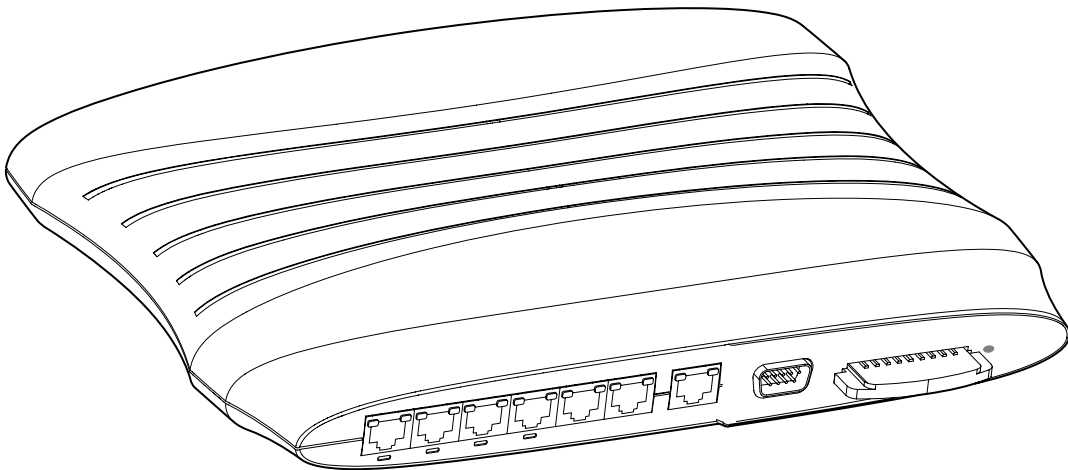


# WS2000 Wireless Switch

## System Reference Guide



© 2009 Motorola, Inc. All rights reserved.

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

# Contents

## Chapter 1: Product Overview

1.1 WS2000 Wireless Switch System Reference Guide .....	1-2
1.1.1 About this Document .....	1-2
1.1.2 Document Conventions .....	1-2
1.2 System Overview .....	1-3
1.2.1 Management of Access Ports .....	1-3
1.3 Hardware Overview .....	1-4
1.3.1 Technical Specifications .....	1-4
1.3.2 WS2000 Wireless Switch LED Functions .....	1-5
1.4 Software Overview .....	1-6
1.4.1 Operating System (OS) Services .....	1-6
1.4.2 Cell Controller Services .....	1-6
1.4.3 Gateway Services .....	1-6

## Chapter 2: Getting Started

2.1 Getting Started with the WS2000 Wireless Switch .....	2-2
Step 1: Install the Switch .....	2-2
Step 2: Set Up Administrative Communication to the Switch .....	2-2
Step 3: Set the Basic Switch Setting .....	2-4
Step 4: Configure the LAN Interface .....	2-5
Enable Subnet1 .....	2-5
Step 5: Configure Subnet1 .....	2-6
Step 6: Configure the WAN Interface .....	2-7
Communicating with the Outside World .....	2-7
Setting Up Point-to-Point over Ethernet (PPPoE) Communication .....	2-8
Step 7: Enable Wireless LANs (WLANs) .....	2-9
Wireless Summary Area .....	2-9
Step 8: Configure WLAN Security .....	2-10
Setting the Authentication Method .....	2-11
Setting the Encryption Method .....	2-11
Mobile Unit Access Control List (ACL) .....	2-11
Step 9: Test Connectivity .....	2-12
2.2 Where to Go from Here? .....	2-12

## Chapter 3: LAN/Subnet Configuration

3.1 Enabling Subnets for the LAN Interface .....	3-2
3.1.1 Defining Subnets .....	3-2
3.2 Configuring Subnets .....	3-3

3.2.1 The DHCP Configuration .....	3-5
3.2.2 Advanced DHCP Settings .....	3-5
3.3 Configuring Subnet Access .....	3-7
3.3.1 The Access Overview Table .....	3-7
3.3.2 The Access Exception Area .....	3-8
3.4 Advanced Subnet Access Settings .....	3-10
3.5 Bridge Configuration .....	3-12
3.6 Virtual LAN (VLAN) Configuration .....	3-14
3.7 Configuring IP Filtering .....	3-15
3.8 URL Filtering .....	3-18
3.9 Port Configuration .....	3-20

## Chapter 4: WAN Configuration

4.1 Configuring the WAN Interface .....	4-2
4.1.1 Configuring WAN IP Information .....	4-2
4.1.2 Setting Up Point-to-Point over Ethernet (PPPoE) Communication .....	4-3
4.2 Configuring the WS2000 Firewall .....	4-5
4.2.1 Disabling the Firewall .....	4-5
4.2.2 Setting the NAT Timeout .....	4-5
4.2.3 Configurable Firewall Filters .....	4-6
4.2.4 Enabling NetBIOS ALG .....	4-7
4.3 Configuring Intrusion Prevention System .....	4-9
4.4 Configuring Network Address Translation (NAT) .....	4-12
4.5 Configuring Static Routes .....	4-14
4.5.1 Configuring the Default Gateway Interface .....	4-14
4.5.2 Creating User Defined Routes .....	4-15
4.5.3 Setting the RIP Configuration .....	4-15
4.6 Configuring a Virtual Private Network (VPN) .....	4-17
4.6.1 Creating a VPN Tunnel .....	4-18
4.6.2 Setting Up VPN Security .....	4-19
4.6.3 Configuring Manual Key Exchange .....	4-19
4.6.4 Setting Up Automatic Key Exchange .....	4-21
4.6.5 Setting Up Internet Key Exchange (IKE) .....	4-23
4.6.6 VPN: Frequently Asked Questions .....	4-25
4.7 Configuring Content Filtering .....	4-29
4.8 Configuring DynDNS .....	4-31
4.8.1 Enabling and Configuring DynDNS .....	4-31
4.8.2 Updating DynDNS .....	4-31

## Chapter 5: Wireless Configuration

5.1 Enabling Wireless LANs (WLANs) .....	5-3
5.1.1 WLAN Summary .....	5-3
5.1.2 AP Adoption Configuration .....	5-5
5.2 Configuring Wireless LANs .....	5-6
5.2.1 Configuring Advanced WLAN Settings .....	5-6



5.3 Configuring Wireless LAN Security .....	5-7
5.3.1 Selecting the Authentication Method .....	5-7
5.3.2 Configuring 802.1x EAP Authentication .....	5-8
5.3.3 Configuring Kerberos Authentication .....	5-10
5.3.4 Setting the Encryption Method .....	5-11
5.3.5 Configuring WEP Encryption .....	5-11
5.3.6 Configuring WPA/WPA2-TKIP Encryption .....	5-12
5.3.7 Configuring WPA2-CCMP (802.11i) Encryption .....	5-13
5.3.8 KeyGuard .....	5-14
5.3.9 No Encryption .....	5-15
5.3.10 IP Filtering .....	5-15
5.3.11 Mobile Unit Access Control List (ACL) .....	5-16
5.4 Configuring Access Ports .....	5-16
5.5 Setting Default Access Port Settings .....	5-19
5.5.1 Common Settings to All Radio Types .....	5-20
5.5.2 Radio-Specific Settings .....	5-22
5.6 Advanced Access Port Settings .....	5-23
5.6.1 Radio Settings .....	5-24
5.6.2 Antenna Settings .....	5-25
5.6.3 Access Port Properties .....	5-25
5.6.4 Advanced Properties .....	5-25
5.7 Quality of Service Configuration .....	5-27
5.7.1 Setting the Bandwidth Share Mode .....	5-28
5.7.2 Configuring Voice Prioritization and Multicast Address Settings .....	5-29
5.8 Setting Up Port Authentication for AP300 Access Ports .....	5-29
5.9 Rogue Access Point (Port) Detection .....	5-30
5.9.1 Setting Up the Detection Method .....	5-31
5.9.2 Defining and Maintaining Approved AP List Rules .....	5-32
5.9.3 Examine the Approve and Rogue Access Ports .....	5-33
5.9.4 Setting SNMP Traps for Rogue APs .....	5-36
5.10 Configuring Wireless Intrusion Protection System (WIPS) .....	5-37
5.11 Wireless Intrusion Detection System .....	5-38
5.11.1 WIDS Configuration .....	5-39
5.11.2 Filtered MUs .....	5-40
5.12 Smart Scan .....	5-41
5.13 Self Heal .....	5-42
5.14 Mesh Settings .....	5-43
5.14.1 Mesh Base Setting .....	5-44
5.14.2 Mesh Client Setting .....	5-44

## Chapter 6: Administrator and User Access

6.1 Configuring Administrator Access .....	6-2
6.1.1 Selecting the Type of Admin Access .....	6-2
6.1.2 Configuring Secure Shell Connection Parameters .....	6-3
6.1.3 Admin Authentication and RADIUS Server Authentication Setup .....	6-3
6.1.4 Setting Up AirBEAM Software Access .....	6-4

6.1.5	Applet Timeout Specification	6-4
6.1.6	Changing the Administrator Password	6-4
6.2	Configuring User Authentication	6-5
6.2.1	Configuring the RADIUS Server	6-5
6.2.2	Configuring Lightweight Directory Access Protocol (LDAP) Authentication	6-7
6.2.3	Setting Up a Proxy RADIUS Server	6-8
6.2.4	Managing the User Database	6-9
6.2.5	Adding New Guest Users Quickly	6-10
6.2.6	Setting the User Access Policy	6-13
6.3	Managing Digital Certificates	6-14
6.3.1	Importing CA Certificates	6-14
6.3.2	Creating Self Certificates	6-16

## Chapter 7: Switch Administration

7.1	Overview of Administration Support	7-2
7.2	Restarting the WS2000 Wireless Switch	7-2
7.3	Changing the Name of the Switch	7-3
7.4	Changing the Location and Country Settings of the WS2000	7-3
7.5	Configuring the DNS Server Information	7-4
7.6	Configuring the Domain Name for the switch	7-5
7.7	Configuring Switch Redundancy	7-6
7.7.1	Setting Up Switch Redundancy	7-6
7.7.2	Redundancy Operations Status	7-7
7.8	Updating the WS2000 Wireless Switch's Firmware	7-7
7.8.1	Checking for and Downloading Firmware Updates	7-7
7.8.2	Performing the Firmware Update	7-8
7.8.3	Formatting a Compact Flash Card	7-9
7.8.4	Limitation of File System on the Compact Flash Card	7-9
7.8.5	Setting Up DHCP Options for Firmware Upload	7-9
7.9	Exporting and Importing Wireless Switch Settings	7-11
7.9.1	To Import or Export Settings to an FTP or TFTP Site	7-11
7.9.2	Sample Configuration File	7-13
7.10	Updating Sensor Firmware	7-47
7.10.1	Setting Sensor Firmware Update Information	7-47
7.10.2	Updating the Sensor Firmware	7-48
7.11	Configuring SNMP	7-48
7.11.1	Setting the SNMP Version Configuration	7-49
7.11.2	Setting Up the Access Control List	7-51
7.11.3	Setting the Trap Configuration	7-51
7.11.4	Setting the Trap Configuration for SNMP v1/v2c	7-51
7.11.5	Setting the Trap Configuration for SNMP V3	7-52
7.11.6	Selecting Traps	7-52
7.11.7	Setting RF Traps	7-55
7.12	Specifying a Network Time Protocol (NTP) Server	7-56
7.13	Setting Up and Viewing the System Log	7-58
7.13.1	Viewing the Log on the Switch	7-58

7.13.2 Setting Up a Log Server .....	7-58
7.14 Commands to unmount a CF card .....	7-59

## Chapter 8: Configuring HotSpot

8.1 Overview .....	8-2
8.1.1 Requirements .....	8-2
8.2 Configuring Hotspot .....	8-2
8.2.1 Enabling Hotspot on a WLAN .....	8-3
8.2.2 Set Hotspot Configuration .....	8-4
8.2.3 Setting the User Access Policy .....	8-8
8.2.4 Defining the Hotspot State of a Mobile Unit .....	8-8
8.2.5 Handling log-in and redirection .....	8-9
8.2.6 Authentication (RADIUS) .....	8-9
8.2.7 Accounting (RADIUS) .....	8-9

## Chapter 9: Using DDNS

9.1 Overview .....	9-2
9.2 Enabling DDNS .....	9-2
9.3 Updating DNS Entries using DDNS .....	9-4
9.3.1 Updating DNS Entries for a Single Subnets .....	9-4
9.3.2 Updating DNS Entries for All Active Subnets .....	9-5

## Chapter 10: Trunking VLANs Through the WAN Port

10.1 Overview .....	10-2
10.1.1 Assigning VLAN Tags to Packets .....	10-2
10.1.2 Installation Considerations and Default VLAN Settings .....	10-2
10.2 Configuring VLAN Trunking .....	10-3
10.2.1 Mapping WLANs to VLANs .....	10-4

## Chapter 11: Status & Statistics

11.1 WAN Statistics .....	11-2
11.2 Subnet Statistics .....	11-3
11.2.1 Subnet Lease stats .....	11-3
11.2.2 Subnet Stats .....	11-5
11.2.3 STP Stats .....	11-6
11.3 Wireless LAN Statistics .....	11-8
11.3.1 Displaying WLAN Summary Information .....	11-8
11.3.2 Getting Statistics for a Particular WLAN .....	11-10
11.3.3 General WLAN Information .....	11-11
11.4 Access Port Statistics .....	11-12
11.4.1 Access Port Statistics Summary Screen .....	11-12
11.4.2 Detailed Information About a Particular Access Port .....	11-13
11.4.3 General Access Port Information .....	11-14
Mobile Unit (MU) Statistics 16	
11.6 Mesh Statistics .....	11-17

11.6.1 Mesh Base Connections .....	11-17
11.6.2 Mesh Client Connections .....	11-17
11.7 Intrusion Prevention Statistics .....	11-19
11.8 View Statistics in Graphic Form .....	11-19

## **Chapter 12: WS2000 Use Cases**

12.1 Retail Use Case .....	12-3
12.1.1 A Retail Example .....	12-3
12.2 The Plan .....	12-3
12.3 Contacting the Wireless Switch .....	12-4
12.3.1 Entering the Basic System Settings .....	12-5
12.3.2 Setting Access Control .....	12-6
12.3.3 The IP Address Plan .....	12-7
12.4 Configuring POS Subnet .....	12-8
12.5 Configuring the Printer Subnet .....	12-9
12.6 Configuring the Cafe Subnet .....	12-11
12.7 Configuring the WAN Interface .....	12-12
12.8 Configuring Network Address Translation (NAT) .....	12-13
12.9 Inspecting the Firewall .....	12-14
12.10 Configuring the Access Ports .....	12-15
12.10.1 Setting Access Port Defaults .....	12-15
12.10.2 Naming the POS Access Port .....	12-17
12.10.3 Configuring the Printer Access Port .....	12-17
12.10.4 Configuring the Cafe Access Port .....	12-18
12.10.5 Associating the Access Ports to the WLANs .....	12-19
12.11 Configuring the Cafe WLAN .....	12-19
12.12 Configuring the Printer WLAN .....	12-21
12.13 Configuring the POS WLAN .....	12-24
12.14 Configuring Subnet Access .....	12-27
12.15 Configuring the Clients .....	12-29
12.15.1 Testing Connections .....	12-29
12.16 Field Office Use Case .....	12-30
12.16.1 A Field Office Example .....	12-30
12.17 The Plan .....	12-30
12.18 Configuring the System Settings .....	12-31
12.18.1 Contacting the Wireless Switch .....	12-31
12.18.2 Entering the Basic System Settings .....	12-33
12.18.3 Setting Access Control .....	12-34
12.19 Configuring the LAN .....	12-35
12.19.1 Configuring the Engineering LAN .....	12-36
12.19.2 Configuring the Sales Subnet .....	12-38
12.20 Configuring the WAN Interface .....	12-40
12.21 Configuring the WAN Interface .....	12-41
12.21.1 Setting Up Network Address Translation .....	12-41
12.22 Confirm Firewall Configuration .....	12-42

12.23 Adopting Access Ports .....	12-43
12.24 Configuring the WLANs .....	12-45
12.24.1 Security .....	12-46
12.25 Configuring the Access Ports .....	12-49
12.26 Configuring Subnet Access .....	12-54
12.27 Configuring the VPN .....	12-57
12.28 Installing the Access Ports and Testing .....	12-60

## **Appendix A: Syslog Messages**

A.1 Informational Log Entries .....	A-2
A.2 Notice Log Entries .....	A-4
A.3 Warning Log Entries .....	A-6
A.4 Alert Log Entry .....	A-9
A.5 Error-Level Log Entries .....	A-9
A.6 Debug-Level Log Entries .....	A-23
A.7 Emergency Log Entries .....	A-27



## ***Product Overview***

1.1	WS2000 Wireless Switch System Reference Guide .....	1-2
1.1.1	About this Document .....	1-2
1.1.2	Document Conventions .....	1-2
1.2	System Overview .....	1-3
1.2.1	Management of Access Ports .....	1-3
1.3	Hardware Overview .....	1-4
1.3.1	Technical Specifications .....	1-4
1.3.2	Wireless Switch LED Functions .....	1-5
1.4	Software Overview .....	1-6
1.4.1	Operating System (OS) Services .....	1-6
1.4.2	Cell Controller Services .....	1-6
1.4.3	Gateway Services .....	1-6

## 1.1 WS2000 Wireless Switch System Reference Guide



This guide is intended to support administrators responsible for understanding, configuring and maintaining the Wireless Switch. This document provides information for the system administrator to use during the initial setup and configuration of the system. It also serves as a reference guide for the administrator to use while updating or maintaining the system.

### 1.1.1 About this Document

We recommend viewing this online system reference guide with Internet Explorer 5.0 and higher or Netscape Navigator 4.7 or higher on a Microsoft Windows based PC. Viewing this document under other configurations may produce undesirable results.

### 1.1.2 Document Conventions



**Note**

**NOTE:** Indicates special tips or requirements



**Caution**

**CAUTION:** Indicates a condition that can cause equipment damage or data loss



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

**GUI Screen Text**

Indicates monitor screen dialog/output from the graphical user interface accessed from any web browser on the network.



## 1.2 System Overview

The WS2000 Wireless Switch provides a low-cost, feature-rich option for sites with one to six Access Ports. The WS2000 Wireless Switch works at the center of a network's infrastructure to seamlessly and securely combine wireless LANs (WLANs) and wired networks. The switch sits on the network. Wireless Access Ports connect to one of the six available ports on the switch and the external wired network (WAN) connects to a single 10/100 Mbit/sec. WAN port.

Mobile units (MUs) associate with the switch via an Access Port. When an MU contacts the switch, the switch cell controller services attempt to authenticate the device for access to the network.

The WS2000 Wireless Switch acts as a WAN/LAN gateway and a wired/wireless switch.

### 1.2.1 Management of Access Ports

This wireless switch provides six 10/100 Mbit/sec. LAN ports for internal wired or wireless traffic. Four of these ports provide IEEE 802.3af-compliant Power over Ethernet (PoE) support for devices that require power from the Ethernet connection (such as Access Ports). Administrators can configure the six ports to communicate with a private LAN or with an Access Port for a wireless LAN (WLAN). The switch provides up to four extended service set identifiers (ESSIDs) for each Access Port connected to the switch.

#### 1.2.1.1 Firewall Security

The LAN and Access Ports are placed behind a user-configurable firewall that provides stateful packet inspection. The wireless switch performs network address translation (NAT) on packets passing to and from the WAN port. This combination provides enhanced security by monitoring communication with the wired network.

#### 1.2.1.2 Wireless LAN (WLAN) Security

Administrators can configure security settings independently for each ESSID. Security settings and protocols available with this switch include:

- Kerberos
- WEP-64
- WEP-128
- 802.1x with RADIUS
- 802.1x with Shared Key
- KeyGuard
- WPA/WPA2-TKIP
- WPA2/CCMP (802.11i)

#### 1.2.1.3 VPN Security

Virtual Private Networks (VPNs) are IP-based networks that use encryption and tunneling to give users remote access to a secure LAN. In essence, the trust relationship is extended from one LAN across the public network to another LAN, without sacrificing security. A VPN behaves similarly to a private network; however, because the data travels through the public network, it needs several layers of security. The WS2000 Wireless Switch acts as a robust VPN gateway.

## 1.3 Hardware Overview

The WS2000 Wireless Switch provides a fully integrated solution for managing every aspect of connecting wireless LANs (WLANs) to a wired network. This wireless switch can connect directly to a cable or DSL modem, and can also connect to other wide area networks through a Layer 2/3 device (such as a switch or router). The switch includes the following features:

- One WAN (RJ-45) port for connection to a DSL modem, cable modem, or any other Layer 2/3 network device.
- Six 10/100 Mbit/sec. LAN (RJ-45) ports: four ports provide 802.3af “Power over Ethernet” (PoE) support; the other two do not provide power.
- Each port has two LEDs, one indicating the speed of the transmission (10 or 100 Mbit/sec.), the other indicating whether there is activity on the port. The four LAN ports with PoE have a third LED that indicates whether power is being delivered over the line to a power device (such as an Access Port). (See the WS2000 Wireless Switch LED explanation for more information on the meaning of the different state of the LEDs.)
- A DB-9 serial port for direct access to the command-line interface from a PC. Use Symbol’s Null-Modem cable (Part No. 25-632878-0) for the best fitting connection.
- A CompactFlash slot that provides AirBEAM<sup>®</sup> support.

### 1.3.1 Technical Specifications

#### 1.3.1.1 Physical Specifications

- Width: 203 mm
- Height: 38 mm
- Depth: 286 mm
- Weight: 0.64 kg

#### 1.3.1.2 Power Specifications

- Maximum Power Consumption: 90-256 VAC, 47-63 Hz, 3A
- Operating Voltage: 48 VDC
- Operating Current: 1A
- Peak Current: 1.6A

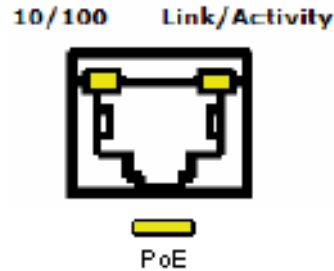
#### 1.3.1.3 Environmental Specifications

- Operating Temperature: 0°C to 40°C
- Storage Temperature: -40°C to 70°C
- Operating Humidity: 10% to 85% Non-condensing
- Storage Humidity: 10% to 85% Non-condensing
- Operating Altitude: 2.4 Km
- Storage Altitude: 4.6 km

### 1.3.2 WS2000 Wireless Switch LED Functions

The switch has a large blue LED on the right front that indicates that the switch is powered on.

Each port on the WS2000 Wireless Switch has either two or three LEDs that indicate the status of the port. Ports 1-4, which supply 802.3af Power over Ethernet (PoE), have three LEDs. The remaining two non-powered LAN ports and the WAN port have two LEDs.



Location	Function
Upper left LED	This LED is present on all ports and indicates the speed of the transmissions through the port. The LED is on when the transmission rate is 100 Mbit per second (100BaseT). The light is off when the transmission rate is 10 Mbit per second.
Upper right LED	This LED indicates activity on the port. This light is solid yellow when a link to a device is made. The light flashes when traffic is being transferred over the line.
Lower LED	This LED is only present on Ports 1-4. These ports provide 802.3af Power over Ethernet (PoE) support to devices (such as Access Ports). The LED has several states: <b>OFF</b> —A non-power device (or no device) is connected; no power is being delivered. <b>GREEN</b> —The switch is delivering 48 volts to the power device connected to that port. <b>RED</b> —There was a valid PoE connection; however, the switch has detected that the power device is faulty. The red light will remain until a non-faulty connection is made to the port.

