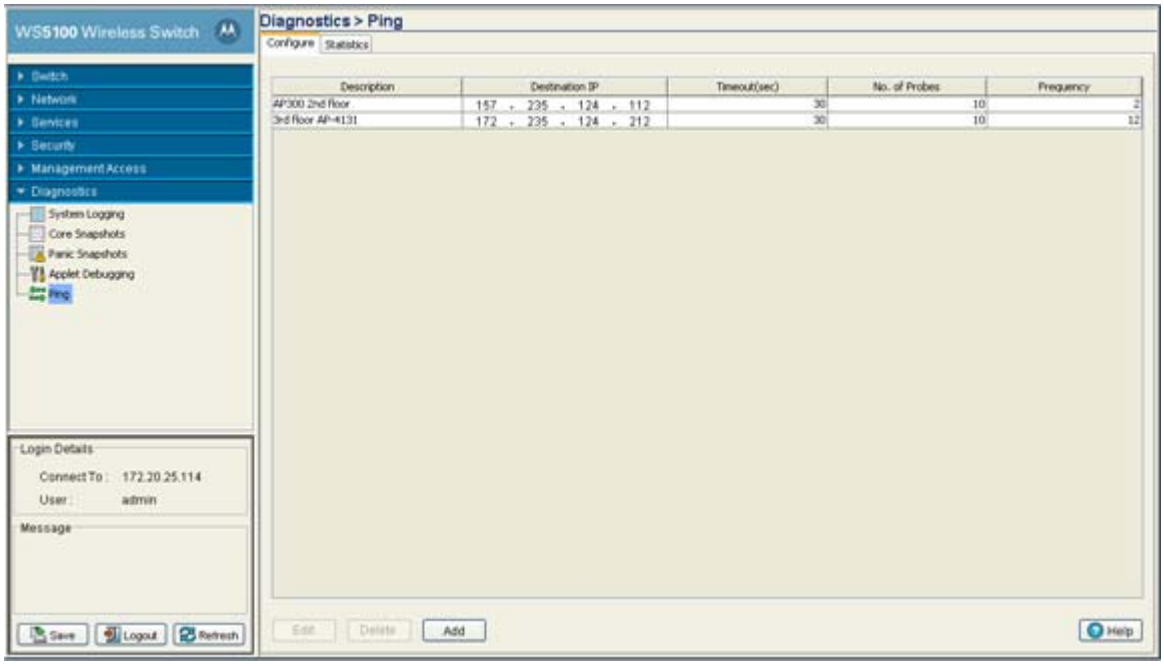
8. Click the **Apply** button to save the changes you have applied within this screen.
9. Click the **Revert** button to revert back to the last saved configuration.

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 transmitted by the switch, statistics are gathered for the *round-trip time* (RTT) between switch and 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 because of 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, modified under the same description 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.
Timeout (sec)	Displays 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.
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	Displays the interval between ping packet transmissions.

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 8-20*.
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 in order 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 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.

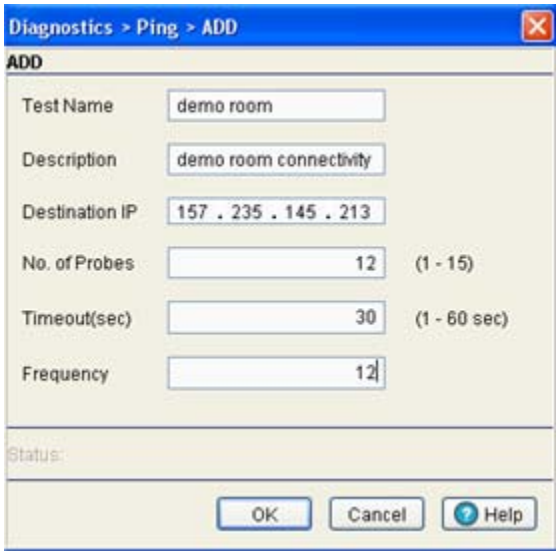
8.6.2 Adding a New Ping Test

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 ping test, a new ping 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 to be 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 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	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.

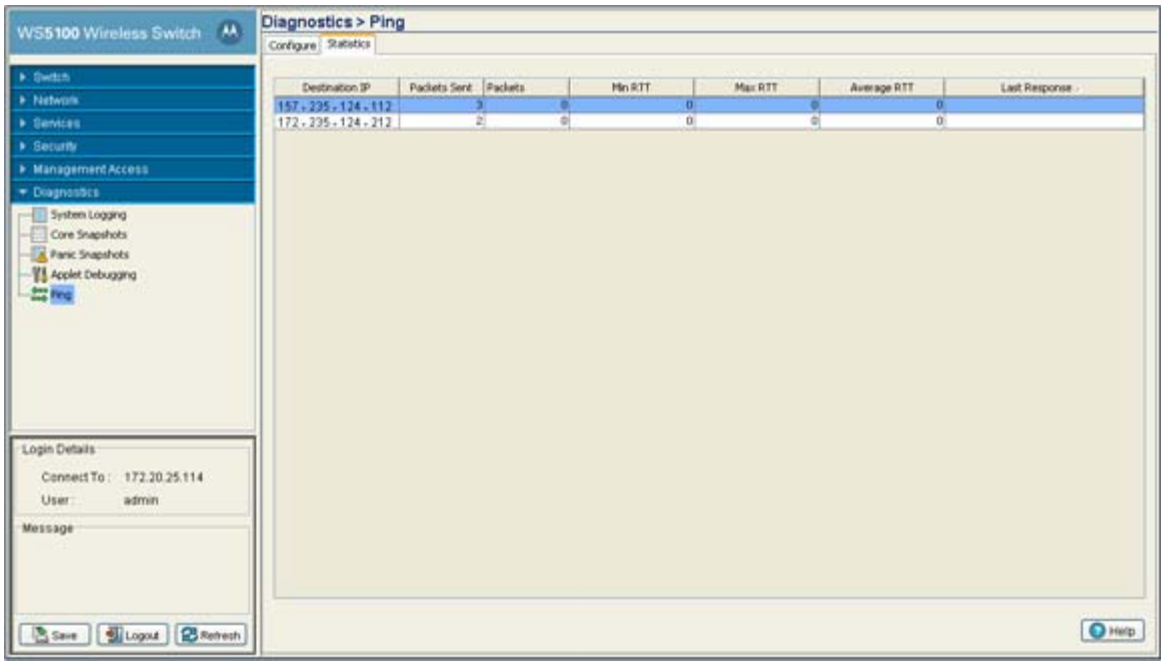
4. Click **OK** to save and add the changes to the running configuration and close the dialog.
5. Refer to the **Status** field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the switch
6. Click **Cancel** to return back to the Configuration tab without implementing changes.

8.6.3 Viewing Ping Statistics

Refer to the Ping 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 that could offer 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 from the switch 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 back from the target device. If this number is significantly lower than the number sent to the target device from the switch, then 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 lightest 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 connection with the switch.

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 at: *http://www.symbol.com/contactsupport*.

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, located at *www.symbol.com/support* provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

Downloads

http://symbol.com/downloads

Manuals

http://symbol.com/manuals

General Information

Obtain additional information by contacting Motorola at:

1-800-722-6234, inside North America

+1-516-738-5200, in/outside North America

http://www.motorola.com/

MOTOROLA INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-100957-01 Revision A
June 2007