## 1.4 Software Overview

The WS2000 Wireless Switch software provides a fully integrated solution for managing every aspect of connecting Wireless LANs (WLANs) to a wired network, and includes the following components:

### 1.4.1 Operating System (OS) Services

Operating System (OS) Services determine how the WS2000 Wireless Switch communicates with existing network and operating system-centric software services, including:

- Dynamic Host Configuration Protocol (DHCP)
- Telnet and File Transfer Protocol (FTP/TFTP) servers
- The Simple Network Time Protocol (SNTP) client, used to keep switch time synchronized for Kerberos authentication
- A mechanism for setting up a redundant (secondary) switch that takes over if the primary switch fails

### 1.4.2 Cell Controller Services

The Cell Controller provides the ongoing communication between mobile units (MUs) on the Wireless LAN (WLAN) and the wired network. Cell Controller services perform the following:

- Initialize the Access Ports
- Maintain contact with Access Ports by sending a synchronized electronic “heartbeat” at regular intervals
- Track MUs when they roam from one location to another
- Manage security schemes based on system configuration
- Maintain system statistics
- Store policies and Access Port information
- Detect and manage rogue Access Ports
- Management of communications QoS

### 1.4.3 Gateway Services

Gateway services provide interconnectivity between the Cell Controller and the wired network, and include the following:

- System management through a Web-based Graphical User Interface (GUI) and SNMP
- 802.1x RADIUS client
- Security, including Secure Sockets Layer (SSL) and Firewall
- Network Address Translation (NAT), DHCP services, and Layer 3 Routing
- Virtual Private Network (VPN)

## ***Getting Started***

2.1 Getting Started with the WS2000 Wireless Switch .....	2-2
Step 1: Install the Switch .....	2-2
Step 2: Set Up Administrative Communication to the Switch .....	2-2
Step 3: Set the Basic Switch Setting .....	2-4
Step 4: Configure the LAN Interface .....	2-5
Enable Subnet1 .....	2-5
Step 5: Configure Subnet1 .....	2-6
Step 6: Configure the WAN Interface .....	2-7
Communicating with the Outside World .....	2-7
Setting Up Point-to-Point over Ethernet (PPPoE) Communication .....	2-8
Step 7: Enable Wireless LANs (WLANs) .....	2-9
Wireless Summary Area .....	2-9
Step 8: Configure WLAN Security .....	2-10
Setting the Authentication Method .....	2-11
Setting the Encryption Method .....	2-11
Mobile Unit Access Control List (ACL) .....	2-11
Step 9: Test Connectivity .....	2-12
2.2 Where to Go from Here? .....	2-12

## 2.1 Getting Started with the WS2000 Wireless Switch

This section provides just enough instruction to set up the WS2000 Wireless Switch, connect an Access Port, and test communications with a single mobile unit (MU) and the wide area network (WAN). The configuration suggestions made here are just the minimum needed to test the hardware. Once finished with this section, additional configuration settings are required. This section covers the following topics:

- **Step 1:** Install the switch and connect it to the WAN, a stand alone computer, and an Access Port
- **Step 2:** Set up administrative communication to the switch
- **Step 3:** Set the basic switch settings
- **Step 4:** Configure the LAN interface
- **Step 5:** Configure Subnet1
- **Step 6:** Configure the WAN Interface
- **Step 7:** Enable Wireless LANs (WLANs)
- **Step 8:** Configure WLAN Security
- **Step 9:** Test Connectivity

### Step 1: Install the Switch

To install the WS2000 Wireless Switch hardware, follow the directions in the [WS2000 Wireless Switch Quick Installation Guide](#) found in the box with the switch and on the CD-ROM that is distributed with the switch. These instructions describe how to:

- Select a site (desk, wall, or rack) for the switch
- Install the switch using the appropriate accessories for the selected location
- Connect devices to WAN and LAN ports (using standard CAT-5 cables)
- Interpret the port LEDs on the front of the switch

After the switch is mounted and powered up, connect the following items to the switch:

1. Connect the WAN to the switch (using the WAN port) with a CAT-5 Ethernet cable. The LEDs for that port should start to flash.
2. Connect an Access Port to the switch using a CAT-5 Ethernet cable using one of the six LAN ports. If the Access Port requires PPPoE, connect the Access Port in ports 1, 2, 3, or 4. Ports 5 and 6 do not provide power.
3. Have a mobile “wireless” device available to test communication with the Access Port.



**NOTE:** Access Ports must be connected to the LAN ports of the wireless switch to enable configuration of the Access Port related settings.

Note

### Step 2: Set Up Administrative Communication to the Switch

Before the configuration process can begin, establish a link with the wireless switch.

1. Connect a “wired” computer to the switch (in any one of the available LAN ports) using a standard CAT-5 cable.
2. Set up the computer for TCP/IP DHCP network addressing and make sure that the DNS settings are not hard coded.
3. Start up Internet Explorer (with Sun Micro systems’ Java Runtime Environment (JRE) 1.4 or higher installed) and type the following IP address in the address field: 192.168.0.1



**NOTE:** For optimum compatibility use Sun Microsystems' JRE 1.4 or higher (available from Sun's website), and be sure to disable Microsoft's Java Virtual Machine if it is installed.

**Note**

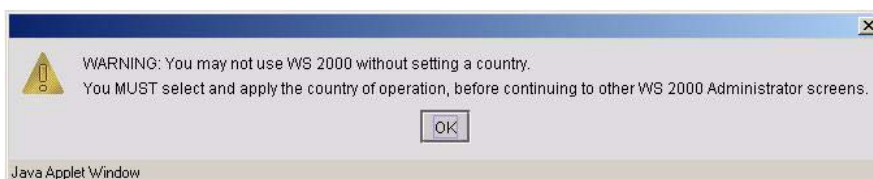
The following screen displays.



4. Log in using **"admin"** as the **User ID** and **"symbol"** as the **Password**.
5. If the login is successful, the following dialog window displays.



Enter a new admin password in both fields, and click the **Update Password Now** button. When the admin password has been updated, the following message displays, and you are prompted to change the country of operation for the switch.



6. Select and change the country from the **Country** drop-down list of the **System Settings** screen.
7. Click the **Apply** button to save the changes.

The *System Setting* screen is displayed.

The screenshot shows the 'System Settings' configuration page for a WS2000 Wireless Switch. The page is titled 'WS2000 Wireless Switch' and features a navigation tree on the left. The main content area is divided into two sections: 'WS 2000 System Settings' and 'Factory Defaults'. The 'WS 2000 System Settings' section contains the following fields:

- System Name: WS2000 Switch
- System Location: Doc Team Area
- Domain Name: docteam.motorola.com
- Admin Email Address: (empty)
- DNS Server IP Address: 192.168.0.1
- Country: United States - us

Below these fields, the 'Factory Defaults' section includes buttons for 'Restore Default Configuration' and 'Restore Partial Default Configuration'. The 'Restart WS 2000' section includes a 'Restart WS 2000' button. At the bottom of the page, there are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'WS2000 Switch' is also displayed in the lower-left corner of the page.

### Step 3: Set the Basic Switch Setting

1. Enter a **System Name** for the wireless switch. The specified name appears in the lower-left corner of the configuration screens, beneath the navigation tree. This name can be a useful reminder if multiple Symbol wireless switches are being administered.
2. Enter a text description of the location of the switch in the **System Location** field. This text is used as a reminder to the network administrator and is also used to set the location variable if the switch is administered using SNMP.
3. In the **Domain Name** field, enter the name of the domain this switch is a member of. This value is returned along with the system name for a Reverse DNS Query on the switch.
4. Enter an email address for the administrator in the **Admin Email Address** field. The switch uses this address for sending SNMP-related and other administration-related messages to the administrator.
5. Enter the IP address of the DNS Name Server in the **DNS Server IP Address** field. The switch uses this field to resolve FQDN information provided in the NTP configuration page. See [Specifying a Network Time Protocol \(NTP\) Server](#) for more information.
6. Select the **Country** for the switch from the drop-down menu. Selecting the correct country is extremely important. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted by Access Ports. To ensure compliance with national and local laws, be sure to set this field accurately.
7. Click **Apply** to save changes. Unapplied changes are lost if the administrator navigates to a different screen.





**NOTE:** The WS2000 switch is shipped with an open default SNMP configuration:  
 Community: public, OID: 1.3.6.1, Access: Read-only  
 Community: private, OID: 1.3.6.1, Access: Read-write

**Note**

If your switch has these settings, it is important to change them immediately; otherwise, users on the same network will have read-write access to the switch through the SNMP interface. Select **System Configuration --> SNMP Access** from the left menu to examine the settings and change them, if necessary.

## Step 4: Configure the LAN Interface

The first step of network configuration process is to figure out the topology of the LAN. The WS2000 Wireless Switch allows the administrator to enable and configure six different subnets. The administrator can assign an IP address, port associations, and DHCP settings for each subnet.

### Enable Subnet1

Select **LAN** under the Network Configuration group from the left menu. Use the LAN configuration screen to view a summary of physical-port addresses and wireless LANs (WLANs) associated with the six supported subnets, and to enable or disable each configured subnet.

Enable	Network	Address	Interfaces
<input checked="" type="checkbox"/>	Subnet1	192.168.0.50	P1,P2,P3,P4,P5,P6,WLAN1
<input type="checkbox"/>	Subnet2	0.0.0.0	WLAN2
<input type="checkbox"/>	Subnet3	0.0.0.0	WLAN3
<input type="checkbox"/>	Subnet4	0.0.0.0	WLAN4
<input type="checkbox"/>	Subnet5	0.0.0.0	
<input type="checkbox"/>	Subnet6	0.0.0.0	

1. In the **LAN** screen, the administrator can enable up to six subnets. Make sure that the check box to the left of **Subnet1** line is enabled.

Each enabled subnet shows up in the directory tree in the left column of the configuration screens. Consider disabling a previously configured subnet if its assigned ports are no longer in use, or to consolidate the LAN's communications on fewer subnets.

The rest of the information on this screen is summary information; it is collected from other screens (such as the subnet configuration screens) where the administrator can set the data.

<b>Network</b>	<b>Network</b> (subnet) name is a descriptive string that should describe the subnet's function. The WS2000 Network Management System uses subnet names throughout the configurations screens.
----------------	--

<b>Address</b>	This IP address allows users from outside the subnet (whether from the WAN or from another subnet from the same switch) to access the right subnet. An IP address uses a series of four numbers that are expressed in dot notation, for example, 194.182.1.1.
<b>Interfaces</b>	The <b>Interfaces</b> field displays which of the six physical LAN ports are associated with the subnet. The possible ports are: P1 (port 1), P2, P3, P4, P5, and P6 (from left to right facing the front of the switch). The administrator assigns a port to a subnet to enable access to the device(s) connected to that port. The administrator can assign a port to only one subnet. The <b>Interfaces</b> field also lists the WLANs that are associated with the subnet.

## Step 5: Configure Subnet1

The WS2000 Network Management System allows the administrator to define and refine the configuration of the enabled subnets. Each of six subnets (short for “subnetworks”) can be configured as an identifiably separate part of the switch-managed local area network (LAN). Each subnet can include some combination of assigned ports and associated wireless LANs (WLANs).

1. Select **Network Configuration** --> **LAN** --> **Subnet1** from the list on the left. The following screen appears for the selected subnet.

2. Check to make sure that all the ports and WLAN1 are selected for this subnet. WLAN1 should automatically be included if the switch and the Access Port are communicating properly. If WLAN1 is not present in the list, check the following:
  - The power to the Access Port
  - The connections between the switch and the Access Port
  - The LEDs to make sure that lights are on and flashing

- For this initial configuration, ensure that **This interface is a DHCP Server** is enabled. If so, the switch sets the IP addresses automatically for the mobile devices. This value can be changed at any time in the future. All other default settings are fine for the system test.

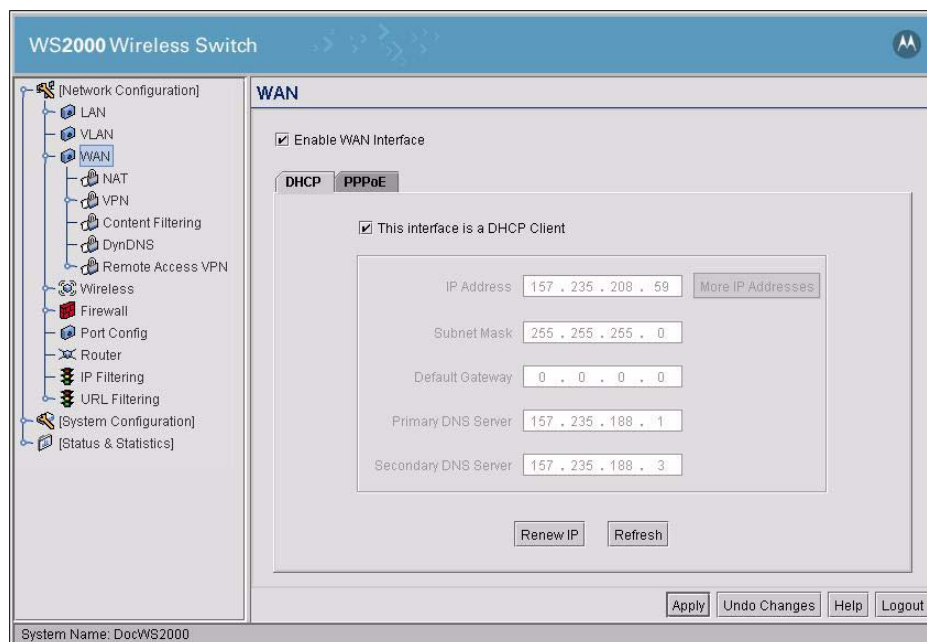
DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. The switch includes internal DHCP server and client features, and the subnet's interface can use either capability.

- Click the **Apply** button to save changes.

## Step 6: Configure the WAN Interface

A wide area network (WAN) is a widely dispersed telecommunications network. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or a cable modem to access the Internet.

The WS2000 Wireless Switch includes one WAN port. In order to set up communications with the outside world, select **Network Configuration** --> **WAN** from the left menu. The following WAN configuration page appears.



## Communicating with the Outside World

- Click the **Enable WAN Interface** check box to enable a connection between the switch and a larger network or the outside world through the WAN port.
- If this switch should be a DHCP client (A DHCP client get it's IP address automatically from a DHCP server or a switch), check the **This interface is a DHCP Client** check box to enable it. If **This interface is DHCP Client** is checked, the switch is limited to one WAN IP address. This choice is required when:
  - The host router or switch on the WAN communicates with the WS2000 Wireless Switch using DHCP.
  - The switch interfaces with an Internet Service Provider (ISP) that uses DHCP addressing.



**NOTE:** This setting is independent from the DHCP settings for the switch's internal subnets.

**Note**

3. If **This interface is DHCP Client** is not checked, other fields in the screen are enabled. To find out the information to enter into these fields, contact your network administrator or the ISP that provided the cable modem or DSL router. All fields take standard IP addresses in the form xxx.xxx.xxx.xxx.
  - **IP Address** refers to the IP address that the outside world uses to address this WS2000 Wireless Switch.
  - Click the **More IP Addresses** button to specify additional static IP addresses for the switch. Additional IP addresses are required when users within the LAN need dedicated IP addresses, or when servers in the LAN need to be accessed (addressed) by the outside world. The pop-up window allows the administrator to enter up to eight WAN IP addresses for the switch.
  - The **Subnet Mask** is the mask used for the WAN.
  - The **Default Gateway** is the address of the device that provides the connection to the WAN (often a cable modem or DSL router).
  - The two DNS Server fields specify DNS addresses of servers that can translate domain names, such as www.motorola.com, into IP addresses that the network uses when passing information. The **Secondary DNS Server** acts as a backup to the **Primary DNS Server** when the primary server is not available.

### **Setting Up Point-to-Point over Ethernet (PPPoE) Communication**

Point-to-Point over Ethernet (PPPoE) provides the ability to connect a network of hosts through a simple device to a remote access concentrator. Many DSL providers require that their clients communicate using this protocol. The facility allows the ISP to control access, billing, and type of service provided to clients on a per-user or per-site basis. Check with the network administrator or ISP to determine whether to enable this feature, and, if so, find out the username and password required for authentication.

To set up PPPoE, click on the **PPPoE** tab under the WAN screen.

1. Check **Enable** in the PPP over Ethernet area to enable the PPPoE protocol for high-speed connections.
2. Enter the **Username** and **Password** required for authentication. The username and password are for the switch's router to use when connecting to the ISP. When the Internet session starts, the ISP authenticates the username.
3. Set the **Idle Time** in seconds to an appropriate number. This number is the amount of time the PPPoE connection will remain idle before it disconnects. 10000 seconds default idle time is appropriate for most situations.
4. Check **Keep Alive** to instruct the switch to continue occasional communications over the WAN even when client communications to the WAN are idle. Some ISPs terminate inactive connections, while others do not. In either case, enabling Keep-Alive mode keeps the switch's WAN connection alive, even when there is no traffic. If the ISP drops the connection after reaching the maximum idle time, the switch automatically reestablishes the connection to the ISP.
5. Select the appropriate WAN authentication method from the drop-down menu. Collect this information from the network administrator. Select between **None**, **PAP**, **CHAP**, or **PAP or CHAP**.

<b>CHAP</b>	A type of authentication in which the user logging in uses a secret information and some special mathematical operations to calculate a numerical value. The server, the user is logging into, knows the same secret value and performs the same mathematical operations to arrive at a value. If the values match, the user is authorized to access the server. One of the numbers used in the mathematical operation is changed after every log-in. This is to protect the server against an intruder secretly copying a valid authentication session and replaying it later to log in.
<b>PAP</b>	An identity verification method used to send a username and password over a network to a computer that compares the username and password to a table listing authorized users. This method of authentication is less secure, because the username and password travel as clear text that a hacker could read and use to launch an attack.

6. Click the **Apply** button to save changes.

## Step 7: Enable Wireless LANs (WLANs)

The WS2000 Wireless Switch works either in a wired or wireless environment; however, the power of the switch is associated with its support of wireless networks. In order to use the wireless features of the switch, the administrator needs to enable up to four wireless LANs (WLANs).

To start the WLAN configuration process, select the **Network Configuration --> Wireless** item from the left menu. The following Wireless summary screen appears.

The screenshot shows the WS2000 Wireless Switch configuration interface. The left sidebar contains a tree view with 'Wireless' selected. The main content area is titled 'Wireless' and has two tabs: 'WLAN Summary' (active) and 'AP Adoption Configuration'. The 'WLAN Summary' tab displays a table with the following data:

Enable	HotSpot	Name	ESSID	Subnet	Access Ports Adopted	Vlan	Security
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WLAN1	101	WS2KD1		1	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN2	102	Subnet2		2	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN3	103	Subnet3		3	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN4	104	Subnet4		4	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN5	105			5	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN6	106			6	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN7	107			7	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN8	108			8	

Below the table is a 'Miscellaneous' section with the following options:

- WEP Shared Mode
- SIP CAC Mode
- Legacy mode (AP300)
- HotSpot Credential Caching Mode
- MU Inactivity Timeout:  Mins
- HotSpot Session Timeout:  Mins

At the bottom right of the interface are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'DocWS2000' is displayed at the bottom left.

### Wireless Summary Area

The top portion of the window displays a summary of the WLANs that are currently defined. This is the screen in which the administrator can enable or disable a WLAN. At first, eight WLANs are listed WLAN1, WLAN2, WLAN3, WLAN4, WLAN5, WLAN6, WLAN7 and WLAN8; however, only WLAN1 is enabled.

1. Verify that WLAN1 is enabled (checked) and associated with Subnet1.

2. Verify that Access Port 1 is shown in the **Access Ports Adopted** field to the right. If it is not, verify the connection between the switch and the Access Port.

The current settings for the associated Subnet and adopted Access Ports are displayed on this screen; however, the screen associated with each WLAN (under **Network Configuration** --> **Wireless**) is where the settings and rules for adopting Access Ports can be modified.

Use the AP Adoption Configuration tab to assign Access Ports to a particular WLAN. The switch can adopt up to six Access Ports at a time, but the list of allowed Access Port addresses (displayed in this area) can exceed six in number. A dual-radio 802.11a/b Access Port counts as one Access Port with respect to the maximum allowed; however, each radio is listed as a separate Access Port.

This adoption list identifies each Access Port by its Media Access Control (MAC) address. This address is the Access Port's hard-coded hardware number that is printed on the bottom of the device. An example of a MAC address is 00:09:5B:45:9B:07.

The default setting associates all adopted Access Ports with WLAN1.

## Step 8: Configure WLAN Security

In the previous step, the administrator set parameters for each WLAN that fine tune the performance of the WLAN. In addition, the administrator can set the type and level of security for each WLAN. These security measures do not control communications from the WAN; instead, they control communication from the clients within the WLAN.

In the **Network Configuration** --> **Wireless** --> <WLAN name> --> <WLAN Name> --> **Security** screen, the administrator can set the user authentication method and the encryption method, as well as define a set of rules that control which MUs can communicate through the WLAN.

The screenshot displays the configuration interface for the WS2000 Wireless Switch, specifically the **WLAN1 Security** page. The interface is divided into several sections:

- Authentication Methods:** Includes radio buttons for 802.1x EAP (with a configuration button), Kerberos (with a configuration button), and No Authentication (selected).
- Encryption Methods:** Includes radio buttons for WEP 64 (40 bit key), WEP 128 (104 bit key), KeyGuard, WPA/WPA2-TKIP, WPA2-CCMP (802.11i), and No Encryption (selected). Each method has a corresponding configuration button.
- IP Filtering:** A checkbox for "Enable IP Filtering" is currently unchecked, with an "IP Filtering" button next to it.
- Mobile Unit Access Control:** A dropdown menu is set to "Allow", followed by the text "access for all Mobile Units, except:". Below this is a table with columns for "Start MAC", "End MAC", and "Name". The table is currently empty, with "Add" and "Del" buttons at the bottom.

At the bottom of the page, there are buttons for "Apply", "Undo Changes", "Help", and "Logout". The system name "DocWS2000" is visible in the bottom left corner.

## Setting the Authentication Method

The authentication method sets a challenge-response procedure for validating user credentials such as username, password, and sometimes secret-key information. The WS2000 Wireless Switch provides two methods for authenticating users: 802.1x EAP and Kerberos. The administrator can select between these two methods. For testing connectivity, WLAN security is not an issue, so there is not reason to enable authentication—the default setting (**No Authentication**) is sufficient.

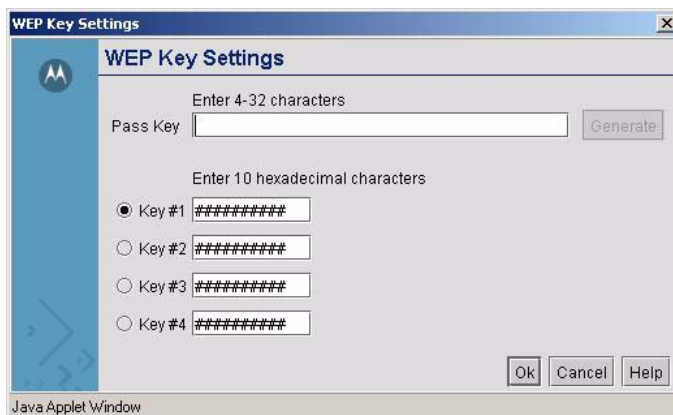
## Setting the Encryption Method

Encryption applies a specific algorithm to data to alter its appearance and prevent unauthorized reading. Decryption applies the algorithm in reverse to restore the data to its original form. Sender and receiver employ the same encryption/decryption method.

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. WEP might 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. An unauthorized person with a sniffing tool can monitor a network for less than a day and decode its encrypted messages.

For the connectivity test, set WEP 128 encryption. This ensures that communications with the switch are secure enough for this stage. Later on, increasing the security level might be necessary.

1. Select the **WEP 128 (104-bit key)** option.
2. To use WEP encryption with the **No Authentication** selection, click the **WEP Key Settings** button to display a sub-screen for entering keys.



3. Add a key to **Key #1**, and use that key with the mobile unit. The keys consist of 26 hexadecimal (0-9, A-E) characters. When finished, click the **Ok** button to close this screen and return to the WLAN Security screen.
4. Click the **Apply** button in the WLAN Security screen to save changes.

## Mobile Unit Access Control List (ACL)

This list is used to specify which mobile units can or cannot gain access to the WLAN. The list employs an adoption rule for allowing or denying specific mobile units by way of exception. By default, all mobile units can gain access.



## Step 9: Test Connectivity

At this point, the switch is set up to allow mobile units to access the LAN.

1. Check and ensure that the MU is setup as a DHCP client.
2. Set the MU to use WEP 128 bit encryption. Use the same key as was entered in the WEP Key Setting dialog. You might need to restart the MU after changing the settings.
3. Open a Web browser and type the IP address: 192.168.0.1.

The WS2000 Switch Management screen should appear. If it does not, go back to the wired system used to configure the switch and see if the mobile device appears in the MU Stats screen (**Status & Statistics** --> **MU Stats**). If it does not appear on the MU Stats screen, recheck the network and WEP settings on the mobile device.

4. In the Web browser, enter a URL for a site (such as www.motorola.com) on the WAN. If the site does not appear, go to the WAN Stats screen (**Status & Statistics** --> **WAN Stats**) to review the status of the WAN connection.

## 2.2 Where to Go from Here?

When full connectivity has been verified, the switch can be configured further to meet the needs of the organization. Refer to the two case studies provided with this reference for specific installation examples. These case studies describe the environment, the desired features, and the configuration selections that were made in two different usage scenarios.

- Case 1: *Retail Use Case*  
(with handheld terminals, wireless printers, wired POS, secured access to in-store server, and public access to WAN)
- Case 2: *Field Office Use Case*  
(with 3 WAN IP addresses, VPN passthrough, RADIUS server, and full-access between subnets)



## ***LAN/Subnet Configuration***

3.1 Enabling Subnets for the LAN Interface.....	3-2
3.1.1 Defining Subnets.....	3-2
3.2 Configuring Subnets.....	3-3
3.2.1 The DHCP Configuration.....	3-5
3.2.2 Advanced DHCP Settings.....	3-5
3.3 Configuring Subnet Access.....	3-7
3.3.1 The Access Overview Table.....	3-7
3.3.2 The Access Exception Area.....	3-8
3.4 Advanced Subnet Access Settings.....	3-10
3.5 Bridge Configuration.....	3-12
3.6 Virtual LAN (VLAN) Configuration.....	3-14
3.7 Configuring IP Filtering.....	3-15
3.8 URL Filtering.....	3-18
3.9 Port Configuration.....	3-20

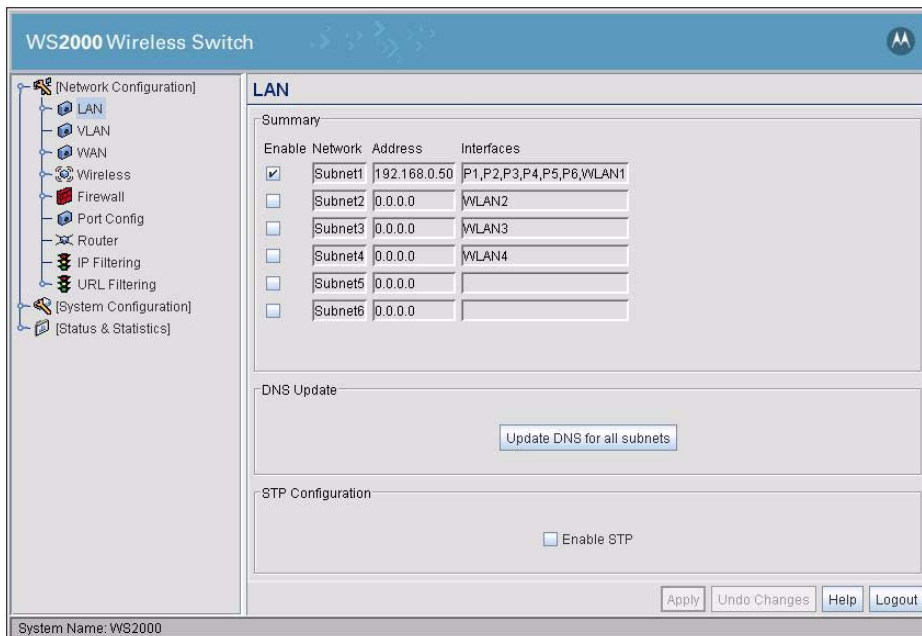
## 3.1 Enabling Subnets for the LAN Interface

Subnets are used to maximize the available network addresses and to logically separate the existing organizational network into smaller related networks.

The WS2000 Wireless Switch allows administrators to enable and configure six different subnets for each switch. Administrators can assign IP addresses, port associations, DHCP settings, and security settings for each subnet. This System Reference Guide provides two case studies that demonstrate how requirements for network access and capabilities drive the decisions of how to configure the subnets.

### 3.1.1 Defining Subnets

Select **LAN** under the **Network Configuration** group from the left menu. Use the LAN configuration screen to view a summary of physical-port addresses and Wireless LANs (WLANs) associated with the six supported subnets, and to enable or disable each configured subnet.



1. Check the box to the left of a subnet to enable it. Up to six subnets can be enabled to use the wired and/or wireless connections of the switch-managed LAN. Enable multiple subnets to divide the communications of different business areas or operations. Each enabled subnet shows up in the directory tree in the left column of the configuration screens. Consider disabling a previously configured subnet if its assigned ports are no longer in use, or to consolidate the LAN's communications on fewer subnets.
2. Click **Update DNS for all Subnets** to asynchronously invoke the Dynamic DNS update module. This module checks the expired and valid DHCP leases for each of the subnets and adds or deletes entries to the Dynamic DNS table accordingly.
3. Click **Enable STP** to enable STP. Spanning Tree Protocol (STP) is a protocol that ensures loop-free topology for any bridged LAN. This feature is not enabled by default.



**Note**

**NOTE:** STP is applied for mesh networks even if it is not enabled through the LAN screen.

4. Click **Apply** to save changes. All “unapplied” changes are lost when the administrator moves to a new screen.

The rest of the information on this screen is summary information. It is collected from other screens (such as the subnet configuration screens) where the administrator can set the data.

<b>Network</b>	<b>Network</b> (subnet) name is a descriptive string that should describe the subnet’s function. The WS2000 Network Management System uses subnet names throughout the configurations screens.
<b>Address</b>	This IP address allows users from outside the subnet (whether from the WAN or from another subnet from the same switch) to access the right subnet. An IP address uses a series of four numbers that are expressed in dot notation, for example, 194.182.1.1.
<b>Interfaces</b>	The <b>Interfaces</b> field displays which of the six physical LAN ports are associated with the subnet. The possible ports are: <b>P1</b> (port 1), <b>P2</b> , <b>P3</b> , <b>P4</b> , <b>P5</b> , and <b>P6</b> (from left to right facing the front of the switch). The administrator assigns a port to a subnet to enable access to the device(s) connected to that port. The administrator can assign a port to only one subnet.  The <b>Interfaces</b> field also lists the WLANs that are associated with the subnet.

To change features of a subnet, select **Network Configuration --> LAN --> <subnet name>** from the menu on the left.

## 3.2 Configuring Subnets

The WS2000 Network Management System allows the administrator to define and refine the configuration of the enabled subnets. Each of the six subnets (short for “subnetworks”) can be configured as an identifiably separate part of the switch-managed Local Area Network (LAN). Each subnet can include some combination of assigned ports and associated Wireless LANs (WLANs). To configure an enabled subnet, select the subnet name from the **Network Configuration --> LAN** list in the left. The following screen appears for the selected subnet.

1. Change the **Name** of the subnet to use a descriptive name that indicates something about the subnet. The name can contain seven characters, including spaces and numbers. It will appear in the left menu under the LAN menu item.

2. Set an **IP address** to be used for the subnet.

The switch uses the IP address to refer to a particular subnet. This IP address could be a WAN address; but is generally a non-routable address.

An IP address uses a series of four numbers that are expressed in dot notation, for example, 194.182.1.1.

3. Set the **Network Mask** for the IP address. A network mask uses a series of four numbers that are expressed in dot notation, similar to an IP number. For example, 255.255.255.0 is a network mask.

4. Select a port or WLAN from the list of Interfaces to associate it with the subnet. Six LAN ports are available on the switch. Assign from one to six ports to a subnet. Two subnets cannot use the same port. However, multiple ports can be assigned to one subnet.

Eight WLANs are available. WLAN assignments are logical designations. Associate from zero to three WLANs with a subnet. Two subnets cannot use the same WLAN. However, multiple WLANs can be associated with one subnet. If two or three WLANs are associated with one subnet, each port dedicated to that subnet can use any of the associated WLANs.

5. Click the **Add** button to add it to the **Interfaces** list.

To remove an interface, select that interface from the **Assigned** list and click the **Delete** button.



**Note**

**NOTE:** Note that wireless devices cannot access the switch unless a WLAN is configured and associated with a subnet. (This process is described in detail in [Configuring Wireless LANs](#) section of this document.)

### 3.2.1 The DHCP Configuration

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. The switch includes internal DHCP server and client features, and the subnet's interface can use either capability.

1. Click the appropriate radio button to select one DHCP setting for the subnet's interfaces:
  - Select **This interface does not use DHCP** to disable DHCP on this subnet and specify IP addresses manually.
  - Select **This interface is a DHCP Client** if this subnet obtains IP parameters from a DHCP server outside the switch.
  - Select **This interface is a DHCP Server** to enable the switch's DHCP server features.
  - Select **This interface is a DHCP Relay** to use an external DHCP server to provide DHCP information to clients on this subnet. Use the associated field to enter the IP address for the external DHCP Server.
2. If **This interface is a DHCP Server** is the selected option, fill in the **Address Assignment Range** fields. These fields allow the administrator to assign a range of IP addresses to devices as they connect.
3. Set the **Advanced Settings**, if necessary.
4. Click the **Apply** button to save all changes.

### 3.2.2 Advanced DHCP Settings

1. Click the **Advanced DHCP Server** button to display a sub-screen to further customize IP address allocation.

The screenshot shows the 'Advanced DHCP Server' configuration window. The window title is 'Advanced DHCP Server'. The interface includes the following elements:

- Enable Dynamic DNS
- Single User Class Option
- Multiple User Class Option
- Primary DNS Server: 192.168.0.1
- Secondary DNS Server: 192.168.0.1
- Default Gateway: 192.168.0.1
- WINS Server: 192.168.0.254
- DHCP Lease Time (sec): 86400
- Domain Name: [Empty field]
- DNS Forward Zone: [Empty field]
- TFTP Server Address: 0.0.0.0
- Bootfile: [Empty field]
- Option 189: [Empty field]
- Option 43: [Empty field]
- Static DHCP Mappings:
 

Client MAC	IP Address
- Buttons: Add, Del, Ok, Cancel, Help

At the bottom left of the window, it says 'Java Applet Window'.

2. If Dynamic DNS services are needed on the subnet, check the box labeled **Enable Dynamic DNS**.

Enabling Dynamic DNS will allow domain name information to be updated when the IP address associated with that domain changes.

When a MU associates and gets an IP address from the DHCP server, the DHCP server then updates the DNS server with the IP allotted to the corresponding hostname when DDNS is enabled.

Any DHCP client can send the User Class Id either in the Single or Multiple user class ID format. The Single or Multiple User class option is provided to enable the switch to interpret the correct format in which the user class ID is sent by the client. The switch then retrieves the correct value of the user class ID sent by the DHCP client based on the selected format. This same user class ID format is used for the DDNS messages.

3. Specify the address of a **Primary DNS Server**. The Internet Server Provider (ISP) or a network administrator can provide this address.

A DNS server translates a domain name, such as www.symbol.com, into an IP address that networks can use.

4. Specify the address of a **Secondary DNS Server** if available.

5. Specify the **Default Gateway** IP address for this subnet's presence on the network. This IP address should be the same as used on the Subnet screen.

6. If your network has a Windows Internet Name Service (WINS) server, specify its IP address in the **WINS Server** field.

A WINS server allows you to map NetBIOS names to IP addresses.

7. Specify a **DHCP Lease Time** period in seconds for available IP addresses.

The DHCP server grants an IP address for as long as it remains in active use. The lease time is the number of seconds that 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.

8. If the MUs on this subnet are members of a domain, enter that name in the **Domain Name** field and it will be sent out via DHCP to all MUs associated with this subnet.

9. **DNS Forward Zone** is used for maintaining DomainName to Address mappings used by the DNS server.

10. Use the **TFTP Server Address** to provide the IP address of the TFTP Server. The TFTP server address is the address of the boot server.

11. Use the Bootfile to provide the path to the Boot file.

12. Option 189 is used to specify the IP address and port address of a WIAP enabled switch, a switch that can adopt Access Ports in WIAP mode. This field accepts a comma separated list, for example, 192.168.0.1:200, 100.1.200.24:24576. Only port 24576 is supported.

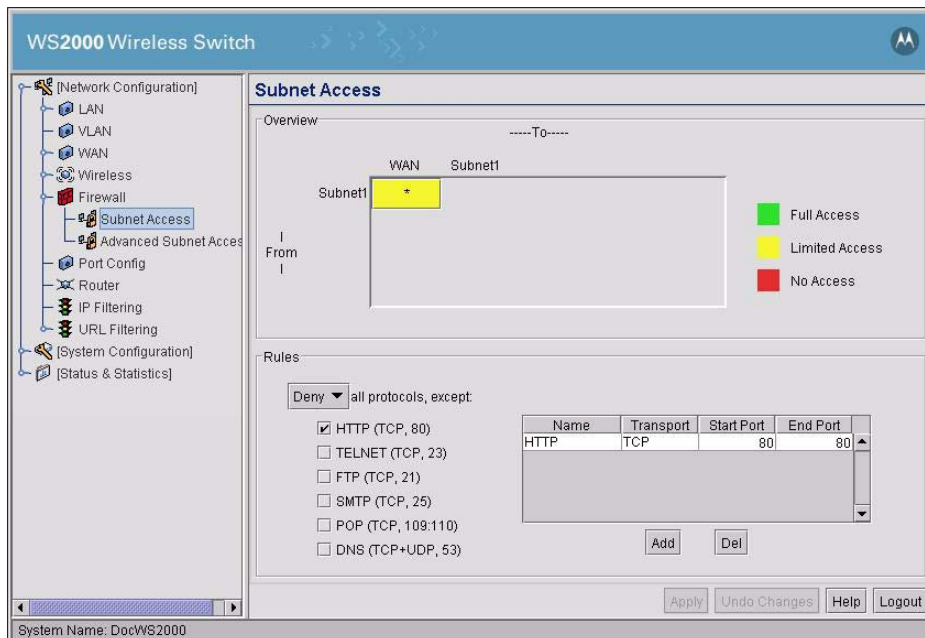
13. Option 43 is used to specify the IP address of a WIAP enabled switch, a switch that can adopt Access Ports in WIAP mode. This field accepts a comma separated list, for example, 192.168.0.1, 100.1.200.24

14. Use the **Static Mappings** table to associate static (or fixed) IP addresses with MAC addresses of specific wireless devices. Every wireless, 802.11x-standard device has a unique Media Access Control (MAC) address.

This address is the device's hard-coded hardware number (shown on the bottom or back). An example of a MAC address is 00:09:5B:45:9B:07. This MAC table of specified devices provides corresponding static IP addresses for users, mobile units, and applications that may prefer or require such access.

### 3.3 Configuring Subnet Access

The WS2000 Network Management System allows the administrator to set up access rules for subnet-to-subnet and subnet-to-WAN communication. These access rules control communication between subnets and the outside world (the WAN). Select **Network Configuration --> Firewall --> Subnet Access** to get to the Subnet Access screen.



#### 3.3.1 The Access Overview Table

In the overview table, each of the rectangles represents a subnet association. The three possible colors indicate the current access level, as defined, for each subnet association.

Color	Access Type	Description
Green	Full Access	No protocol exceptions (rules) are specified. All traffic may pass between these two areas.
Yellow	Limited Access	One or more protocol rules are specified. Specific protocols are either enabled or disabled between these two areas. Click the table cell of interest and look at the exceptions area in the lower half of the screen to determine the protocols that are either allowed or denied.
Red	No Access	All protocols are denied, without exception. No traffic will pass between these two areas.

### 3.3.2 The Access Exception Area

In the lower half of the screen, the access is controlled by specific rules that control the protocols that are allowed or denied between the two subnets or the subnet and the WAN. All rules are added to the exception table. The **Allow** or **Deny** menu item applies to all entries in the table. There are two ways to add entries (access rules) to the table. The first is by checking the check boxes for specific protocols (on the left). The second is by adding rules for specific port numbers by clicking the **Add** button and filling in the necessary information. A combination of the two methods can be used to add multiple entries to the table.

You can allow or deny communication through specific protocols using the following process:

1. Click in a cell of the table that represents the subnet-to-subnet (or subnet-to-WAN) relationship to define. All access rules (if any are defined) appear in the table in the lower-half of the screen.
2. Use the pull-down menu above the list to **Allow** or **Deny** all the entries specified in the exception table. You cannot allow some protocols (or ports) and deny others.
3. Enable or disable logging of firewall access by using the Enable logging check box. When enabled, a log entry is created every time a packet is denied by the action "Deny". A log entry is created once per session for packets that match the firewall rules when the action is "Allow".
4. From the list of check boxes on the left side, select those protocols to allow or deny. The protocols are automatically added to the table with the relevant Name, Transport, Start Port, and End Port information. The available protocols are shown in the table below.

Protocol	Transport, Port Used	Description
<b>HTTP</b>	TCP, 80	Hypertext Transfer Protocol (HTTP) is the protocol for transferring files on the World Wide Web. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols, the foundation protocols for the Internet.
<b>TELNET</b>	TCP, 23	TELNET is the terminal emulation protocol of TCP/IP. TELNET uses TCP to achieve a virtual connection between server and client, then negotiates options on both sides of the connection.
<b>FTP</b>	TCP, 21	File Transfer Protocol (FTP) is an application protocol that uses the Internet's TCP/IP protocols. FTP provides a simple and efficient way to exchange files between computers on the Internet.
<b>SMTP</b>	TCP, 25	Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used for sending and receiving email. Due to its limited ability to queue messages at the receiving end, SMTP is often used with POP3 or IMAP. SMTP sends the email, and then POP3 or IMAP receives the email.
<b>POP</b>	TCP, 109:110	Post Office Protocol (POP3) is a TCP/IP protocol intended to permit a workstation to dynamically access a maildrop on a server host. A workstation uses POP3 to retrieve email that the server is holding for it.
<b>DNS</b>	TCP+UDP, 53	Domain Name Service (DNS) protocol searches for resources using a database that is distributed among different name servers.

You can make changes to the information automatically filled into the table; however, note that changes in the selected transport type can change the port numbers that can be specified in the table.

5. To add an access rule for a protocol, port, or transport other than the ones available from the check boxes on the left, click the **Add** button. An empty row is added to the table.



- Specify a **Name** to identify the new access rule. For example, this could be the name of a particular application.
- Select a transport type from the **Transport** column's pull-down menu. The available transports are:

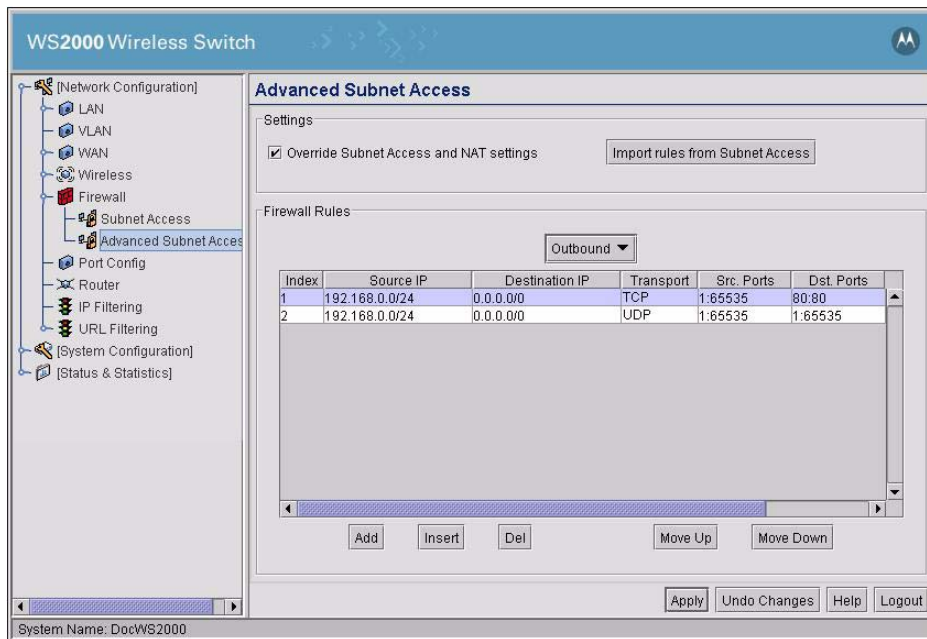
<b>Transport</b>	<b>Description</b>
<b>ALL</b>	This selection designates all of the protocols displayed in the table's pull-down menu, as described below.
<b>TCP</b>	Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.
<b>UDP</b>	User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.
<b>ICMP</b>	Internet Control Message Protocol (ICMP) is tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation. Because ICMP uses IP, ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.
<b>AH</b>	Authentication Header (AH) is one of the two key components of IP Security Protocol (IPSec). The other key component is Encapsulating Security Protocol (ESP), described below. AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
<b>ESP</b>	Encapsulating Security Protocol (ESP) is one of the two key components of IP Security Protocol (IPSec). The other key component is Authentication Header (AH), described above. ESP encrypts the payload of packets, and also provides authentication services. ESP can be used in transport mode, providing security between two end points. Also, ESP can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
<b>GRE</b>	General Routing Encapsulation (GRE) supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet that uses globally assigned IP addresses.

- Specify port information for the protocol. If the protocol uses only one port, enter the same port number in the **Start Port** and **End Port** columns, or leave the **End Port** column blank. Otherwise, use both columns for an entry that has a range of ports.
6. To enable or disable logging for a particular firewall rule, select the appropriate option from the pull-down menu for the field. When **default** option is selected, logging will depend on the global **Enable logging** field. To enable logging, select **enable**.
  7. Click the **Apply** button to save changes.

### 3.4 Advanced Subnet Access Settings

There can be situations in which the standard subnet access setting process is not specific enough for the needs of an organization. Instead, access or firewall rules need to be defined based upon destination and source IP addresses, transport types, and ports. The *Advanced Subnet Access* screen allows the administrator to create more complicated inbound and outbound policies.

Select **Network Configuration --> Firewall --> Advanced Subnet Access** from the left menu. The screen consists of two areas. The Settings area enables or disables the data found on this screen. The *Firewall Rules* area displays the currently defined and active firewall rules. This area will display either the inbound or outbound rules. The rules are applied in the order that they are listed. The rules at the top of the list take precedence over the rules lower in the list.



1. To enable the advanced access settings, check the **Override Subnet Access and NAT settings** box. The rest of the screen will become active. When this box is not checked, the settings in both the Subnet Access screen (under Firewall) and the NAT screen (under WAN) are disabled; the switch will use the settings found on this screen instead.
2. If you want the application to translate the subnet access settings into Firewall Rules (displayed in the lower area), click the **Import rules from Subnet Access** button. This button removes the need for the administrator to reenter the information defined on the Subnet Access screen.

Next, add, delete, or modify rules in the Firewall Rules list, as required.

3. Select **Inbound** or **Outbound** from the pull-down menu at the top of the Firewall Rules area, to display either the inbound (data entering the LAN) or outbound (data exiting the LAN) rules.
4. To modify a rule, select the rule from the **Firewall Rules** list, then edit the fields by clicking in the field to modify. Often a dialog box will appear to facilitate the entry of the field data.
5. To add a rule, click the **Add** button and then add data to the six rule fields. Note that not all fields are required.
6. To delete a rule, select a rule from the list and click the **Del** button.

7. Move rules to a higher or lower precedence by clicking the **Move Up** or **Move Down** buttons, as necessary.
8. When you have finished defining the Firewall Rules, click the **Apply** button to save changes.

Use the following information to help set the Firewall Rule fields:

- **Index**—The index number determines the order in which firewall rules will be executed. The rules are executed in order from lowest index number to highest number. Use the **Move Up** and **Move Down** buttons to change the index number.
- **Source IP**—The Source IP range determines the origin address(es) for the firewall rule. To set the Source IP range, click the field and a new window will pop up to enter the IP address and a second number that indicates that number of IP numbers starting at the first address (the range). An IP address of 0.0.0.0 indicates all IP addresses.
- **Destination IP**—The Destination IP range determines the target address(es) for the firewall rule. To configure the Destination IP range, click the field and a new window will pop up to enter the IP address and range. An IP address of 0.0.0.0 indicates all IP addresses.
- **Transport**—To determine the transport protocol to be filtered in the firewall rule, click the field to choose from the list of protocols:

Transport	Description
<b>ALL</b>	This selection designates all of the protocols displayed in the table's pull-down menu, as described below.
<b>TCP</b>	Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.
<b>UDP</b>	User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.
<b>ICMP</b>	Internet Control Message Protocol (ICMP) is tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation. Because ICMP uses IP, ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.
<b>AH</b>	Authentication Header (AH) is one of the two key components of IP Security Protocol (IPSec). The other key component is Encapsulating Security Protocol (ESP), described below. AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
<b>ESP</b>	Encapsulating Security Protocol (ESP) is one of the two key components of IP Security Protocol (IPSec). The other key component is Authentication Header (AH), described above. ESP encrypts the payload of packets, and also provides authentication services. ESP can be used in transport mode, providing security between two end points. Also, ESP can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).

Transport	Description
<b>GRE</b>	General Routing Encapsulation (GRE) supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet that uses globally assigned IP addresses.

- **Src. Ports (Source Ports)**—The source port range determines which ports the firewall rule applies to on the source IP address. To configure the source port range, click the field and a new window will pop up to enter the starting and ending ports in the range. For rules where only a single port is necessary, enter the same port in the start and end port fields.
- **Dst. Ports (Destination Ports)**—The destination port range determines which ports the firewall rule applies to on the destination IP address. To configure the destination port range, click the field and a new window will pop up to enter the starting and ending ports in the range. For rules where only a single port is necessary, enter the same port in the start and end port fields.
- **Rev. NAT (Reverse NAT) (inbound) / NAT (outbound)**—To enable NAT or reverse NAT for a firewall rule, enter this value.

For Inbound, click the **Rev. NAT** field and a new window will pop up to enter the IP address and translation port for the reverse NAT host.

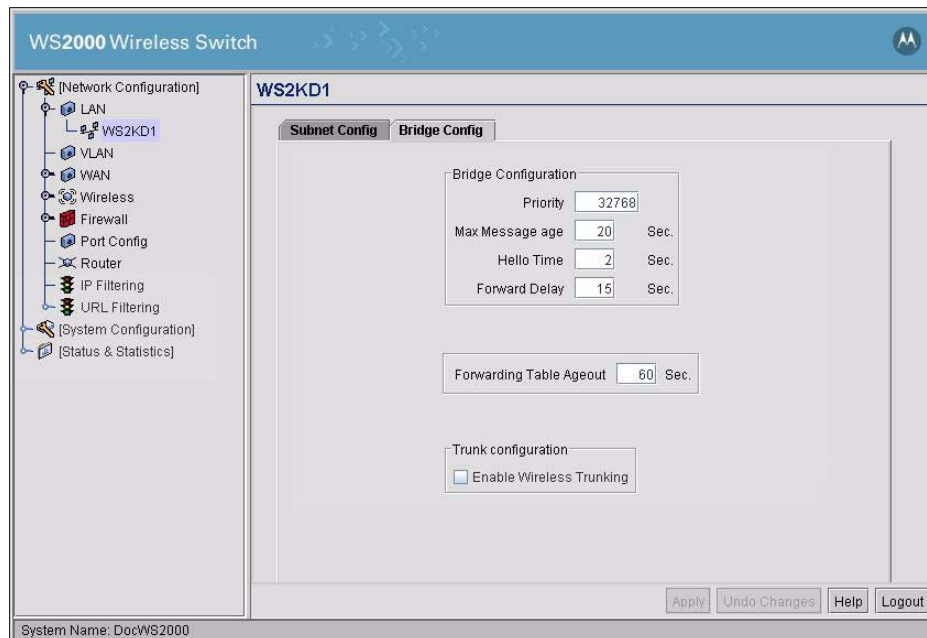
For the Outbound direction, select the WAN (WAN1, WAN2, and so on) from the **NAT** field menu that is associated with the appropriate NAT definition. (See [Configuring Network Address Translation \(NAT\)](#)).

- **Action**—Choose **Allow** or **Deny** from the pull-down menu in this field to determine whether the firewall rule is to allow or deny the specified rule.
- **Log** - Choose disable or enable from the pull-down menu in this field. When enabled, the following is the behavior.
  - A log entry is created every time a packet that matches this rule is denied by the action "Deny".
  - A log entry is created once per session for packets that match this rule is allowed access by the action "Allow".

## 3.5 Bridge Configuration

Bridges are data link layer devices. They operate at the Layer 2 of the OSI reference model. Bridges are generally used to connect different segments of the same network.

To configure Bridging, select **Network Configuration --> LAN --> <subnet>** and select the Bridging tab. The Bridge Config (Bridge Configuration) screen appears.



To configure the bridge:

1. Set the **Priority** for the bridge. Set the **Priority** as low as possible to force other devices within the mesh network to defer to this bridge as the root. A root bridge defines the mesh configuration. Motorola recommends assigning a Base Bridge AP with the lowest bridge priority so it becomes the root in the STP. If a root already exists, set the Bridge Priorities of new APs accordingly so that the root of the STP does not get altered. Each access point starts with a default bridge priority of 32768.
2. Set the **Maximum Message age** timer is used with the Message Age timer. The Message Age timer is used to measure the age of the received protocol information recorded for a port, and to ensure the information is discarded when it exceeds the value set for the Maximum Message age timer.
3. Set the **Hello Timer**. The **Hello Time** is the time between each bridge protocol data unit sent. This time is equal to 2 seconds by default, but you can tune the time to be between 1 and 10 seconds. If you drop the hello time from 2 seconds to 1 second, you double the number of bridge protocol data units sent or received by each bridge. The 802.1d specification recommends the **Hello Time** be set to a value less than half of the **Max Message age** value.
4. Set the **Forward Delay**. It is the time spent in the listening and learning state. This time is equal to 15 seconds by default, but you can tune the time to be between 4 and 30 seconds. The 802.1d specification recommends the **Forward Delay** be set to a value greater than half the **Max Message age** timeout value.
5. The **Forwarding Table Ageout** value defines the length of time an entry will remain in the a bridge's forwarding table before being deleted due to lack of activity. If the entry replenishments a destination generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table.
6. To enable wireless trunking, check the **Enable Wireless Trunking** check box. Also provide the IDs of the VLAN which allow tunneling.

## 3.6 Virtual LAN (VLAN) Configuration

A Virtual Local Area Network or VLAN is a switched network that has been segmented by function or application rather than by the traditional LAN segmentation which is based on physical location. VLANs allow a greater level of flexibility than a standard LAN, and enable changes to be made to the network infrastructure without physically disconnecting network equipment. The WS2000 Wireless Switch supports assigning one VLAN ID to each of the configured subnets.

To configure one or more VLANs, select **Network Configuration** --> **VLAN** from the navigation menu on the left. The *VLAN Configuration* screen appears.

The upper part of the screen is used to set up the VLAN type to be created.

1. Use the pull-down menu to select a **VLAN Type** for this switch. The two options available are *User Based* and *Port Based*.

**Port-based VLANs** partitions traffic based on port on which the packet is received. The switch inspects each packet, extracts the port on which it was received (from control information provided by the driver) and processes the packet based on the port. The port is mapped to a subnet and each subnet is mapped to a single VLAN. The switch processes the packet based on this mapping.

**User-based VLAN** traffic classification is performed only for Wireless traffic. The VLAN for a particular MU is identified when the MU authenticates itself with the RADIUS server using a user ID and password. The RADIUS server provides the VLAN ID corresponding to this MU and User ID information combination. The switch processes the packet based on the VLAN ID provided by the RADIUS server.

For wired traffic, the classification as done in Port-based VLANs applies.

2. Use the pull-down menu to select a **Trunk Port** for the switch. Only the WAN port can be configured as the Trunk Port.
3. Enter the **Default VLAN ID** to be used for packets that do not have the VLAN tag inserted. The default VLAN ID must be one of the IDs assigned to the subnets if the **VLAN Type** is *Port Based*. If the **VLAN Type** is *User Based*, then the **Default VLAN ID** must be one from the **Allowed VLANs** list.
4. For each enabled Subnet, enter the **VLAN ID**.

5. Enter a list of allowed VLANs between 1 and 4094 in the **Allowed VLANs** box. The VLANs in this list will be allowed access through the WAN port. When entering multiple VLAN IDs, separate each ID with a comma. When entering a range of VLAN IDs, separate the starting and ending values with a "-".
6. To enable filtering using IP, check the **Enable IP Filtering** check box. This option is only available only when **Trunk Port** is set to *Wan*. To add an IP filter, click **IP Filtering** button. The *IP Filtering* dialog appears. Set the appropriate filter and click **Ok** to close the dialog.
7. Click **Ok** on the *VLAN Configuration* screen to save changes.

**Note**

**NOTE:** Trunking VLANs through LAN ports is not available. For more information on trunking VLAN through the WAN port, and for assigning VLANs to WLANs, see *Chapter 10, Trunking VLANs Through the WAN Port*.

## 3.7 Configuring IP Filtering

IP based filtering allows administrators to configure Incoming and Outgoing IP filtering policies on packets within the same Subnet / WLAN and between wired and wireless hosts. Filters can be set up based on IP Address or as a default rule for all IPs in a given direction

Select **Network Configuration** --> **IP Filtering** from the left navigation menu.

1. Click the **Add** button to create a new filter in the table. The new filter can then be edited by clicking on the corresponding fields in the table.
2. Click on the **Filter Name** field and provide a name or edit an existing name for the filter. The Filter Name should be unique for each filter rule that is added.
3. Select a Protocol for the filter from the pull-down menu. The available protocols are:

Transport	Description
<b>ALL</b>	This selection designates all of the protocols displayed in the table's pull-down menu, as described below.



<b>Transport</b>	<b>Description</b>
<b>TCP</b>	Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.
<b>UDP</b>	User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.
<b>ICMP</b>	Internet Control Message Protocol (ICMP) is tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation. Because ICMP uses IP, ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.
<b>PIM</b>	Protocol Independent Multicast (PIM) is a collection of multicast routing protocols, each optimized for a different environment. There are two main PIM protocols, PIM Sparse Mode and PIM Dense Mode. A third PIM protocol, Bi-directional PIM, is less widely used.
<b>GRE</b>	General Routing Encapsulation (GRE) supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet that uses globally assigned IP addresses.
<b>RSVP</b>	The RSVP protocol is used by a host to request specific qualities of service from the network for particular application data streams or flows. RSVP is also used by routers to deliver quality-of-service (QoS) requests to all nodes along the path(s) of the flows and to establish and maintain state to provide the requested service. RSVP requests will generally result in resources being reserved in each node along the data path.
<b>IDP</b>	Datagram Protocol (IDP) is a simple, unreliable datagram protocol, which is used to support the SOCK_DGRAM abstraction for the Internet Protocol (IP) family. IDP sockets are connection less and normally used with the sendto and recvfrom subroutines.
<b>PUP</b>	It is the first open protocol, named the Public Unitary Protocol (PUP protocol). It was developed to standardize communications protocol among controls manufacturers in the facility automation industry. This protocol is generally understood to form the basis of the current BACnet protocol, which has become popular of late.
<b>EGP</b>	The Exterior Gateway Protocol (EGP) is an exterior routing protocol used for exchanging routing information with gateways in other autonomous systems.
<b>IPIP</b>	IPIP is a protocol which is used to encapsulate an IP packet within another IP packet.
<b>ESP</b>	Encapsulating Security Protocol (ESP) is one of the two key components of IP Security Protocol (IPSec). The other key component is Authentication Header (AH), described above. ESP encrypts the payload of packets, and also provides authentication services. ESP can be used in transport mode, providing security between two end points. Also, ESP can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).
<b>AH</b>	Authentication Header (AH) is one of the two key components of IP Security Protocol (IPSec). The other key component is Encapsulating Security Protocol (ESP), described below. AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).



<b>Transport</b>	<b>Description</b>
<b>IGMP</b>	The Internet Group Management Protocol (IGMP) is used between IP hosts and their immediate neighbor multicast agents to support the creation of transient groups, the addition and deletion of members of a group, and the periodic confirmation of group membership. IGMP is an asymmetric protocol and is specified here from the point of view of a host, rather than a multicast agent.
<b>IPv6</b>	IPv6 is short for "Internet Protocol Version 6". IPv6 is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4").
<b>COMPR_H</b>	COMPR_H is the Compressed Header Protocol.
<b>RAW_IP</b>	RAW IP is used when communication is done directly to the IP layer without using any additional protocols.

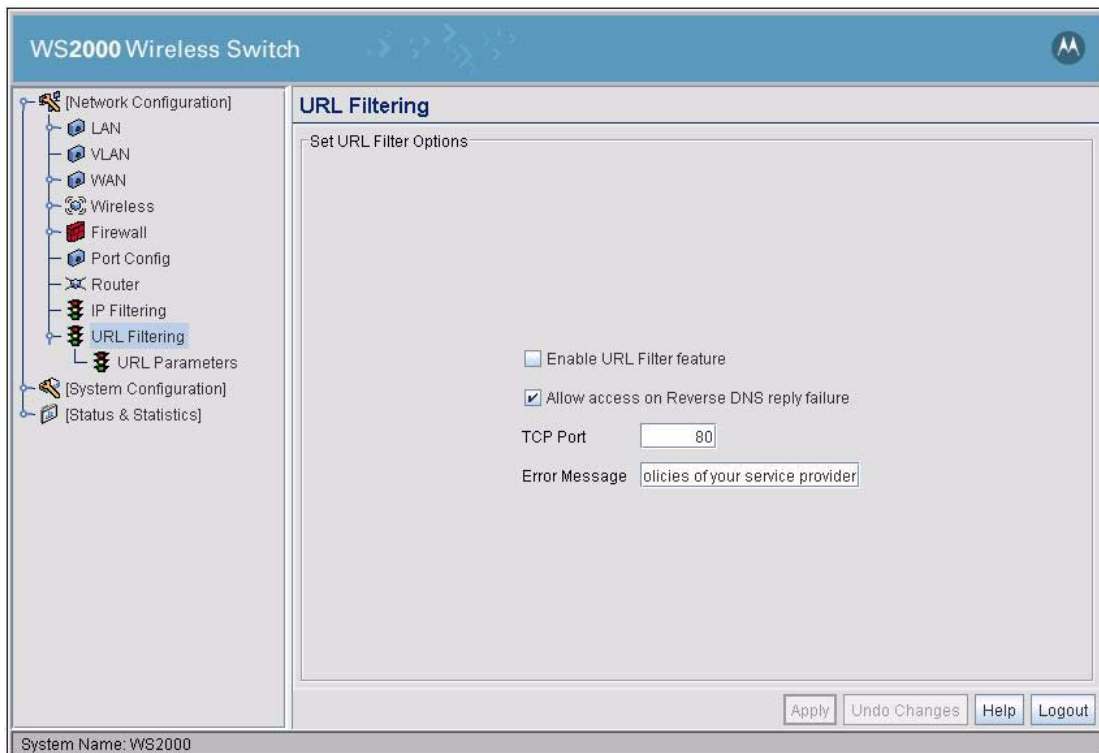
4. Select a **Port** from the pulldown menu for this IP Filtering rule to apply to. The default is **All** and will apply the filtering to all ports on the switch.
5. Enter the source IP range for the filtering rule in the **Src Start** and **Src End** fields.
6. Enter the destination IP range for the filtering rule in the **Dst Start** and **Dst End** fields.
7. The **In Use** field will display the current state of the filtering rule. When the rule is in use it will read **YES**. When the rule is not in use this field will read **NO**.

## 3.8 URL Filtering

Use the **URL Filtering** screen to filter out access through HTTP to websites and services that do not meet the organization's access policies. URL Filtering works on the principles of maintaining a list of websites that are permitted access to, a set of keywords that are allowed or denied search permissions, a list of blacklisted websites, and a list of trusted IP addresses. This combination controls the HTTP access of any user behind the WS2000 to any resources on the internet.

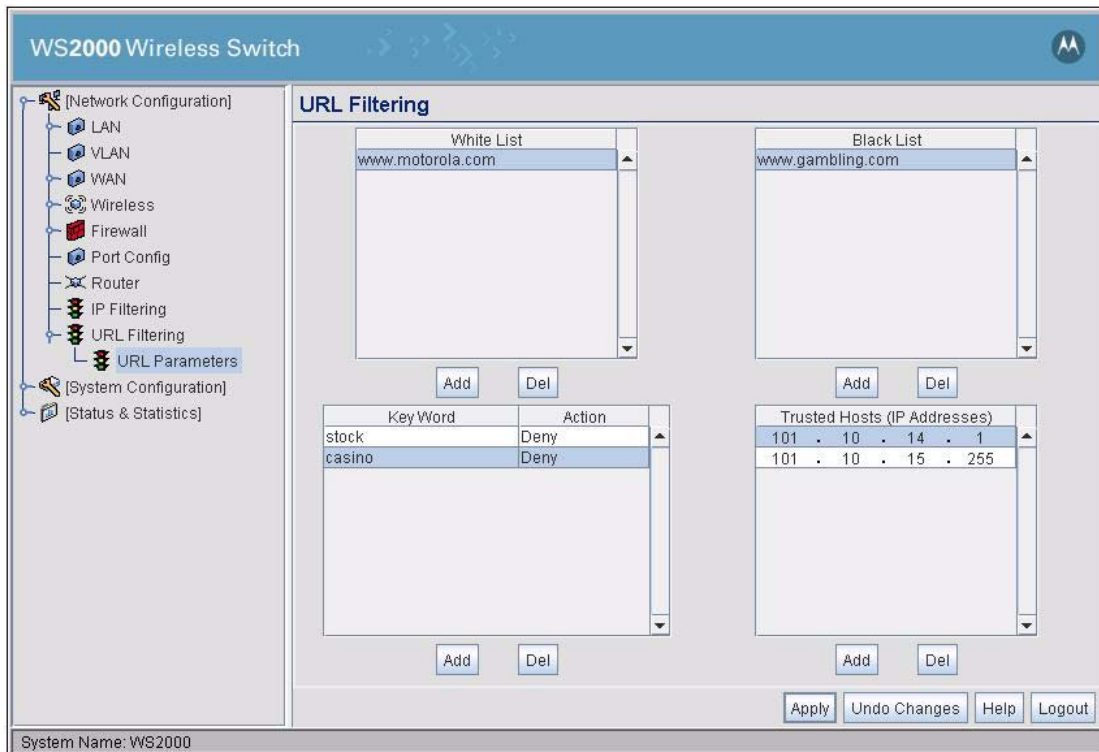
To use the URL Filtering feature, it must be enabled. By default, this feature is disabled enabling users unrestricted access. To enable the URL Filtering feature,

Select **[Network Configuration]** --> **URL Filtering** from the left navigation menu.



1. To enable the URL Filtering feature, select **Enable URL Filter feature**.
2. If required, select **Allow access on Reverse DNS reply failure**. This feature is used to control access to restricted website when the user tries to use an IP address instead of the URL of the restricted website. In this scenario, the WS2000 performs a reverse DNS lookup for the IP address. The reply is received in the form of a URL and this URL is used to apply filtering rules. If the reverse DNS lookup does not return an URL, then this feature enables you to control access.
3. The default port for TCP access is port 80. If your configured port for TCP is other than port 80, then use the **TCP Port** field to configure it. URL Filter feature will filter any traffic through this port.
4. Use the **Error Message** field to display the message a user will see when a URL is blocked.

To configure the filters to be used for URL Filter, select **[Network Configuration]** --> **URL Filtering** --> **URL Parameters**.



The URL Parameters screen contains four lists containing parameters used for URL filtering. There are four parameters:

- **White list** – Use this list to provide access to specific websites. Websites in the white list are always allowed access. Up to 50 URLs can be configured.
- **Black list** – Use this list to deny access to specific websites. Any attempt to access blacklisted websites are always denied. Up to 50 URLs can be configured.
- **Key word** – Use this list to provide a list of keywords and the action to undertake when this keyword is encountered in any URL. By default, the action is deny. Change this to allow to allow access when specific words are found in an URL. Up to 100 strings can be configured.
- **Trusted Hosts** – These devices on the network are always allowed access. URL filtering is not performed on requests from these hosts. Up to 50 hosts can be configured.

The URL filtering rules are checked in this order – Trusted Hosts, White List, Black List, Key word.

Use the **Add** button under each list to add a row. Enter the required information directly into the list.

Use the **Del** button under each list to remove a row. Select the row to delete and then click the **Del** button to remove.

## 3.9 Port Configuration

Use the **Port Configuration** screen to enable or disable each of the 6 LAN ports and the WAN port. Use this screen to set their Auto Negotiation mode, speed and duplex states too.

When the **Auto Negotiation** is enabled, the WS2000 determines the best operating speed and the duplex states for each port. To disable this, select **Disable** from the Auto Negotiation drop-down list.

To select the operating speed for the port, select either **10 M** or **100M** from the **Speed** drop-down list for each port. This value should be selected based on your network configuration.

To select the duplex mode for a port, select either **Half** or **Full** from the **Duplex** drop-down list. In half-duplex mode, traffic can pass only in one direction at a time. It can be either Rx or Tx. In full-duplex mode, traffic can pass in both direction simultaneously.

## ***WAN Configuration***

4.1	Configuring the WAN Interface	4-2
4.1.1	Configuring WAN IP Information	4-2
4.1.2	Setting Up Point-to-Point over Ethernet (PPPoE) Communication	4-3
4.2	Configuring the Firewall	4-5
4.2.1	Disabling the Firewall	4-5
4.2.2	Setting the NAT Timeout	4-5
4.2.3	Configurable Firewall Filters	4-6
4.2.4	Enabling NetBIOS ALG	4-7
4.3	Configuring Intrusion Prevention System	4-9
4.4	Configuring Network Address Translation (NAT)	4-12
4.5	Configuring Static Routes	4-14
4.5.1	Configuring the Default Gateway Interface	4-14
4.5.2	Creating User Defined Routes	4-15
4.5.3	Setting the RIP Configuration	4-15
4.6	Configuring a Virtual Private Network (VPN)	4-17
4.6.1	Creating a VPN Tunnel	4-18
4.6.2	Setting Up VPN Security	4-19
4.6.3	Configuring Manual Key Exchange	4-19
4.6.4	Setting Up Automatic Key Exchange	4-21
4.6.5	Setting Up Internet Key Exchange (IKE)	4-23
4.6.6	VPN: Frequently Asked Questions	4-25
4.7	Configuring Content Filtering	4-29
4.8	Configuring DynDNS	4-31
4.8.1	Enabling and Configuring DynDNS	4-31
4.8.2	Updating DynDNS	4-31

## 4.1 Configuring the WAN Interface

A wide area network (WAN) is a widely dispersed telecommunications network. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or cable modem to access the Internet.

The administrator needs to enter the WAN configuration information. The WS2000 Wireless Switch includes one WAN port. In order to set up communications with the outside world, select **Network Configuration** -> **WAN** from the left menu. The following WAN configuration page appears.

### 4.1.1 Configuring WAN IP Information

1. Check the **Enable WAN Interface** check box to enable a connection between the switch and a larger network or the outside world through the WAN port.
2. Check **This interface is a DHCP Client** check box to enable Dynamic Host Configuration Protocol (DHCP) for the WAN connection. If **This interface is DHCP Client** is checked, the switch is limited to one WAN IP address. This choice is required when:
  - The host router or switch on the WAN is communicating with the WS2000 Wireless Switch using DHCP.
  - The switch is interfacing with an Internet Service Provider (ISP) that uses DHCP addressing.



**Note**

**NOTE:** This setting is independent from the DHCP settings for the switch's internal subnets.

3. It is not necessary to specify the **IP Address** or any of the other fields on the top section of this form when the WS2000 Wireless Switch is set as a DHCP Client. The network host (router, switch, or modem) will provide these values each time it makes a connection with the switch.
4. If DHCP setting is not checked, fill in the information in this area. To find out the information to enter into these fields, contact the network administrator or the ISP that provided the cable modem or DSL router. All the fields below take standard IP addresses of the form xxx.xxx.xxx.xxx.

- The **IP Address** refers to the IP address that the outside world will use to address the WS2000 Wireless Switch.
- Click the **More IP Addresses** button to specify additional static IP addresses for the switch. Additional IP addresses are required when users within the LAN need dedicated IP addresses, or when servers in the LAN need to be accessed (addressed) by the outside world. The pop-up window allows the administrator to enter up to eight WAN IP addresses for the switch.
- The **Subnet Mask** is the mask used for the WAN.
- The **Default Gateway** is the address of the device that provides the connection to the WAN (often a cable modem or DSL router).
- The two DNS Server fields specify DNS addresses of servers that can translate domain names, such as `www.symbol.com`, into IP addresses that the network uses when passing information. The **Secondary DNS Server** acts as a backup to the **Primary DNS Server**, when the primary server is not responding.

## 4.1.2 Setting Up Point-to-Point over Ethernet (PPPoE) Communication

The screenshot shows the configuration interface for a WS2000 Wireless Switch. The left sidebar contains a tree view with categories like [Network Configuration], LAN, VLAN, WAN, Wireless, Firewall, Port Config, Router, IP Filtering, URL Filtering, [System Configuration], and [Status & Statistics]. The main area is titled 'WAN' and includes the following settings:

- Enable WAN Interface
- Tabbed interface with **DHCP** and **PPPoE** selected.
- Enable
- Configuration section:
  - Username: [ ]
  - Keep-Alive:
  - Password: [ ]
  - Idle Time (seconds): [ 600 ]
  - Authentication Type: [ PAP or CHAP ]
  - PPPoE MSS size: [ 1452 ]
- Status section:
  - IP Address: [ 0 . 0 . 0 . 0 ]
  - Primary DNS Server: [ 0 . 0 . 0 . 0 ]
  - Default Gateway: [ 157 . 235 . 208 . 246 ]
  - Secondary DNS Server: [ 0 . 0 . 0 . 0 ]
- PPPoE State: [ ]

Buttons at the bottom include Apply, Undo Changes, Help, and Logout. The system name 'DocWS2000' is visible at the bottom left.

PPPoE provides the ability to connect a network of hosts through a simple device to a remote access concentrator. Many DSL providers require that their clients communicate using this protocol. The facility allows the ISP to control access, billing, and type of service provided to clients on a per-user or per-site basis. Check with the network administrator or ISP to determine whether to enable this feature, and, if so, find out the username and password required for authentication.

1. Check **Enable** in the **PPP over Ethernet** area to enable the PPPoE protocol for high-speed connections.
2. Enter the **Username** and **Password** required for authentication. The username and password is for the switch's router to use when connecting to the ISP. When the Internet session starts, the ISP authenticates the username.
3. Set the **Idle Time** to an appropriate number. This number is the amount of time the PPPoE connection will be idle before it disconnects. The 10000 second default idle time is appropriate for most situations.

4. Check **Keep Alive** to instruct the switch to continue occasional communications over the WAN even when client communications to the WAN are idle. Some ISPs terminate inactive connections, while others do not. In either case, enabling Keep-Alive mode keeps the switch's WAN connection alive, even when there is no traffic. If the ISP drops the connection after some idle time, the switch automatically reestablishes the connection to the ISP.
5. Select the appropriate WAN authentication method from the drop-down menu. Collect this information from the network administrator. Select between **None**, **PAP**, **CHAP**, or **PAP or CHAP**.

<b>CHAP</b>	A type of authentication in which the person logging in uses secret information and some special mathematical operations to come up with a number value. The server he or she is logging into knows the same secret value and performs the same mathematical operations. If the results match, the person is authorized to access the server. One of the numbers in the mathematical operation is changed after every login, to protect against an intruder secretly copying a valid authentication session and replaying it later to log in.
<b>PAP</b>	An identity verification method used to send a user name and password over a network to a computer that compares the user name and password to a table listing authorized users. This method of authentication is less secure, because the user name and password travel as clear text that a hacker could read.

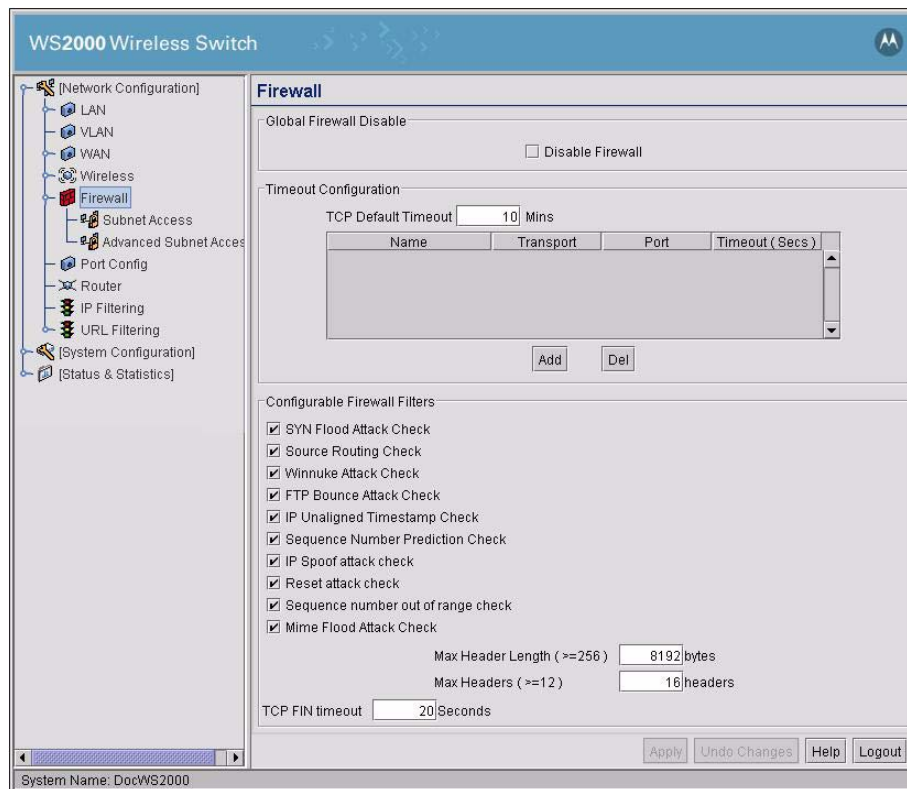
6. Click the **Apply** button to save changes.
7. Once connected, the **PPPoE State** section will display the provided **IP Address**, **Default Gateway**, **Primary DNS Server** and **Secondary DNS Server**



## 4.2 Configuring the WS2000 Firewall

The WS2000 Wireless Switch provides a secure firewall/Network Address Translation (NAT) solution for the WAN uplink. The firewall includes a proprietary CyberDefense Engine to protect internal networks from known Internet attacks. It also provides additional protection by performing source routing, IP unaligned timestamp, and sequence number prediction. The firewall uses a collection of filters to screen information packets for known types of system attacks. Some of the switch's filters are always enabled, and others are configurable.

To view or change the firewall settings, select **Network Configuration** --> **Firewall** from the left menu.



### 4.2.1 Disabling the Firewall

The firewall can be enabled or disabled with one click. Check **Disable Firewall** if the filters should not be active. By default the firewall is enabled.

### 4.2.2 Setting the NAT Timeout

#### 4.2.2.1 TCP Default Timeout

The **TCP Default Timeout** field is used to set the NAT timeout value. The table below **TCP Default Timeout** field enables you to setup the NAT timeout values based on the Port and the protocol used. If the table has no rows, the timeout value entered in the **TCP Default Timeout** is used for all protocols and ports.

In WS2000 Wireless Switch, the NAT timeout configuration is global for any TCP/IP packet going through the firewall. This configuration restricts the type of UDP or TCP applications that can be used with WS2000.

Enter a default timeout value (in seconds) for the switch to use as the timeout value when no matching records are found in the NAT Timeout Table below. This is a global configuration for any TCP/IP packets going through firewall that don't match other values.

#### 4.2.2.2 NAT Timeout Table

In addition to the **TCP Default Timeout** setting, NAT timeout rules for specific TCP and UDP ports can be configured.

To add rules to the NAT Timeout Table:

1. Click the **Add** button to add a row to the table.
2. Select a Transport method from the pull-down menu. Available options are:

<b>TCP</b>	Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.
<b>UDP</b>	User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.

3. Specify the **Port** number which the new timeout record will apply to.
4. Enter a **Timeout** value to specify the number of seconds before a NAT request is timed out by the switch's firewall.
5. Click the **Apply** button to save the changes to this page.

#### 4.2.3 Configurable Firewall Filters

The administrator can enable or disable the following filters. By default, all filters are activated. It is safe to turn the filters off if one of the following things is true:

- The switch is on a completely isolated network with no access to the Internet and is therefore secure.
- The switch is heavily loaded and a slight increase in performance outweighs the safety of the network.
- Blocking these types of attacks would also block legitimate traffic on their network, although this scenario is highly unlikely.

<b>SYN Flood Attack Check</b>	A SYN flood attack requests a connection and then fails to promptly acknowledge a destination host's response, leaving the destination host vulnerable to a flood of connection requests.
<b>Source Routing Check</b>	A source routing attack specifies an exact route for a packet's travel through a network, while exploiting the use of an intermediate host to gain access to a private host.
<b>Winnuke Attack Check</b>	A "Win-nuking" attack uses the IP address of a destination host to send junk packets to its receiving port. This attack is a type of denial of service (DOS) attack that completely disables networking on systems Microsoft Windows 95 and NT. Because this attack is only affective on older systems, it may not be necessary to enable this feature on a LAN with newer Microsoft Windows operating systems or with systems that have the appropriate "Winnuke" patches loaded.

<b>FTP Bounce Attack Check</b>	An FTP bounce attack uses the PORT command in FTP mode to gain access to arbitrary ports on machines other than the originating client.
<b>IP Unaligned Timestamp Check</b>	An IP unaligned timestamp attack uses a frame with the IP timestamp option, where the timestamp is not aligned on a 32-bit boundary.
<b>Sequence Number Prediction Check</b>	A sequence number prediction attack establishes a three-way TCP connection with a forged source address, and the attacker guesses the sequence number of the destination host's response.
<b>IP Spoof Attack Check</b>	An IP Spoof Attack floods a destination host using an IP address that is not reachable on that interface.
<b>Reset Attack Check</b>	An attack where the TCP session is ended prematurely by an attacking host.
<b>Sequence Number Out of Range Check</b>	An attack which uses packet numbers which are out of the valid sequence range.
<b>Mime Flood Attack Check</b>	<p>A MIME flood attack uses an improperly formatted MIME header in "sendmail" to cause a buffer overflow on the destination host.</p> <ul style="list-style-type: none"> <li>• Use the Max Header Length field to set the maximum allowable header length. Set this value to be at least 256 bytes.</li> <li>• Use the Max Headers field to set the maximum number of headers allowed. Set this value to be at least 12.</li> </ul>
<b>TCP FIN timeout</b>	Enter a TCP FIN timeout value (in seconds) to determine how long the WS2K has to wait to receive a FIN before it closes the TCP connection.

Click the **Apply** button to save changes made on this screen.

#### 4.2.4 Enabling NetBIOS ALG

Use the NetBIOS ALG feature to allow hosts on WAN side of WS2000 to access Windows™ share folders with HOSTNAME instead of the IP address of the LAN PC. When this feature is enabled, the Host need not know the IP address of the LAN PC to access it. The LAN PC can be access by it's name\share combination through Windows Explorer. For example, \\UserHome\JohnDoe.

Configuring NetBIOS ALG access requires two steps. Most of the configuration for using NetBIOS must be performed on the client device on the WAN side. On the devices on the WAN side of WS2000, the following configuration must be performed.

#### Configuring WAN Hosts



##### Note

**NOTE** These instructions are only valid for the Windows™ operating system.

- The WAN hosts should map the HOSTNAME of the LAN side PC against the WAN IP address of the WS2000 in their `c:\windows\system32\drivers\etc\lmhosts` file.
- WAN hosts should have their NetBIOS over TCP/IP enabled.

To enable NetBIOS over TCP/IP on the WAN Hosts, do the following

1. Open the *Local Area Connection Properties* dialog for the WAN Host.
2. Click **Internet Protocol (TCP/IP)** to select it.

3. Click **Properties** button. The *Internet Protocol (TCP/IP) Properties* dialog box opens
4. Click the **Advanced** button located at the bottom right of the dialog box. The *Advanced TCP/IP Settings* dialog opens.
5. Select the WINS tab to enable it.
6. In the NetBIOS setting group, select the **Default** radio. You can also select the **Enable NetBIOS over TCP/IP** radio.
7. Click **OK** in each dialog box to close it.

The LAN side PC can be accessed using this format:

```
\\<host-name>\<shared-drive-name>
```

PCs on the LAN side need not be configured.

### **Configuring the WS2000**

Navigate to the Firewall screen using **[Network Configuration]** --> **Firewall** in the left navigation menu tree. Click **Enable NetBIOS ALG** check box to select it.

## 4.3 Configuring Intrusion Prevention System

IP networks are vulnerable to security breaches by attackers exploiting known bugs in installed softwares. These attacks can originate from any host on the network or from devices outside the network. These attacks can either be intentional or un-intentional. If such an attack succeeds, the attacker could get access to vital and sensitive information stored on the host or can execute malicious code on the host or just prevent the host or hosts from functioning normally.

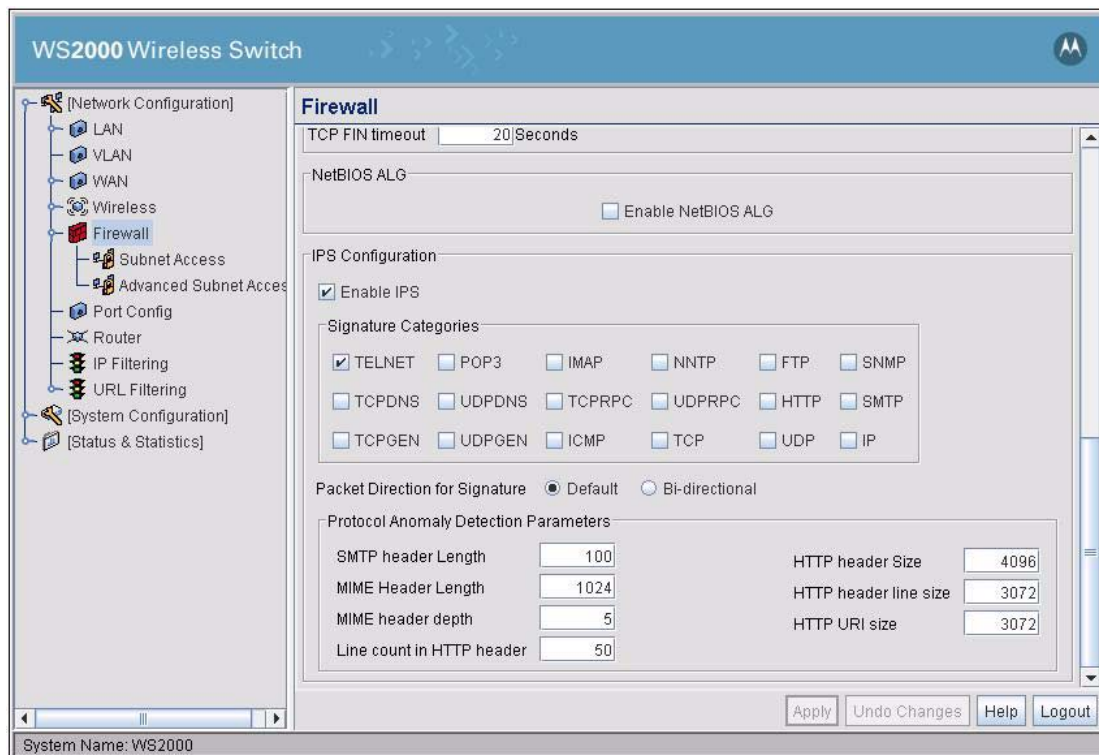
Intrusion Prevention System (IPS) works alongside the firewall to detect vulnerability to such attacks. Any packet that flows through the network is examined by the IPS. Unlike the firewall which examines and blocks traffic based on IP addresses and ports, the IPS looks at different fields of the network traffic and then manages the traffic based on pre-defined patterns called "Signatures".

A signature is based on the protocol, source/destination ports, and the data pattern of the load. The signature also defines the action to be taken when an attack is detected. The action can be one of:

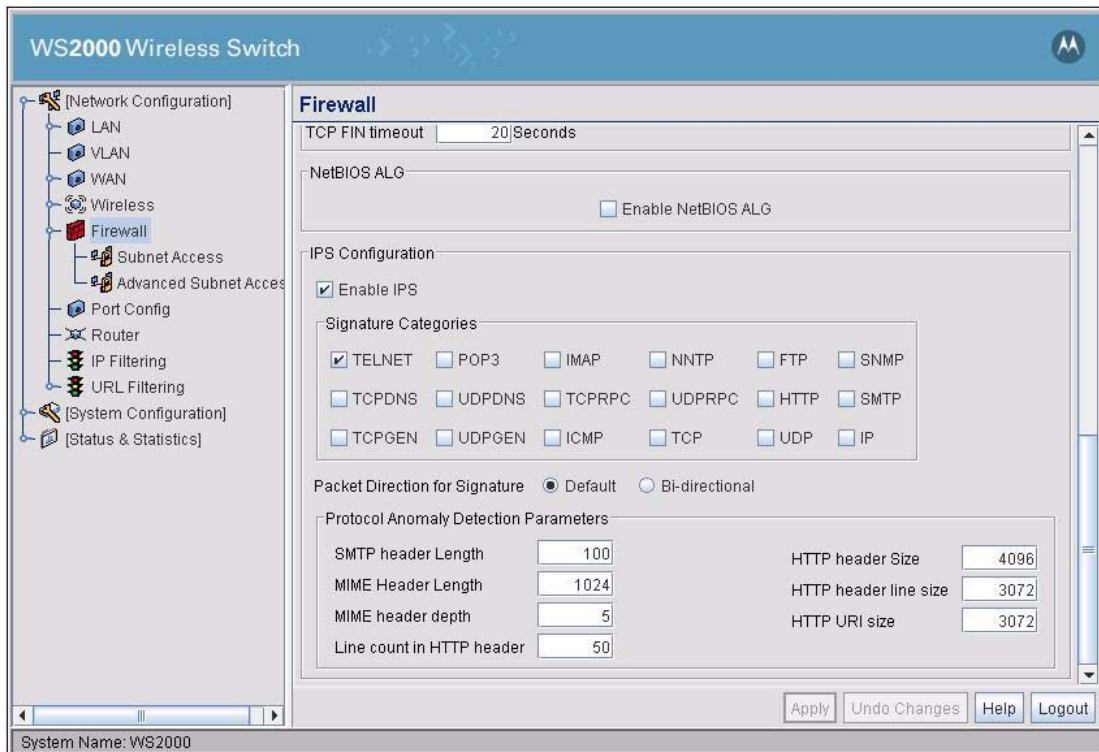
- Drop the connection (in case of TCP connection)
- Drop the packet
- Generate an informative log message and then allow the packet through.

Each and every packet entering or leaving the network is matched and the appropriate action taken.

1. IPS can be configured from the **Network Configuration --> Firewall** menu. The following screen appears.



Scroll to the bottom of the window to configure IPS settings.



- To enable IPS, select the **Enable IPS** check box.
- To enable the different signature categories that IPS uses, check the appropriate check box in the **Signature Categories** group. When checked, the IPS checks for intrusion on that protocol. The following IPS signature categories are available.

<b>TELNET</b>	<b>POP3</b>	<b>IMAP</b>
<b>NNTP</b>	<b>FTP</b>	<b>SNMP</b>
<b>TCPDNS</b>	<b>UDPDNS</b>	<b>TCRPC</b>
<b>UDPRPC</b>	<b>HTTP</b>	<b>SMTP</b>
<b>TCPGEN</b>	<b>UDPGEN</b>	<b>ICMP</b>
<b>TCP</b>	<b>UDP</b>	<b>IP</b>

- Select the packet direction for applying signature-categories. The signature-categories define the packet direction - inbound, outbound, or both - when the packet is checked for any attack. **Default** indicates the direction as defined in the signature-category. **Bi-directional** indicates that the any incoming and outgoing packet for that protocol is checked.

5. Set the Protocol Anomaly Detection Parameters next. The following values have to be provided.

<b>SMTP Header Length</b>	Enter the SMTP header length in this field.
<b>MIME Header Length</b>	Enter the MIME header length in this field.
<b>MIME Header Depth</b>	Enter the MIME header depth in this field.
<b>Line count in HTTP Header</b>	Enter the number of lines in the HTTP header in this field.
<b>HTTP Header Size</b>	Enter the HTTP header size in this field.
<b>HTTP Header Line Size</b>	Enter the HTTP header line size in this field.
<b>HTTP URI Size</b>	Enter the HTTP URI size in this field.

The values entered for each of the above parameters are the maximum allowed values for that parameter.

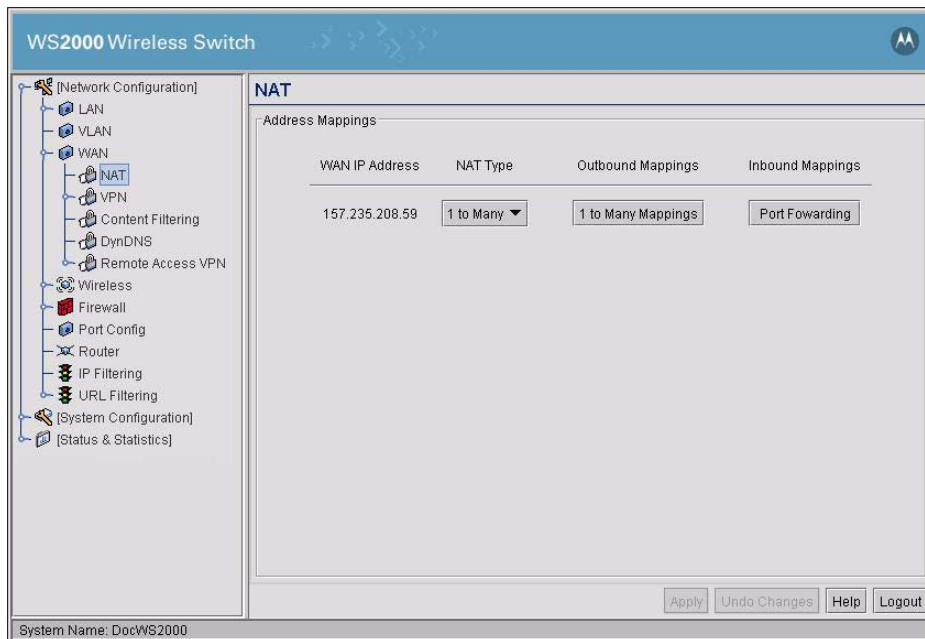
6. Click **Apply** to save changes to the device.

## 4.4 Configuring Network Address Translation (NAT)

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. Generally NAT allows a single device such as a router to act as an agent between the public network and the private network to address issues related to IP address shortage.

NAT here translates the WAN addresses to the external network addresses.

1. Select **Network Configuration** --> **WAN** --> **NAT** from the left menu. The following screen appears.



This screen displays the IP addresses specified in the WAN screen (**Network Configuration** --> **WAN** from the left menu). Up to eight WAN addresses can be associated with the switch. The NAT screen enables the administrator to set of the type of translation and port forwarding required.

2. For each of the addresses, the select the NAT type.
  - Select **1 to 1** from the pull-down menu to map a WAN IP address to a single local (subnet) IP address. This selection is useful in situations in which users require dedicated IP addresses or when public-facing servers are connected to the switch.
  - Select **1 to Many** from the pull-down menu to map a WAN IP address to a range of local IP addresses. Use this option when there are fewer public IP address on the WAN than there are users on the LAN. **1 to Many** NAT allows a single IP address to handle traffic from multiple private LAN IP addresses.
  - Select **None** from the pull-down menu when the administrator sets up routable IP addresses (set on the **Network Configuration** --> **Routing** screen).
3. If the NAT type is **1 to 1**, the **Outbound Mappings** field allows the administrator to specify a single IP Address. This address specifies the 1-to-1 mapping between the WAN IP address the specified LAN IP address.



WAN IP Address	NAT Type	Outbound Mappings	Inbound Mappings
157.235.208.238	1 to 1	0 . 0 . 0 . 0	Port Forwarding

4. If the NAT type is **1 to Many**, the **1 to Many** button in the adjacent **Outbound Mappings** field is active, allowing the administrator to specify address assignments for each subnet. If no translation should be done, none should be selected for the subnet.

**1 to Many Mappings**

Subnet1 IP addresses get translated to: 157.235.208.238

Ok Cancel Help

Java Applet Window

5. Click the **Port Forwarding** button to display a sub-screen of port forwarding parameters for inbound traffic from the associated WAN IP address. When finished, click the **Ok** button to close the screen.

**157.235.208.238 Port Forwarding**

Name	Transport	Start Port	End Port	IP Address	Translation Port
TestCon	TCP	80	80	157.235.208.10	1080

Add Del

Forward all unspecified ports to: 157.235.0.10

Ok Cancel Help

Java Applet Window

6. Click **Add** to add a new port forwarding entry and fill in the following fields.

<b>Name</b>	Enter a name for the service that is being forwarded. The name can be any alphanumeric string and is used for easy identification of the service.
<b>Transport</b>	Use this pull-down menu to specify the transport protocol used in this service. The choices are <b>ALL</b> , <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , <b>AH</b> , <b>ESP</b> , and <b>GRE</b> .
<b>Start Port / End Port</b>	Enter the port or ports used by this service. To specify a single port, enter the port number in the <b>Start Port</b> field. To specify a range of ports, use both the <b>Start Port</b> and <b>End Port</b> fields to enter the port numbers. For example, enter 110 in the <b>Start Port</b> field and 115 in the <b>End Port</b> field.
<b>IP Address</b>	Enter the <b>IP address</b> to which the specified service is forwarded. This address must be within the specified NAT range for the associated WAN IP address.

<b>Translation Port</b>	Enter the port to which traffic is sent to after translation.
-------------------------	---

- Click the **Forward all unspecified ports to** check box and then specify an IP address to enable port forwarding for incoming packets with unspecified ports.
- Click the **Apply** button on the NAT screen to save changes.

## 4.5 Configuring Static Routes

A router uses routing tables and protocols to forward data packets from one network to another. The WS2000 switch's router manages traffic within the switch's network, and directs traffic from the WAN to destinations on the switch-managed LAN. The WS2000 Network Management System provides the Router screen to view and set the router's connected routes. To view this screen, select **Network Configuration --> Router** from the menu on the left.

The **Route Table** area of the screen displays a list of currently connected routes between the enabled subnets, the WAN, and the router. The information here is generated from settings applied on the Subnet and WAN screens. The destination for each subnet is its IP address. The subnet mask (or network mask) and gateway settings are those belonging to each subnet, or to the WAN in general. To make changes to the information in the Connected Routes information, go to the appropriate subnet screen (**LAN --> <subnet name>**) or the WAN screen (**WAN**).

### 4.5.1 Configuring the Default Gateway Interface

The Default Gateway Interface allows you to specify which interface will be used as the default gateway for all unspecified routes on the WS2000. The available options are:

<b>None</b>	Selecting this option will not set a Default Gateway Interface for unspecified routes.
<b>WAN</b>	Sets the WAN interface as the Default Gateway Interface for all unspecified routes.
<b>Subnet 1</b>	If Subnet 1 is enabled, sets it as the Default Gateway Interface for all unspecified routes.

<b>Subnet 2</b>	If Subnet 2 is enabled, sets it as the Default Gateway Interface for all unspecified routes.
<b>Subnet 3</b>	If Subnet 3 is enabled, sets it as the Default Gateway Interface for all unspecified routes.
<b>Subnet 4</b>	If Subnet 4 is enabled, sets it as the Default Gateway Interface for all unspecified routes.
<b>Subnet 5</b>	If Subnet 5 is enabled, sets it as the Default Gateway Interface for all unspecified routes.
<b>Subnet 6</b>	If Subnet 6 is enabled, sets it as the Default Gateway Interface for all unspecified routes.
<b>default</b>	Sets the gateway to <b>default</b> for all unspecified routes.

## 4.5.2 Creating User Defined Routes

The **User Defined Routes** area of the screen allows the administrator to view, add or delete internal static (dedicated) routes, and to enable or disable routes that are generated using the Routing Information Protocol (RIP). If RIP is enabled, this table can also include routes that RIP generates.

This table also includes internal static routes that the administrator adds. Internal static routes are dedicated routes for data that travels from the WAN, through the switch, and to a specified subnet. Such routes are supplemental to the default routes already set up for each of the subnets.

1. Click the **Add** button to create a new table entry.
2. Specify the destination IP address, subnet mask, and gateway information for the internal static route.
3. Select an enabled subnet from the **Interface** column's drop-down menu to complete the table entry. Information in the **Metric** column is automatically generated, and is used by router protocols to determine the best hop routes.
4. Click the **Apply** button to save changes.

## 4.5.3 Setting the RIP Configuration

Routing Information Protocol (RIP) is an interior gateway protocol that specifies how routers exchange routing-table information. The Routing screen also allows the administrator to select the type of RIP and the type of RIP authentication used by the switch. To set or view the RIP configuration, click the **RIP Configuration** button. The following subscreen appears.

The screenshot shows the 'RIP Configuration' window with the following settings:

- RIP Configuration:**
  - RIP Type: No RIP
  - RIP Direction: Both
- RIP v2 Authentication:**
  - Authentication Type: None
  - Password (Simple Authentication): [Empty field]
  - Key #1:
    - MD5 ID (1-256): 1
    - MD5 Auth Key (16 Characters): [Redacted]
  - Key #2:
    - MD5 ID (1-256): 1
    - MD5 Auth Key (16 Characters): [Redacted]

Buttons: Ok, Cancel, Help

Java Applet Window

1. Select the **RIP Type** from the pull-down menu to be one of the following values.

<b>No RIP</b>	Depending on the <b>RIP Direction</b> setting, the <b>No RIP</b> option partially or completely disallows the switch's router from exchanging routing information with other routers. Routing information may not be appropriate to share, for example, if the switch manages a private LAN.
<b>RIP v1</b>	RIP version 1 is a mature, stable, and widely supported protocol. It is well suited for use in stub networks and in small autonomous systems that do not have enough redundant paths to warrant the overhead of a more sophisticated protocol.
<b>RIP v2 (v1 compat)</b>	RIP version 2 (compatible with version 1) is an extension of RIP v1's capabilities, but it is still compatible with RIP version 1. RIP version 2 increases the amount of packet information to provide a simple authentication mechanism to secure table updates.
<b>RIP v2</b>	RIP version 2 enables the use of a simple authentication mechanism to secure table updates. More importantly, RIP version 2 supports subnet masks, a critical feature that is not available in RIP version 1. This selection is not compatible with RIP version 1 support.

2. Select a routing direction from the RIP Direction drop-down menu. **Both** (for both directions), **Rx only** (receive only), and **TX only** (transmit only) are available options.
3. If **RIP v2** or **RIP v2 (v1 compat)** is the selected RIP type, the **RIP v2 Authentication** area of the screen becomes active. Select the type of authentication to use from the Authentication Type drop-down menu. Available options are:

<b>None</b>	This option disables the RIP authentication.
<b>Simple</b>	This option enable RIP version 2's simple authentication mechanism. This setting activates the <b>Password (Simple Authentication)</b> field.
<b>MD5</b>	This option enables the MD5 algorithm for data verification. MD5 takes as input a message of arbitrary length and produces a 128-bit fingerprint. The MD5 algorithm is intended for digital signature applications, in which a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptographic system. The MD5 setting activates the <b>RIP v2 Authentication</b> settings for keys (below).

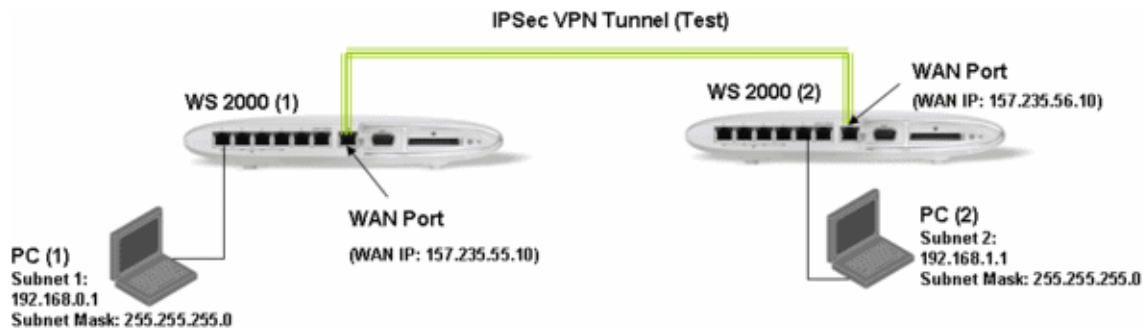
4. If the **Simple** authentication method is selected, specify a password of up to 15 alphanumeric characters in the **Password (Simple Authentication)** field.
5. If the **MD5** authentication method is selected, fill in the **Key #1** and **Key #2** fields. Type in any numeric value between 0 and 256 into the **MD5 ID** field. Type in any string consisting of 16 alphanumeric characters into the **MD5 Auth Key** field.
6. Click the **Ok** button to return to the Routing screen.

## 4.6 Configuring a Virtual Private Network (VPN)

VPNs are IP-based networks that use encryption and tunneling to give users remote access to a secure LAN. In essence, the trust relationship is extended from one LAN across the public network to another LAN, without sacrificing security. A VPN behaves similarly to a private network; however, because the data travels through the public network, three types of security mechanisms are required: confidentiality, integrity, and authentication.

- Confidentiality (through public-key or secret-key cryptography) ensures the privacy of information being exchanged between communicating parties.
- Integrity ensures that information being transmitted over the public Internet is not altered in any way during transit (by using hash codes, message authentication codes, or digital signatures).
- Authentication (with password authentication or digital signatures) ensures the identity of all communicating parties.

A diagram of a typical VPN situation is shown below, where there is a VPN tunnel created between two WS2000 switches across the WAN. The diagram shows the settings for both switches.



### VPN Tunnel Configuration Settings for WS 2000 (1):

- Tunnel Name: Test
- Local Subnet: Subnet1
- Local WAN IP: 157.235.55.10
- Remote Subnet: 192.168.1.1 [For PC on WS 2000 (2)]
- Remote Subnet Mask: 255.255.255.0
- Remote Gateway: 157.235.56.10 [WAN IP of WS 2000 (2)]
- Default Gateway: 157.235.56.10 [Set in WAN config of WS 2000 (1)]

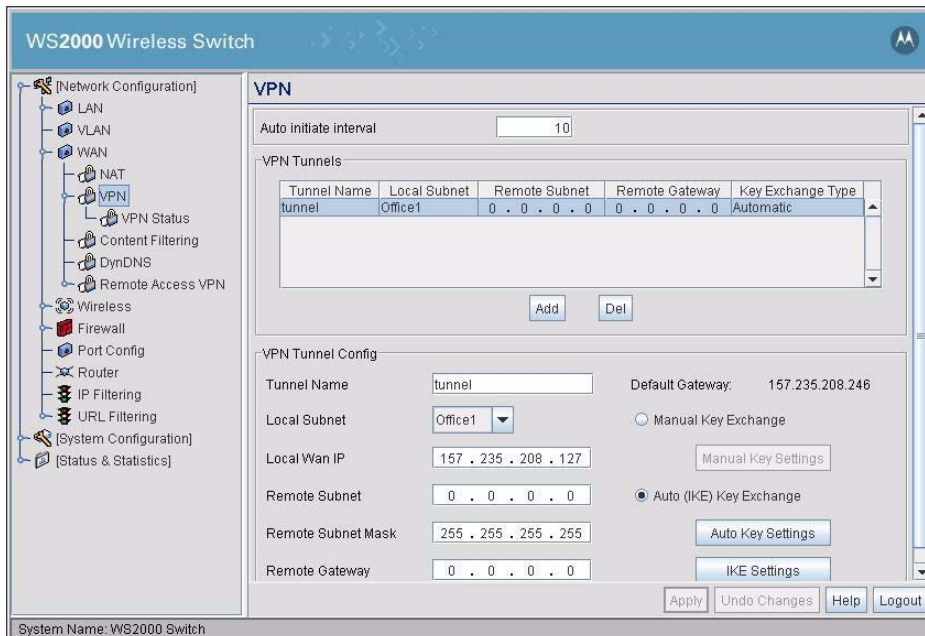
Note: When connecting the WS 2000 through a router the Default Gateway will be the interface of that router.

### VPN Tunnel Configuration Settings for WS 2000 (2):

- Tunnel Name: Test
- Local Subnet: Subnet2
- Local WAN IP: 157.235.56.10
- Remote Subnet: 192.168.0.1 [For PC on WS 2000 (1)]
- Remote Subnet Mask: 255.255.255.0
- Remote Gateway: 157.235.55.10 [WAN IP of WS 2000 (1)]
- Default Gateway: 157.235.55.10 [Set in WAN config of WS 2000 (2)]

Note: When connecting the WS 2000 through a router the Default Gateway will be the interface of that router.

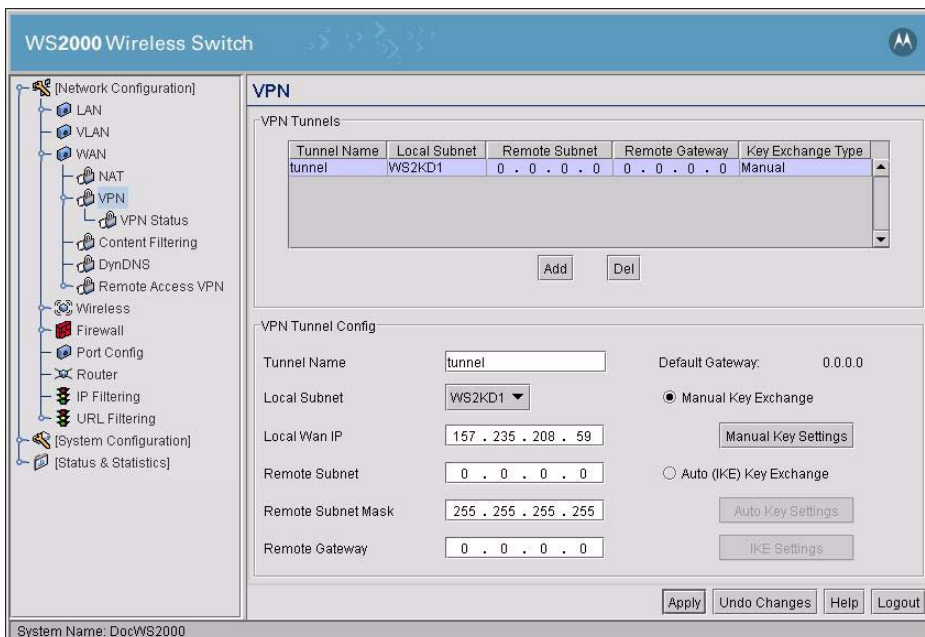
The WS2000 Network Switch provides VPN technology with a variety of security and setup options. Select **Network Configuration** --> **WAN** --> **VPN** from the left menu to create a VPN tunnel.



Use the **Auto Initiate Interval** to set the interval when the status of all tunnels are checked. This is a global configuration which is common for all the tunnels and is valid only when *Auto Initiate* is enabled. Normally, when the tunnel's life time gets over, its gets disconnected. This feature ensures that the tunnel is automatically initiated once its life time is over.

#### 4.6.1 Creating a VPN Tunnel

1. Click the **Add** button to create a VPN tunnel. The lower portion of the screen, which then appears, is used to configure VPN tunneling.



2. Type a name for the tunnel into the **Tunnel Name** field. Use a name that indicates the role and purpose of the tunnel.

3. Select the subnet that will be the local end of the tunnel from the **Local Subnet** menu.
4. Specify the IP address to use for the local WAN (**Local Wan IP**), which should be one of the (up to) eight IP addresses specified in the WAN screen.
5. Specify the IP address for the **Remote Subnet** along with its subnet mask (**Remote Subnet Mask**). Remote Subnet is the remote end of the VPN tunnel. This field accepts 0.0.0.0 as the remote subnet IP address.
6. Specify the IP address for the **Remote Gateway**.
7. Click the **Apply** button to save the changes.

## 4.6.2 Setting Up VPN Security

The WS2000 Wireless Switch provides several different options for VPN security, all based upon encryption key exchange:

1. **Manual Key Exchange** uses the **Manual Key Settings** screen to specify the transform sets that will be used for VPN access.

A transform set is a combination of security protocols and algorithms that are applied to IPSec protected traffic. A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies which algorithms to use with the selected security protocol. During security association (SA) negotiation, both gateways agree to use a particular transform set to protect the data flow.

If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform. When a particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match the transform set at the remote end of the gateway.

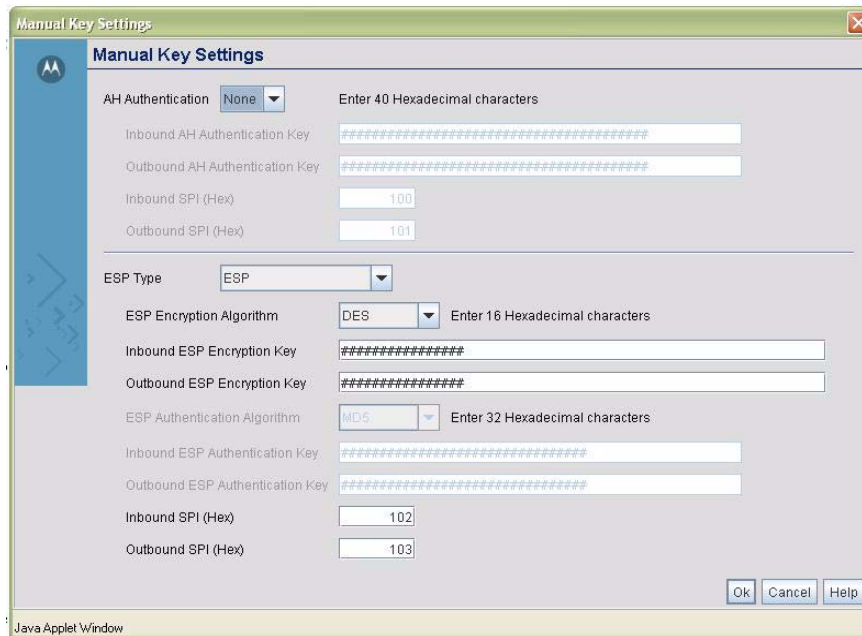
2. **Automatic Key Exchange** enables the WS2000 Wireless Switch to automatically set encryption and authentication keys for VPN access. The Auto Key Settings subscreen provides the means to specify the type of encryption and authentication, without specifying the keys.
3. **Internet Key Exchange (IKE)** 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.

Each of these options requires some configuration, as described below.

## 4.6.3 Configuring Manual Key Exchange

1. Select the **Manual Key Exchange** radio button.
2. Click the **Manual Key Settings** button to specify the encryption method and the following screen appears. The setup process requires specifying both the authentication and the encryption methods and keys.





3. Select the authentication and anti-replay method you wish to use for the tunnel from the **AH Authentication** menu.

<b>None</b>	Disables AH authentication and the rest of the fields in this area will not be active.
<b>MD5</b>	Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
<b>SHA1</b>	Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

4. If either **MD5** or **SHA1** is the authentication type, specify an **Inbound Authentication Encryption Key** and an **Outbound Authentication Encryption Key**. If **MD5** is the authentication type, specify 32-character hexadecimal keys. If **SHA1** is the authentication type, specify 40-character hexadecimal keys.

5. Provide up to an eight-character hexadecimal values for the **Inbound SPI** and **Outbound SPI** fields (minimum is 100). These fields are used to identify the inbound security association created by the AH algorithm. These values must match the corresponding outbound and inbound SPI values (respectively) configured on the remote security gateway. These values should also be unique across all tunnels on the system.

6. Select the **ESP Type** from the menu.

<b>None</b>	Disables ESP and the rest of the fields in this area will not be active.
<b>ESP</b>	Enables Encapsulating Security Payload encryption for this tunnel.
<b>ESP with Authentication</b>	Enables Encapsulating Security Payload encryption with authentication for this tunnel.

7. If **ESP** or **ESP with Authentication** is enabled, select an **Encryption Algorithm** from the menu.

<b>DES</b>	This option selects the DES encryption algorithm, which requires 64-bit (16-character hexadecimal) keys.
<b>3DES</b>	This option selects the 3DES encryption algorithm, which requires 192-bit (48-character hexadecimal) keys. When creating keys for 3DES, the first 8 bytes cannot equal the second 8 bytes, and the second 8 bytes cannot equal the third 8 bytes.



<b>AES 128-bit</b>	This option selects the Advanced Encryption Standard algorithm in use with 128-bit (32-character hexadecimal) keys.
<b>AES 192-bit</b>	This option selects the Advanced Encryption Standard algorithm in use with 192-bit (48-character hexadecimal) keys.
<b>AES 256-bit</b>	This option selects the Advanced Encryption Standard algorithm in use with 256-bit (64-character hexadecimal) keys.

8. Provide keys for both **Inbound ESP Encryption Key** and **Outbound ESP Encryption Key**. The length of the keys is mandated by the selected encryption algorithm. These keys must match the opposite keys at the remote gateway. The outbound key here must match the inbound key at the remote gateway, and the inbound key here must match the outbound key at the remote gateway.
9. If **ESP with Authentication** is enabled, an authentication algorithm must be selected to be used with ESP from the **ESP Authentication Algorithm** menu.

<b>MD5</b>	Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
<b>SHA1</b>	Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

10. If **ESP with Authentication** is enabled, specify both the **Inbound** and **Outbound ESP Authentication Keys**.
11. Provide two (up to) eight-character hexadecimal values used to identify the inbound and outbound security association created by the encryption algorithm. These values must match the reciprocal inbound/outbound SPI values configured on the remote security gateway, so the local inbound key must match the remote outbound key, and so on. This value should also be unique across all tunnels on the system.
12. Select **Ok** to return to the VPN screen.

#### 4.6.4 Setting Up Automatic Key Exchange

1. Select the **Auto (IKE) Key Exchange** radio button. This enables the Automatic **Key Settings** and **IKE Settings** buttons.
2. Click the **Automatic Key Settings** button to set up this security scheme and the following screen appears.



- Forward secrecy is a key-establishment protocol that guarantees that the discovery of a session key or a long-term private key will not compromise the keys of any other sessions. Select **Yes** from the **Use Perfect Forward Secrecy** menu to enable this option. Select **No** to disable Perfect Forward Secrecy.
- If **Perfect Forward Secrecy** is enabled, select an IKE Authentication Algorithm.

<b>G1 - 768bit</b>	Diffie-Hellman Group 1 Authentication uses a 768 bit algorithm for key exchange. Somewhat faster than the 1024-bit algorithm, but secure enough in most situations
<b>G2- 1024bit</b>	Diffie-Hellman Group 2 Authentication uses a 1024 bit algorithm for key exchange. Somewhat slower than the 768-bit algorithm, but much more secure and a better choice for extremely sensitive situations.

- In the **Security Association Life Time** field, enter a value (in minutes) that indicates how long the association will last before the VPN client will need to reauthenticate.
- Select the type of authentication from the **AH Authentication** menu. AH provides data authentication and anti-replay services for the VPN tunnel.

<b>None</b>	Disables AH authentication and the rest of the fields in this area will not be active.
<b>MD5</b>	Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
<b>SHA1</b>	Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

- Select the **ESP Type** from the menu.

<b>None</b>	Disables ESP and the rest of the fields in this area will not be active.
<b>ESP</b>	Enables Encapsulating Security Payload encryption for this tunnel.
<b>ESP with Authentication</b>	Enables Encapsulating Security Payload encryption with authentication for this tunnel.

- If **ESP** or **ESP with Authentication** is enabled, select an **Encryption Algorithm** from the menu.

<b>DES</b>	This options selects the DES encryption algorithm, which requires 64-bit (16-character hexadecimal) keys.
------------	---

<b>3DES</b>	This option selects the 3DES encryption algorithm, which requires 192-bit (48-character hexadecimal) keys. When creating keys for 3DES, the first 8 bytes cannot equal the second 8 bytes, and the second 8 bytes cannot equal the third 8 bytes.
<b>AES 128-bit</b>	This options selects the Advanced Encryption Standard algorithm in use with 128-bit (32-character hexadecimal) keys.
<b>AES 192-bit</b>	This options selects the Advanced Encryption Standard algorithm in use with 192-bit (48-character hexadecimal) keys.
<b>AES 256-bit</b>	This options selects the Advanced Encryption Standard algorithm in use with 256-bit (64-character hexadecimal) keys.

9. If **ESP with Authentication** is selected for the ESP type, select the authentication algorithm to be used with ESP from the ESP Authentication Algorithm menu.

<b>MD5</b>	Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
<b>SHA1</b>	Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

10. Check the **Auto Initiate** box to enable the feature. This feature ensures that a tunnel is available for use even when there is no traffic. Normally, the tunnel is disconnected when there is no traffic and the tunnel's life time gets over.

11. Select **Ok** to return to the VPN screen.

## 4.6.5 Setting Up Internet Key Exchange (IKE)

1. Select the **Auto (IKE) Key Exchange** radio button.
2. Click the **IKE Settings** button to set up the Internet Key Exchange and the following screen appears.

The screenshot shows the 'IKE Settings' dialog box with the following configuration:

- Operation Mode: Main
- Local ID Type: IP
- Local ID Data: empty
- Remote ID Type: IP
- Remote ID Data: empty
- IKE Authentication Mode: Pre Shared Key (PSK)
- IKE Authentication Algorithm: MD5
- IKE Authentication Passphrase: #####
- IKE Encryption Algorithm: DES
- Key Lifetime: 3600
- Diffie-Hellman Group: Group 1 - 768 bit
- Delete IPSEC SA with IKE SA: No
- Auto Initiate:

3. Select the **Operation Mode** for IKE. The Phase I protocols of IKE are based on the ISAKMP identity-protection and aggressive exchanges. IKE main mode refers to the identity-protection exchange, and IKE aggressive mode refers to the aggressive exchange.

<b>Main</b>	This is the standard IKE mode for communication and key exchange.
<b>Aggressive</b>	Aggressive mode is faster and less secure than Main mode. Identities are not encrypted unless public key encryption is used. The Diffie-Hellman group cannot be negotiated; it is chosen by the initiator. Also, the authentication method cannot be negotiated if the initiator chooses to use public key encryption.

4. Select the type of ID to be used for the WS2000 end of the tunnel from the **Local ID Type** menu.

<b>IP</b>	Select this option if the local ID type is the IP address specified as part of the tunnel.
<b>FQDN</b>	Select this item if the local ID type is a fully qualified domain name (such as sj.symbol.com). The setting for this field does not have to be fully qualified, it just must match the setting of the field for the Certificate Authority.
<b>UFQDN</b>	Select this item if the local ID type is a user unqualified domain name (such as john-doe@symbol.com). The setting for this field does not have to be unqualified, it just must match the setting of the field of the Certificate Authority.

5. If **FQDN** or **UFQDN** are selected, specify the data (either the qualified domain name or the user name) in the **Local ID Data** field.
6. Repeat steps 4 and 5 for the **Remote ID Type** and **Remote ID Data** fields.
7. Choose the authentication mode to be used with the IKE algorithm from the **IKE Authentication Mode** menu.

<b>Pre-shared key</b>	This option requires that you specify an authentication algorithm and passcode to be used during authentication.
<b>RSA Certificates</b>	Select this option to use RSA certificates for authentication purposes. See <a href="#">Managing Digital Certificates</a> to create and import certificates into the system.

8. IKE provides data authentication and anti-replay services for the VPN tunnel. Select the desired authentication methods from the **IKE Authentication Algorithm** menu.

<b>MD5</b>	Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
<b>SHA1</b>	Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

9. If **Pre-Shared Key** is the authentication mode, provide a key in the **IKE Authentication Passphrase** field. If **MD5** is the selected authentication algorithm, provide a 32-character hexadecimal key. If **SHA1** is the selected algorithm, provide a 40-character hexadecimal key.

10. Use the **IKE Encryption Algorithm** menu to select the encryption and authentication algorithms for this VPN tunnel.

<b>DES</b>	This options selects the DES encryption algorithm, which requires 64-bit (16-character hexadecimal) keys.
<b>3DES</b>	This option selects the 3DES encryption algorithm, which requires 192-bit (48-character hexadecimal) keys. When creating keys for 3DES, the first 8 bytes cannot equal the second 8 bytes, and the second 8 bytes cannot equal the third 8 bytes.

<b>AES 128-bit</b>	This options selects the Advanced Encryption Standard algorithm in use with 128-bit (32-character hexadecimal) keys.
<b>AES 192-bit</b>	This options selects the Advanced Encryption Standard algorithm in use with 192-bit (48-character hexadecimal) keys.
<b>AES 256-bit</b>	This options selects the Advanced Encryption Standard algorithm in use with 256-bit (64-character hexadecimal) keys.

11. Specify a **Key Lifetime**, which is the number of seconds that the key is valid. At the end of the lifetime, the key is renegotiated between the two parties.

12. Select the **Diffie-Hellman Group** to use. The Diffie-Hellman key agreement protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Two algorithms exist, one 768-bit and one 1024-bit algorithm.

<b>Group 1 - 768 bit</b>	Somewhat faster than the 1024-bit algorithm, but secure enough in most situations.
<b>Group 2 - 1024 bit</b>	Somewhat slower than the 768-bit algorithm, but much more secure and a better choice for extremely sensitive situations.

13. If you wish to delete the IPSEC Security Association (SA) with the IKE Security Association (SA) choose **Yes** from the **Delete IPSEC SA with IKE SA** menu. Otherwise select **No**.

14. Click the **Ok** button to return to the VPN screen.

## 4.6.6 VPN: Frequently Asked Questions

**WARNING! Disclaimer: Using a VPN connection over the WAN interface is subject to the limitations of your Internet Service Provider.**

### 4.6.6.1 My tunnel works fine when I use the Subnet Access page to configure my firewall. Now that I use Advanced Subnet Access, my VPN no longer works. What am I doing wrong?

VPN requires certain packets to be passed through the firewall. Subnet Access automatically inserts these rules for you when you do VPN. Using Advanced Subnet Access requires the following rules to be in effect for each tunnel.

An **allow** inbound rule:

<b>Src</b>	<Remote Subnet IP range>
<b>Dst</b>	<Local Subnet IP range>
<b>Transport</b>	ANY
<b>Src port</b>	1:65535
<b>Dst port</b>	1:65535
<b>Rev NAT</b>	None

An **allow** outbound rule:

<b>Src</b>	<Local Subnet IP range>
<b>Dst</b>	<Remote Subnet IP range>
<b>Transport</b>	ANY
<b>Src port</b>	1:65535
<b>Dst port</b>	1:65535
<b>Rev NAT</b>	None

For IKE, an **allow** inbound rule:

<b>Src</b>	<Remote Gateway IP address>
<b>Dst</b>	<Wan IP address>
<b>Transport</b>	UDP
<b>Src port</b>	1:65535
<b>Dst port</b>	500
<b>Rev NAT</b>	None

These rules must be above (higher in priority than) any default or other rules that would process these packets differently.

#### **4.6.6.2 Do I need to add any special routes on the WS2000 switch to get my VPN tunnel to work?**

No. Packets for VPN are tunneled directly to the Remote VPN gateway. As long as a route exists to the Remote VPN gateway, no other routes are required.

Clients, however, might need extra routing information to tell them to use the WS2000 switch as the gateway to reach the remote subnet. This is only required if the clients are not using the WS2000 switch as their default gateway.

#### **4.6.6.3 Can I setup the WS2000 Wireless Switch so that clients can both access the WAN normally and use the VPN when talking only to specific networks?**

Yes. Only packets that are going from the defined local subnet to the remote subnet will be send through the VPN tunnel. All other packets will be handled by whatever firewall rules are set.

#### 4.6.6.4 How do I specify which certificates to use from the WS2000 certificate manager to be used for an IKE policy?

When generating a certificate to be used with IKE, you must use one of the following fields: IP address, Domain Name, or E-mail address. Also make sure that you are using NTP when attempting use the certificate manager. Certificates are time sensitive.

On the IKE configuration page, Local ID type refers to the way that IKE selects a local certificate to use.

IP tries to match the local WAN IP to the IP addresses specified in a local certificate.

FQDM tries to match the user entered local ID data string to the domain name field of the certificate.

UFQDM tries to match the user entered local ID data string to the email address field of the certificate.

Remote ID type refers to the way you identify an incoming certificate as being associated with the remote side.

IP tries to match the remote gateway IP to the IP addresses specified in the received certificate.

FQDM tries to match the user entered remote ID data string to the domain name field of the received certificate.

UFQDM tries to match the user entered remote ID data string to the email address field of the received certificate.

The screenshot shows a 'Certificate Request' form with the following fields and controls:

- Key ID (required):
- Subject (required):
- Department:
- Organization:
- City:
- State:
- Postal Code:
- Country Code:
- Email:
- Domain Name:
- IP Address:
- Signature Algorithm: MD5-RSA (dropdown)
- Key Length: 512 (dropdown)
- Buttons: Generate, Clear, Cancel, Help

#### 4.6.6.5 I am using a direct cable connection between by two VPN gateways for testing and cannot get a tunnel established, yet it works when I setup them up across another network or router. What gives?

The packet processing architecture of the WS2000 VPN solution requires a WAN default gateway to work properly. When connecting two gateways directly, you really do not need a default gateway when the two addresses are on the same subnet. As a work around, you can point the WS2000 switch's WAN default gateway to be the other VPN gateway, and vice-versa.

#### 4.6.6.6 My WS2000 switch is a DHCP client on my WAN interface. How can I setup a tunnel without knowing my WAN IP address?

First of all, one end of a VPN tunnel **must have** a static IP address. Assuming the other end of your VPN tunnel has a static IP, here is how you configure your WS2000 switch to use a DHCP WAN address with VPN.

1. Your VPN tunnel entry must have the Local WAN IP set to 0.0.0.0.
2. If you are using the IKE, the Local ID type (and corresponding Remote ID type on the other end) cannot be set to IP, since the IP address is not known.

#### **4.6.6.7 How can I setup the WS2000 switch to accept VPN tunnels from gateways that have a DHCP WAN address?**

To accept a VPN tunnel from a unknown (DHCP) address, the WS2000 Wireless Switch operates in what is called responder-only mode. That is, it cannot initiate the VPN connection. It can only wait for a VPN connection to come in. Clients behind a responder-only cannot connect to the remote subnet until the remote subnet has connected to them.

To setup responder-only mode, set the Remote Gateway to **0.0.0.0**. If you are using IKE the following restrictions are in place:

- Remote ID type cannot be **IP**. We do not know the IP of the remote since it is DHCP.
- IKE Authentication Mode cannot be set to **PSK** if IKE mode is set to **Main Mode**.
- You may not use **xAuth** for this tunnel.

#### **4.6.6.8 I have two WS2000 switches and both have DHCP WAN addresses. Is there any possible way to open a VPN tunnel between them?**

Yes, but the configuration for each tunnel will need to change anytime a WAN IP lease expires. You can make this work temporarily by performing the following steps:

1. Set **0.0.0.0** as the local WAN IP for each gateway.
2. Configure the opposite WS2000 switch's current DHCP address as the Remote Gateway. This is the field that needs to change every time the DHCP addresses change.
3. If using IKE, you cannot use ID type IP for either Local or Remote ID types.

#### **4.6.6.9 I have set up my tunnel and the status still says "Not Connected." What should I do now?**

VPN tunnels are negotiated on an as-needed basis. If you have not sent any traffic between the two subnets, the tunnel will not be established. Once a packet is sent between the two subnets, the VPN tunnel setup will occur.

#### **4.6.6.10 I still can't get my tunnel to work after attempting to initiate traffic between the 2 subnets. What now?**

Here are some troubleshooting tips:

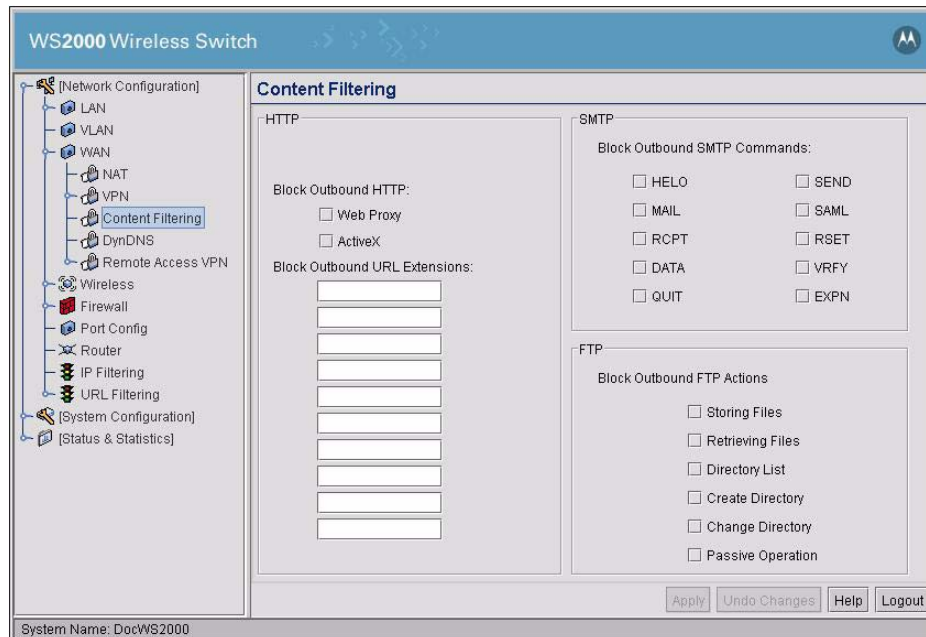
1. Verify that you can ping each of the remote gateway IP addresses from clients on either side. Failed pings can indicate general network connection problems.
2. Pinging the internal gateway address of the remote subnet should run the ping through the tunnel as well. Allowing you to test even if there are no clients on the remote end.
3. Verify that your WAN IP address is not DHCP. VPN requires a static WAN IP address to work.



## 4.7 Configuring Content Filtering

Content filtering allows system administrators to block specific commands and URL extensions from going out through the WS2000 switch's WAN port. This feature allows blocking up to 10 files or URL extensions and allows blocking of specific outbound HTTP, SMTP, and FTP requests.

To configure content filtering, select **Network Configuration** --> **WAN** --> **Content Filtering** from the left menu.



1. Select the type of blocking for outbound HTTP requests. Check one or both of the options:

<b>Web Proxy</b>	This selection blocks the use of web proxies by clients.
<b>ActiveX</b>	This selection blocks all outgoing ActiveX requests by clients.

2. Enter the **Outbound URL** extensions to block. Do this by typing one URL extension or file name (filename.ext) per line. Use an asterisk (\*) as a wildcard in place of the filename to block all files with a specific extension (for example \*.exe).
3. Simple Mail Transport Protocol (SMTP) is the Internet standard for host-to-host mail transport. SMTP generally operates over TCP on port 25. SMTP filtering allows the blocking of any or all outgoing SMTP commands. Choose which SMTP commands to block from the list, by checking those commands to block.

<b>HELO</b>	(Hello) This command is used to identify the SMTP sender to the SMTP receiver.
<b>MAIL</b>	(Mail) This command initiates a mail transaction where mail data is delivered to one or more mailboxes on the local server.
<b>RCPT</b>	(Recipient) This command is used to identify a recipient of mail data.
<b>DATA</b>	(Data) This command tells the SMTP receiver to treat the following information as mail data from the sender.
<b>QUIT</b>	(Quit) This command tells the receiver to respond with an OK reply and then terminate communication with the sender.
<b>SEND</b>	(Send) This command initiates a mail transaction where mail is sent to one or more remote terminals.

<b>SAML</b>	(Send and Mail) This command initiates a mail transaction where mail data is sent to one or more local mailboxes and remote terminals.
<b>RESET</b>	(Reset) This command cancels the current mail transaction and informs the recipient to discard any data sent during this transaction.
<b>VRFY</b>	(Verify) This command asks the receiver to confirm that the specified argument identifies a user. If the argument does identify a user the full name and fully qualified mailbox is returned.
<b>EXPN</b>	(Expand) This command asks the receiver to confirm that a specified argument identifies a mailing list. If the argument does identify a mailing list the membership list of that mailing list is returned.

4. Specify the outbound FTP actions that should get blocked by checking the FTP action to block. File Transfer Protocol (FTP) is the Internet standard for host-to-host file transport. FTP generally operates over TCP on port 21.

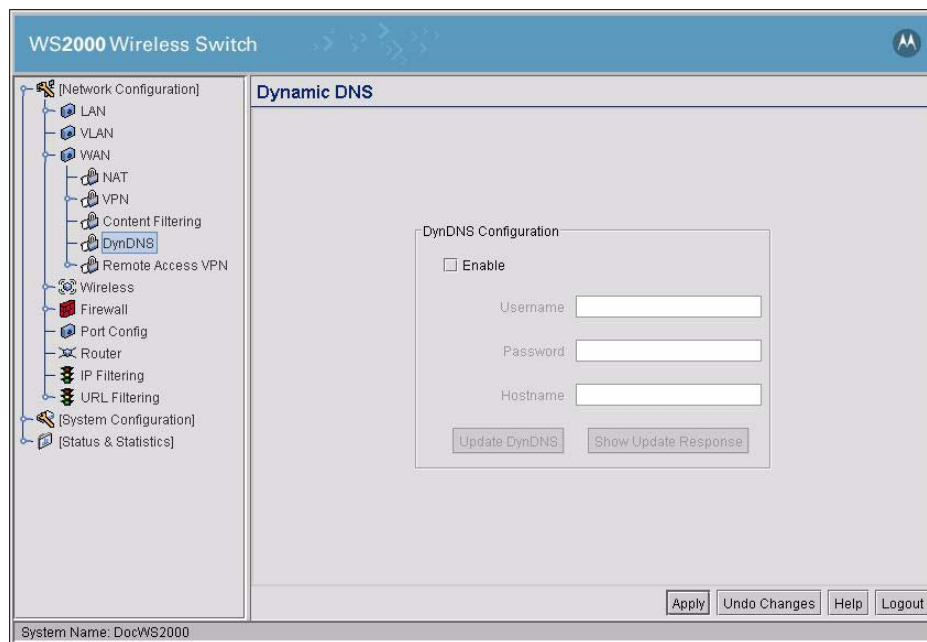
<b>Storing Files</b>	Blocks the request to transfer files sent from the client across the switch's WAN port to the FTP server.
<b>Retrieving Files</b>	Blocks the request to retrieve files sent from the FTP server across the switch's WAN port to the client.
<b>Directory List</b>	Blocks requests to retrieve a directory listing sent from the client across the switch's WAN port to the FTP server.
<b>Create Directory</b>	Blocks requests to create directories sent from the client across the switch's WAN port to the FTP server.
<b>Change Directory</b>	Blocks requests to change directories sent from the client across the switch's WAN port to the FTP server.
<b>Passive Operation</b>	Blocks passive mode FTP requests sent from the client across the switch's WAN port to the FTP server.

5. Click the **Apply** button to save changes made on this screen.

## 4.8 Configuring DynDNS

The WS2000 Wireless Switch provides support for using the DynDNS service. Dynamic DNS is a feature offered by www.dyndns.com which allows the mapping of domain names to dynamically assigned IP addresses. When the dynamically assigned IP address of a client changes that new IP address is sent to the DynDNS servers and traffic for the specified domain(s) is routed to the new IP address.

To view or change the DynDNS settings, select **Network Configuration** --> **WAN** --> **DynDNS** from the left menu.



### 4.8.1 Enabling and Configuring DynDNS

1. Click **Enable** check box to activate DynDNS configuration. Enabling Dyn DNS will allow domain name information to be updated when the IP address associated with that domain changes. In order for changes to go through, a username, password, and hostname must be specified in the fields below.
2. Enter a your DynDNS **Username** for the DynDNS account you wish to use for the WS2000.
3. Enter your **Password** for the DynDNS account you wish to use for the WS2000.
4. Enter your **Hostname** for the DynDNS account you wish to use for the WS2000.
5. Click **Apply** button to save changes.

### 4.8.2 Updating DynDNS

Click the **Update DynDNS** button to update the WS2000's current WAN IP address with the DynDNS service. After you have clicked the **Update DynDNS** button, click the **Show Update Response** button to open a dialogue which displays the hostname, IP address and any messages received during the update from the DynDNS servers.



# 5

## ***Wireless Configuration***

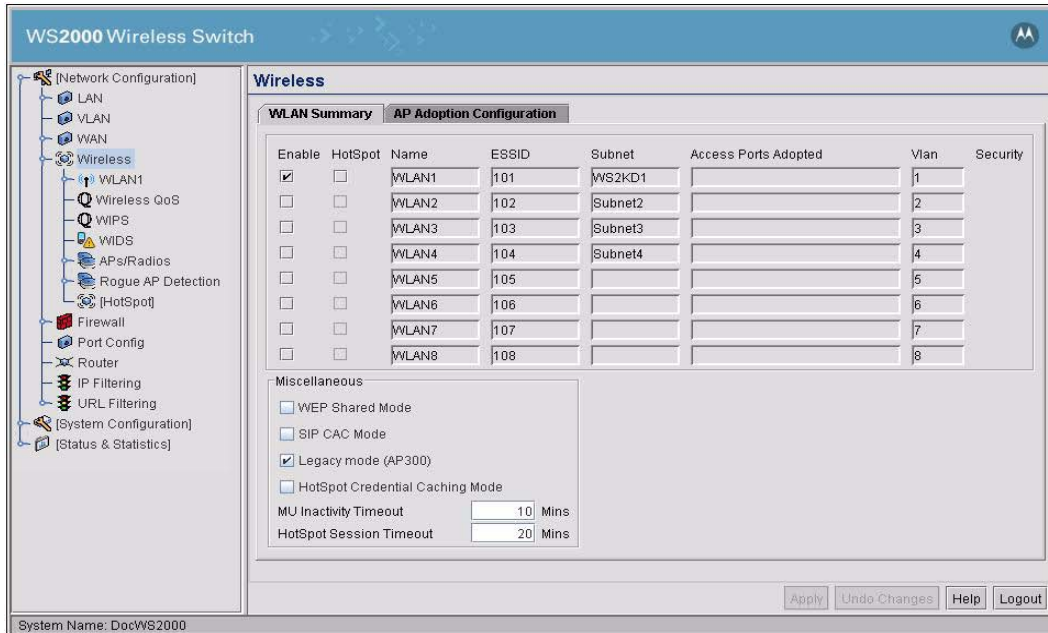
5.1 Enabling Wireless LANs (WLANs) .....	5-3
5.1.1 WLAN Summary .....	5-3
5.1.2 AP Adoption Configuration .....	5-5
5.2 Configuring Wireless LANs .....	5-6
5.2.1 Configuring Advanced WLAN Settings .....	5-6
5.3 Configuring Wireless LAN Security .....	5-7
5.3.1 Selecting the Authentication Method .....	5-7
5.3.2 Configuring 802.1x EAP Authentication .....	5-8
5.3.3 Configuring Kerberos Authentication .....	5-10
5.3.4 Setting the Encryption Method .....	5-11
5.3.5 Configuring WEP Encryption .....	5-11
5.3.6 Configuring WPA/WPA2-TKIP Encryption .....	5-12
5.3.7 Configuring WPA2-CCMP (802.11i) Encryption .....	5-13
5.3.8 KeyGuard .....	5-14
5.3.9 No Encryption .....	5-15
5.3.10 IP Filtering .....	5-15
5.3.11 Mobile Unit Access Control List (ACL) .....	5-16
5.4 Configuring Access Ports .....	5-16
5.5 Setting Default Access Port Settings .....	5-19
5.5.1 Common Settings to All Radio Types .....	5-20
5.5.2 Radio-Specific Settings .....	5-22
5.6 Advanced Access Port Settings .....	5-23
5.6.1 Radio Settings .....	5-24
5.6.2 Antenna Settings .....	5-25
5.6.3 Access Port Properties .....	5-25
5.6.4 Advanced Properties .....	5-25
5.7 Quality of Service Configuration .....	5-27
5.7.1 Setting the Bandwidth Share Mode .....	5-28
5.7.2 Configuring Voice Prioritization and Multicast Address Settings .....	5-29
5.8 Setting Up Port Authentication for AP300 Access Ports .....	5-29
5.9 Rogue Access Point (Port) Detection .....	5-30
5.9.1 Setting Up the Detection Method .....	5-31
5.9.2 Defining and Maintaining Approved AP List Rules .....	5-32
5.9.3 Examine the Approve and Rogue Access Ports .....	5-33
5.9.4 Setting SNMP Traps for Rogue APs .....	5-36
5.10 Configuring Wireless Intrusion Protection System (WIPS) .....	5-37

5.11 Wireless Intrusion Detection System .....	5-38
5.11.1 WIDS Configuration .....	5-39
5.11.2 Filtered MUs .....	5-40
5.12 Smart Scan .....	5-41
5.13 Self Heal .....	5-42
5.14 Mesh Settings .....	5-43
5.14.1 Mesh Base Setting .....	5-44
5.14.2 Mesh Client Setting .....	5-44

## 5.1 Enabling Wireless LANs (WLANs)

The WS2000 Wireless Switch works in either a wired or wireless environment; however, the power of the switch is associated with its support of wireless networks. To use the wireless features of the switch, the administrator needs to enable one, two, or three wireless LANs (WLANs).

To start the WLAN configuration process, select the **Network Configuration** --> **Wireless** item from the left menu. The following Wireless summary screen appears.



### 5.1.1 WLAN Summary

Enable	HotSpot	Name	ESSID	Subnet	Access Ports Adopted	Vlan	Security
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WLAN1	101	Subnet1		1	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN2	102			2	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN3	103	Subnet3		3	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN4	104	Subnet4		4	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN5	105			5	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN6	106			6	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN7	107			7	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN8	108			8	

The top portion of the window displays a summary of the WLANs that are currently defined. This is the screen in which the administrator can enable or disable a WLAN. By default, eight WLANs will be listed WLAN1, WLAN2, WLAN3, WLAN4, WLAN5, WLAN6, WLAN7 and WLAN8. However, only WLAN1 will be enabled.

1. To enable a WLAN, check the check box to the left of the WLAN name. When the administrator enables one of the WLANs, the name of an enabled WLAN shows up as an item on the list of WLANs that reside under **Wireless** menu tree on the left (after clicking the **Apply** button). When an administrator disables a WLAN, it disappears from the menu tree. A WLAN cannot be configured unless it is enabled.
2. To enable a WLAN as a hotspot, check the box marked **Hotspot** next to the WLAN(s) you wish to use as a hotspot. To configure hotspot settings see [Chapter 8, Configuring HotSpot](#).

The screen also displays the following information:

1. By default, the switch assigns consecutive Extended Service Set Identification (ESSIDs). This is the name that users will see when accessing the wireless network. The **ESSID** can be given any recognizable alphanumeric string up to 32 characters in length.
2. The **Subnet** field displays the subnet assigned to the WLAN.
3. The **Access Ports Adopted** field displays the Access Port numbers adopted by this WLAN.

The following configuration for each WLAN can be performed from the **Network Configuration --> Wireless --> <WLANx>** screen.

1. Assign the enabled WLANs descriptive names. The administrator can change the name of any of the WLANs in the **Name** field. This change will affect several other screens and the interface will change the name in the left menu tree.
2. By default, the switch assigns consecutive Extended Service Set Identification (ESSIDs). This is the name that users will see when accessing the wireless network. The **ESSID** can be given any recognizable alphanumeric string up to 32 characters in length.
3. An icon of a lock will appear under the **Security** heading if any wireless encryption or authentication is enabled for the WLAN.

The current settings for the associated Subnet and adopted Access Ports are also displayed on this screen; however, the screen associated with each WLAN (under **Network Configuration --> Wireless**) is where the settings and rules for adopting Access Ports can be modified.

#### 5.1.1.1 WEP Shared Mode

The **WEP Shared Mode** check box enables WEP Shared secret key authentication. IEEE802.11 defines two types of Authentication service: Open System and Shared Key. In Shared Key authentication service prior to Association phase STAs need to authenticate itself using the shared secret key. This authentication scheme is only available if the WEP option is implemented. The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE802.11.

#### 5.1.1.2 SIP CAC Mode

The **SIP CAC Mode** check box enables or disables the SIP Call Admission Control feature which when used in conjunction with compatible VoIP hardware will test for network congestion before allowing VoIP calls to connect. This can help ensure call quality and connection when making VoIP calls.

#### 5.1.1.3 Legacy Mode (AP300)

The **Legacy Mode (AP300)** check box enables AP300s to be adopted in Legacy mode. When this feature is disabled, all AP300s are adopted in the WiAP mode. This feature is only available for AP300s and is enabled by default.

#### 5.1.1.4 HotSpot Credential Caching Mode

The **HotSpot Credential Caching Mode** check box enables the administrator to cache hotspot user credentials on the WS2000. This feature is not enabled by default. The administrator has to explicitly enable this feature.

#### 5.1.1.5 MU Inactivity Timeout

Enter the duration of inactivity after which inactive MUs are disassociated from the WLAN. The default value is 10 minutes.



### 5.1.1.6 Hotspot Inactivity Timeout

Enter the duration of inactivity for a user after which the user is timed out from the hotspot. The default value is 20 minutes and the maximum timeout value is 1440 minutes (1 day).

## 5.1.2 AP Adoption Configuration

The AP Adoption Configuration screen allows for setting up default Access Port adoption rules as well as a deny list to prevent the adoption of specific Access Ports.

### 5.1.2.1 AP Deny List

The **AP Deny List** allows you to prevent individual Access Ports from associating with the switch. For each Access Port you wish to deny, click the **Add** button and enter the device's MAC Address into the field provided.

To add an AP to the **AP Deny List**:

1. Click the **Add** button located below the **AP Deny List** table. A new row will be added to the table.
2. Enter the MAC Address of the Access Port you wish to deny.
3. Click the **Apply** button to save the changes.

### 5.1.2.2 Access Port Radio Adoption List

Use this list to adopt detected Access Ports and to assign them to a particular WLAN. The switch can adopt up to six Access Ports at a time, but the list of allowed Access-Port addresses (displayed in this area) can exceed six in number. A dual-radio 802.11a/b Access Port counts as one Access Port with respect to the maximum allowed; however, each radio will be listed as a separate Access Port.

This adoption list identifies each Access Port by its Media Access Control (MAC) address. This address is the Access Port's hard-coded hardware number that is printed on the bottom of the device. An example of a MAC address is 00:09:5B:45:9B:07.

1. To adopt an Access Port, click the **Add** button to add a new criteria line to the table.
2. Specify the following fields:

Field	Description
<b>Start MAC</b>	This field contains the lowest value in a range of MAC addresses that will use this particular adoption criteria. To specify a single MAC address instead of a range, enter it in this field as well as the <b>End MAC</b> field.
<b>End MAC</b>	This field contains that highest number in a range of MAC addresses that will use this particular adoption criteria. If this value is empty, the Access Port adopted by this criteria must match the <b>Start MAC</b> field exactly.
<b>WLAN columns</b>	The next eight columns are associate with the eight WLANs that are shown in the upper portion of the screen. To the left, specify a range of Access Port MAC address for adoption. Then, click the check boxes of the WLANs that need to adopt the Access Ports in the specified range.



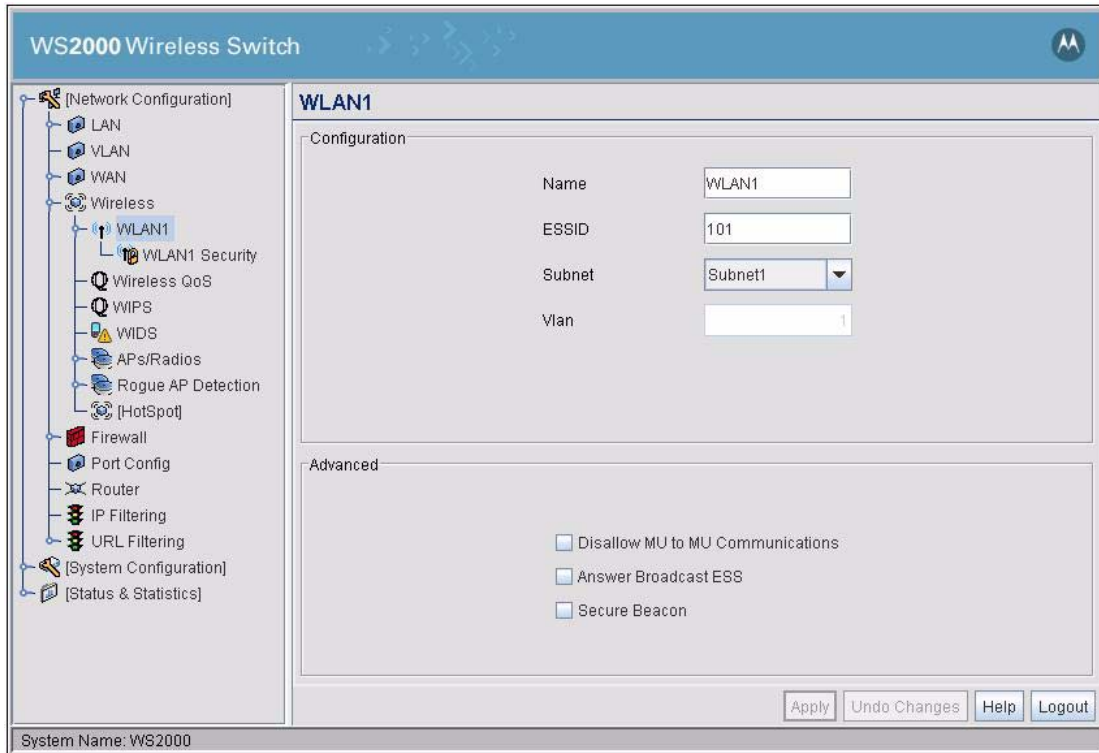
**Note**

**NOTE:** The default setting for the switch has both the Start MAC and End MAC addresses set to "ANY", and all enabled WLANs checked. This setting allows all the WLANs to adopt any Access Port that it detects, automatically.

3. Up to 20 entries can be added to the Access Port Adoption list. Click the **Apply** button to save changes.

## 5.2 Configuring Wireless LANs

The **Network Configuration** --> **Wireless** window (covered in [Enabling Wireless LANs \(WLANs\)](#)) is where WLANs are enabled; however, the **Network Configuration** --> **Wireless** --> <WLAN name> screen is where the administrator configures each WLAN, after it is enabled. The screen is titled with the name of the WLAN.



Within the WLAN window, the administrator can modify both standard and advanced configuration features of the WLAN.

Field	Description
<b>Name</b>	Rename the WLAN in this field, if desired. Character spaces are allowed. This change affects several other screens and the interface will also change the name in the left menu tree. Symbol Technologies recommends the use of descriptive names for WLANs.
<b>ESSID</b>	Specify an Extended Service Set Identification (ESSID) for the WLAN. The ESSID is an alphanumeric string up to 32 characters. Its purpose is to identify one or more Access Ports that are associated with the WLAN.
<b>Subnet</b>	This field provides a pull-down menu of the enabled subnets. Select the subnet to associate with the current WLAN.
<b>VLAN</b>	This is a read-only field which displays the VLAN ID of the VLAN associated with this WLAN. This setting can be changed on the VLAN Configuration screen.

### 5.2.1 Configuring Advanced WLAN Settings

The lower section of the WLAN screen provides several settings that the administrator might need to modify; however, the default settings are usually sufficient for most installations.

1. Check the **Disallow MU to MU Communications** box to enable a communication block between mobile units (MUs) using this WLAN. Such communication might be a security issue, for example, on a corporate network. Leave this check box unchecked (default setting) to allow MU-to-MU communications on this WLAN.
2. Check the **Answer Broadcast ESS** check box to enable adopted Access Ports to transmit the WLAN's Extended Service Set Identification (ESSID). The purpose of allowing WLANs to answer the broadcast ESS is to identify Access Ports that are associated with the WLAN. This might be appropriate, for example, in a customer environment, such as a "hot spot."  
  
Disable this option if broadcasting the WLAN's ESSID poses a security risk, such as with a private, corporate network. The default setting is unchecked.
3. Check the **Secure Beacon** check box to disallow the Access Port from broadcasting its ESSID in its beacons. This is to prevent intruders from becoming members of the WLAN. Use this for a more secure network.
4. Click the **Apply** button to save changes.

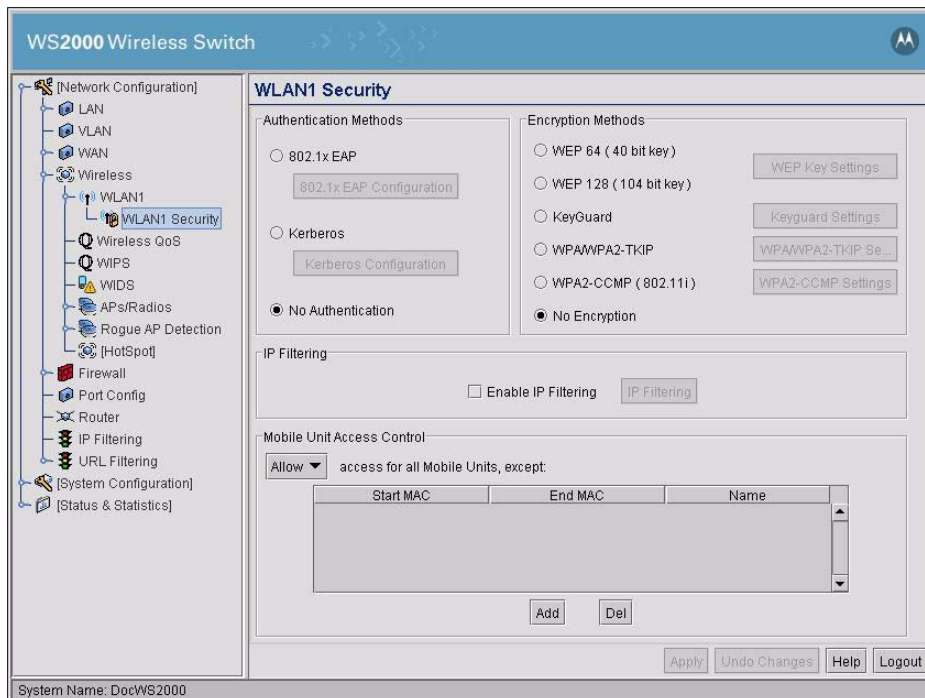
For more advanced WLAN settings see [Quality of Service Configuration](#) or [Configuring Wireless LAN Security](#) later in this chapter.

## 5.3 Configuring Wireless LAN Security

The WS2000 Wireless Switch allows the administrator to set the type and level of security for each WLAN. These security measures do not control communications from the WAN; instead, they control communication from the clients within the WLAN.

In the **Network Configuration --> Wireless --> <WLAN name> --> <WLAN Name> Security** screen, the administrator can set the user authentication method and the encryption method, as well as define a set of rules that control which MUs can communicate through the WLAN.

### 5.3.1 Selecting the Authentication Method



The authentication method sets a challenge-response procedure for validating user credentials such as username, password, and sometimes, secret-key information. The WS2000 Wireless Switch provides two methods for authenticating users: **802.1x EAP** and **Kerberos**. The administrator can select between these two methods. If WLAN security is not an issue, the administrator can decide not to enable authentication (**No Authentication**), because authentication protocols create overhead for the switch's processor.

### 5.3.2 Configuring 802.1x EAP Authentication

The IEEE 802.1x is an authentication standard that ties EAP to both wired and wireless LAN applications. EAP provides effective authentication with or without IEEE 802.1x Wired Equivalent Privacy (WEP) encryption, or with no encryption at all. EAP supports multiple authentication measures. It requires that the site have an authentication (Remote Dial-In User Service, or RADIUS) server on the wired side of the Access Port. All other packet types are blocked until the authentication server verifies the client's identity. To set up 802.1x EAP authentication:

1. On the **Network Configuration** --> **Wireless** --> <WLAN Name> --> <WLAN Name> **Security** screen, select the **802.1x EAP** radio button to enable the 802.1x Extensible Authentication Protocol (EAP). The **802.1x EAP Configuration** button is enabled.
2. Click the **802.1x EAP Configuration** button to display a sub-screen for specific authentication settings.

The screenshot shows the '802.1x EAP Configuration' window. It is divided into several sections:

- Server Settings:**
  - Primary: Radius Server Address (127.0.0.1), Radius Port (1812), Radius Shared Secret (empty), RADIUS client bind interface (NONE).
  - Secondary: Radius Server Address (0.0.0.0), Radius Port (1812), Radius Shared Secret (empty), RADIUS client bind interface (NONE).
  - A 'Use Local Radius' button is located between the shared secret fields.
- Reauthentication:**
  - Enable Reauthentication
  - Period: 3600 (30-9999) secs
  - Max. Retries: 2 (1-99) retries
- Advanced Settings:**
  - MU Quiet Period: 10 (1-65535) secs
  - MU Tx Period: 5 (1-65535) secs
  - Server Timeout: 5 (1-255) secs
  - MU Timeout: 10 (1-255) secs
  - MU Max Retries: 2 (1-10) retries
  - Server Max Retries: 2 (1-255) retries
- Radius Client Accounting:**
  - Enable Accounting (Save to CF Card)
  - Enable Syslog
  - MU Timeout: 10 (1-255) sec
  - Retries: 2 (1-10) retries
  - Syslog Server IP: 0.0.0.0

Buttons: Ok, Cancel, Help

- The administrator is required to specify the **RADIUS Server Address** of a primary RADIUS server for this type of authentication to work. Providing the IP address of a secondary server is optional. The secondary server acts as a failover server if the switch cannot successfully contact the primary server.
- Specify the port on which the primary RADIUS server is listening in the **RADIUS Port** field. Optionally, specify the port of a secondary (failover) server. Older RADIUS servers listen on ports 1645 and 1646. Newer servers listen on ports 1812 and 1813. Port 1645 or 1812 is used for authentication. Port 1646 or 1813 is used for accounting. The ISP or a network administrator can confirm the appropriate primary and secondary port numbers.
- The administrator can specify a **RADIUS Shared Secret** for authentication on the primary RADIUS server. Shared secrets are used to verify that RADIUS messages (with the exception of the Access-Request message) are sent by a RADIUS-enabled device that is 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.
- To use the local RADIUS server as the primary server, click the **Use Local Radius** button.
- Specify the interface to bind the RADIUS client to. Select the interface to bind the RADIUS client from the drop down list under each authentication server. With this feature, it is now possible to authenticate a wireless (802.1x authentication) user with a RADIUS server through a VPN tunnel.

If the RADIUS server is on a network accessible through a VPN tunnel, then the tunnel must be configured. The bind interface should be the same as the Local Subnet configured for the VPN tunnel.

### **Reauthentication Settings**

- Check the **Enable Reauthentication** check box to enable this authentication method.
- In the **Period** field, set the EAP reauthentication period to match the appropriate level of security. A shorter time interval (~30 seconds or longer) provides tighter security on this WLAN's wireless connections. A longer interval (5000-9999 seconds) relaxes security on wireless connections. The reauthentication period setting does not affect a wireless connection's throughput. The engaged Access Port continues to forward traffic during the reauthentication process.

10. In the **Max. Retries** field, set the maximum number of retries for a client to successfully reauthenticate after failing to complete the EAP process. If the mobile unit fails the authentication process in specified number of retries, the switch will terminate the connection to the mobile unit.

### **Advanced Settings**

11. The **MU Quiet Period** field allows the administrator to specify the idle time (in seconds) between a mobile unit's authentication attempts, as required by the server.
12. The **MU Timeout** field allows the administrator to specify the time (in seconds) for the mobile unit's retransmission of EAP-Request packets.
13. The **MU Tx Period** field allows the administrator to specify the time period (in seconds) for the server's retransmission of the EAP-Request/Identity frame.
14. The **MU Max Retries** field allows the administrator to set the maximum number of times for the mobile unit to retransmit an EAP-Request frame to the server before it times out the authentication session. Note that this is a different value from the Max Retry field at the top of the window.
15. The **Server Timeout** field indicates the maximum time (in seconds) that the switch will wait for the server's transmission of EAP Transmit packets.
16. The **Server Max Retries** field allows the administrator to set the maximum number of times for the server to retransmit an EAP-Request frame to the client before it times out the authentication session. Note that this is a different value from the **Max. Retries** field at the top of the window.



**NOTE:** When changing the **Server Max Retries** setting to anything other than the default value, there is a known bug that can cause RADIUS authentication to fail.

#### **Note**

### **RADIUS Client Accounting and Syslog Setup**

17. Use the **Enable Accounting** check box to enable saving the RADIUS logs on the device's Compact Flash (CF) card.
18. If accounting is enabled, enter the maximum amount of time a client will wait for an acknowledgement from the RADIUS accounting server before resending the accounting packet in the **MU Timeout** field. In the **Retries** field, enter the maximum number of times for the client will resend the accounting packet to the RADIUS accounting server before giving up.
19. To enable 802.1x EAP message logging to an external Syslog server, check the **Enable Syslog** box and then specify the IP address of the syslog server in the **Syslog Server IP** field.
20. Click the **Ok** button to save changes.

### **5.3.3 Configuring Kerberos Authentication**

Kerberos provides a strong authentication method for client/server applications by using secret-key cryptography. Using this protocol, a client can prove their identity to a server (and vice versa) across an insecure network connection. After a client and server use Kerberos to prove their identity, they can encrypt all communications to assure privacy and data integrity.

1. Select the **Kerberos** radio button to enable Kerberos authentication.
2. Click the **Kerberos Configuration** button to display a sub-screen for authentication settings.

The screenshot shows a Java Applet window titled "Kerberos Configuration". The window has a blue header bar with the title and a close button. Below the header, there is a logo on the left and the title "Kerberos Configuration". The main area contains several input fields: "Realm Name" (a text box), "Username" (a text box), "Password" (a text box), "Server IP" (a text box), "Port" (a text box), "Primary KDC" (a text box), "Backup KDC" (a text box), and "Remote KDC" (a text box). The IP address fields are pre-filled with "0 . 0 . 0 . 0". The port fields are pre-filled with "88". At the bottom right, there are three buttons: "Ok", "Cancel", and "Help". The window title bar also includes "Java Applet Window".

3. A realm name functions similar to a DNS domain name. In theory, the realm name is arbitrary; however, in practice, a Kerberos realm is typically named using an uppercase version of the DNS domain name that is associated with hosts in the realm. Specify a realm name that is case-sensitive, for example, *MyCompany.com*.
4. Specify a **Username** for the Kerberos configuration.
5. Specify a **Password** for the Kerberos configuration.  
The *Key Distribution Center* (KDC) implements an authentication service and a ticket granting service, whereby an authorized user is granted a ticket that is encrypted with the user's password. The KDC has a copy of every user password.
6. Specify a server IP address and a port to be used as the **Primary KDC**.
7. Optionally, specify a **Backup KDC** server by providing the IP address and port.
8. Optionally, specify a **Remote KDC** server by providing the IP address and port.
9. Make sure that NTP is enabled (go to **System Configuration** --> **NTP Servers** from the left menu). NTP is required for Kerberos Authentication. For more information, see [Specifying a Network Time Protocol \(NTP\) Server](#).
10. Click **Ok** when done.

### 5.3.4 Setting the Encryption Method

Encryption applies a specific algorithm to data to alter its appearance and prevent unauthorized reading. Decryption applies the algorithm in reverse to restore the data to its original form. Sender and receiver employ the same encryption/decryption method.

The WS2000 Wireless Switch provides four methods for data encryption: WEP, KeyGuard, WPA-TKIP, and WPA2-CCMP (802.11i). The WPA-TKIP and KeyGuard methods use WEP 104-bit key encryption. WPA-TKIP offers the highest level of security among the encryption methods available with the switch.

The available encryption methods also depend on the authentication method used. Kerberos authentication supports only the **WEP 128 (104 bit key)** and **KeyGuard** encryption methods.

### 5.3.5 Configuring WEP Encryption

*Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi-Fi) standard, 802.11b. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. WEP might 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. Key changes require the manual re-configuration of each Access Port. An unauthorized person with a sniffing tool can monitor a network for less than a day and decode its encrypted messages.



WEP is available in two encryption modes: 40 bit (also called 64-bit) and 104 bit (also called 128 bit). The 104-bit encryption mode provides a longer algorithm that takes longer to decode than that of the 40-bit encryption mode.



**Note**

**NOTE:** The WEP 128 encryption mode allows devices using 104-bit key and devices using 40-bit keys to talk to each other using 40-bit keys, if the 104-bit devices permit this option.

1. Choose between the **WEP 64 (40-bit key)** and **WEP 128 (104-bit key)** option by selecting the appropriate radio button.
2. To use WEP encryption with the **No Authentication** selection, click the **WEP Key Settings** button to display a sub-screen for entering keys.

3. When finished, click the **Ok** button to close this screen.
4. Specify a **Pass Key** and click the **Generate** button. The pass key can be any alphanumeric string. The switch, other proprietary routers, and Symbol cards in mobile units (MUs) use an algorithm to convert an ASCII string to the same hexadecimal number, but this conversion is not required for a wireless connection.
5. Use the **Key #1-4** fields to specify key numbers that use 26 hexadecimal characters. Select one of these keys for active use by selecting its radio button. Four different keys can be specified, allowing each WLAN to have a different key.
6. Click the **Apply** button on the WLAN Security screen to save changes.

### 5.3.6 Configuring WPA/WPA2-TKIP Encryption

Wi-Fi Protected Access (WPA) is specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i. This security standard 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 weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check, and an extended initialization vector. WPA/WPA2 also provides strong user authentication that is based on 802.1x EAP.

1. Select the **WPA/WPA2-TKIP** radio button to enable Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP).



- To use WPA/WPA2-TKIP encryption with **802.1x EAP authentication** or the **No Authentication** selection, click the **WPA/WPA2-TKIP Settings** button to display a sub-screen for key and key rotation settings.

- To Enable WPA2 check the **Use WPA2** check box to use WPA2 encryption in conjunction with WPA-TKIP.
- If using WPA2 in conjunction with 802.1x EAP authentication you may enable **Pre-Authentication** and **Opportunistic Key Caching** by checking the corresponding check boxes.
- Check the **Broadcast Key Rotation** check box to enable or disable the broadcasting of encryption-key changes to mobile units.
- Specify a time period in seconds for broadcasting encryption-key changes to mobile units. Set key broadcasts to a shorter time interval (at least 300 seconds) for tighter security on this WLAN's wireless connections. Set key broadcasts to a longer time interval (at most, 80,000 seconds) to relax security on wireless connections.

A Pre-Shared Key (PSK) is an Internet Protocol security (IPSec) technology that uses a shared, secret key for authentication in IPSec policy. IPSec is a set of industry-standard, cryptography-based protection services and protocols. IPSec protects all protocols in the TCP/IP protocol suite and Internet communications by using Layer Two Tunneling Protocol (L2TP). Use pre-shared key authentication only in a WLAN environment intended for relaxed security. The administrator can specify the key either as an ASCII passphrase or as a 128-bit key. All WLAN clients must use the same PSK.

- Select either the **ASCII Passphrase** or **256-bit Key** radio button.
- If **ASCII Passphrase** is selected, specify a 8 to 63 character alphanumeric string. The alphanumeric string allows character spaces. The switch converts the string to a numeric value.
- To use the **256-bit Key** option, enter 16 hexadecimal characters into each of the four fields.
- Click the **Ok** button to return to the WLAN security screen.
- Click the **Apply** button on the WLAN Security screen to save changes.

### 5.3.7 Configuring WPA2-CCMP (802.11i) Encryption

WPA2 is a newer 802.11i standard that provides stronger wireless security than WiFi Protected Access (WPA) and WEP.

CCMP is the security protocol used by AES. It is the equivalent of TKIP in WPA. CCMP computes a Message Integrity Check (MIC) using the well known, and proven, Cipher Block Chaining Message Authentication Code

(CBC-MAC) method. Changing even one bit in a message produces a totally different result thus providing strong authentication.

WPA2-CCMP is based upon the concept of a robust security network (RSN), which defines a hierarchy of keys that have a limited lifetime, similar to TKIP. Also like TKIP, the keys that 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 encryption that is extremely secure.

1. Select the **WPA2-CCMP** radio button to enable Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP).
2. To use WPA-TKIP encryption with **802.1x EAP authentication** or the **No Authentication** selection, click the **WPA-TKIP Settings** button to display a sub-screen for key and key rotation settings.

3. Check the **Broadcast Key Rotation** check box to enable or disable the broadcasting of encryption-key changes to mobile units.
4. Specify a time period in seconds for broadcasting encryption-key changes to mobile units. Set key broadcasts to a shorter time interval (at least 300 seconds) for tighter security on this WLAN's wireless connections. Set key broadcasts to a longer time interval (at most, 200,000 seconds) to relax security on wireless connections.
5. Select either the **ASCII Passphrase** or the **256-bit Key** radio button.
6. If **ASCII Passphrase** is selected, specify a 8 to 63 character ASCII string. The ASCII string allows character spaces. The switch converts the string to a numeric value.
7. To use the **256-bit Key** option, enter 16 hexadecimal characters into each of four fields.
8. **WPA2-CCMP Mixed Mode** enables WPA2-CCMP and WPA-TKIP Clients to operate simultaneously on the network. Enabling this option allows backwards compatibility for clients that support WPA-TKIP but do not support WPA2-CCMP.
9. The **Fast Roaming** area provides two fields. Enabling **Pre-Authentication** enables a client associated with one Access Port to carry out an 802.1x authentication with another Access Port before it roams over to it. The WS2000 switch will cache the keying information of the client until it roams to the new Access Port. This enables the roaming the client to start sending and receiving data sooner by not having to do 802.1x authentication after it roams. Enabling **Opportunistic Key Caching** allows the switch to use a Pairwise Master Key (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.

10. Click the **Ok** button to return to the WLAN security screen.
11. Click the **Apply** button on the WLAN Security screen to save changes.

### 5.3.8 KeyGuard

KeyGuard is a proprietary encryption method developed by Symbol Technologies. KeyGuard is Symbol's enhancement to WEP encryption and can work with any WEP device. This encryption method rotates WEP keys for devices that support the method. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

1. Select the **KeyGuard** radio button to enable the KeyGuard encryption method.
2. To use KeyGuard encryption with the No Authentication selection, click the **MCM Key Settings** button to display a sub-screen for entering keys. (Note that these are the same keys specified for WEP encryption.)

3. Select a **Key #** radio button to enter or change a passkey.
4. Specify a pass key string in the **Pass Key** field. The pass key can be any alphanumeric string. The switch, other proprietary routers, and Symbol cards in mobile units (MUs) use an algorithm to convert an ASCII string to the same hexadecimal number, but this conversion is not required for a wireless connection.
5. Click the **Generate** button and the pass key will be entered in the appropriate Key # field.
6. When finished entering pass keys, click the **Ok** button to close this screen.
7. Click the **Apply** button on the WLAN Security screen to save changes.

### 5.3.9 No Encryption

If **No Authentication** is selected, the **No Encryption** radio button can disable encryption on this WLAN. If security is not an issue, this setting avoids the overhead that an encryption protocol demands on the switch's processor.

### 5.3.10 IP Filtering

IP based filtering allows administrators to configure Incoming and Outgoing IP filtering policies on packets within the same Subnet / WLAN and between wired and wireless hosts.



To Configure IP Filtering for the WLAN:

1. Check the box marked **Enable IP Filtering** to turn on IP Address based filtering for inbound and outbound traffic on the WLAN.
2. Click the **IP Filtering** button to display a sub-screen for filtering settings on the WLAN.
3. Click the **Add** button to create a new filter in the table. The new filter can then be edited by clicking on the corresponding fields in the table.
4. Click the **Filter Name** and provide a name or edit an existing name for the filter. The **Filter Name** should be unique for each filter rule that is added.
5. Click the **Direction** field for the corresponding filter to specify if the filter applies to traffic Inbound or Outbound on the WLAN. 'Incoming' traffic refers to traffic coming from an MU to the AP. 'Outgoing' traffic refers to the traffic going from the AP to an MU.
6. Click the **Action** field for the corresponding filter to specify if the filter will be set to Allow or Deny traffic in the chosen direction. 'Allow' will enable traffic to pass freely in the specified direction between the APs and MUs. 'Deny' will prevent traffic from passing in the specified direction between the APs and MUs.
7. Check the **Default Inbound Deny** box to prevent traffic inbound on the WLAN from passing freely from the MUs to the APs.
8. Check the **Default Outbound Deny** box to prevent traffic outbound on the WLAN from passing freely from the APs to the MUs.
9. Click the **OK** button to return to the WLAN Security screen.
10. Click the **Apply** button the WLAN Security screen to commit the changes to the system.

### 5.3.11 Mobile Unit Access Control List (ACL)

Use this list to specify which mobile units can or cannot gain access to the WLAN. The list employs an adoption rule for allowing or denying specific mobile units by way of exception.

1. Select **Allow** or **Deny** from the pull-down menu. This rule applies to all mobile units except those listed in the table. If Allow is visible, the access criteria (MAC addresses) will be used to indicated which mobile units will be allowed access to the Access Port. If **Deny** is visible, the access criteria will be used to indicated which mobile units should not be allowed access.
2. Click the **Add** button to add a new entry to the list.

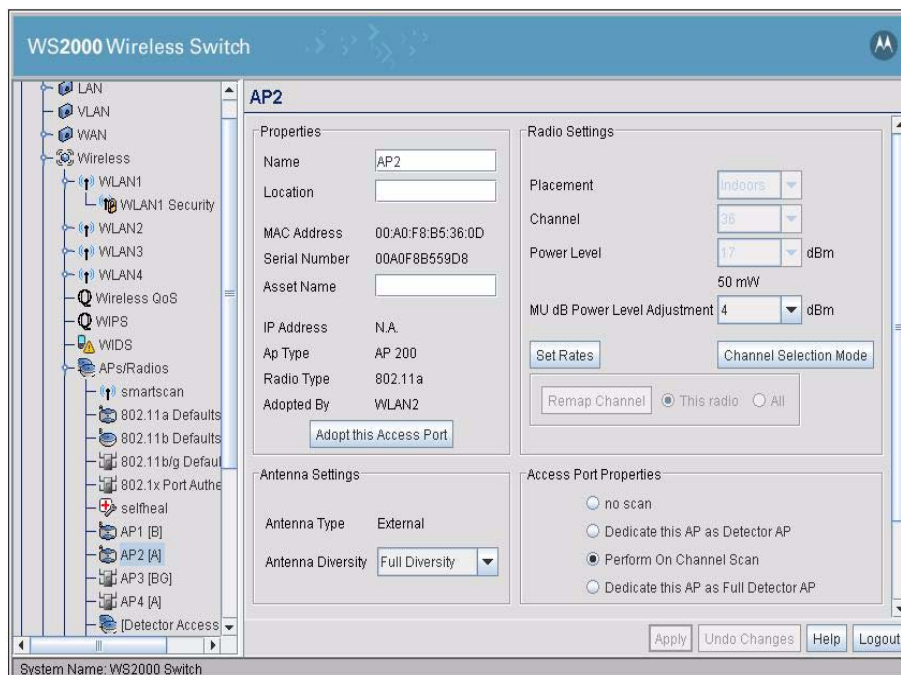
- Each entry in the table specifies one or more MAC address to be used to match with a mobile unit's MAC address that is attempting to gain access to the WLAN. Specify a single address (by specifying **Start Address** only) or a range of MAC access (by using both the **Start Address** and the **End Address**).

For example, if **Allow** is selected, all mobile units that match any of the specified MAC addresses or MAC address ranges in the table can be adopted by the WLAN. If Deny is selected, all mobile units that match any of the specified MAC addresses or MAC address ranges in the table cannot be adopted by the WLAN.

- Click the **Apply** button to save changes.

## 5.4 Configuring Access Ports

The WS2000 Wireless Switch automatically detects Access Ports when they are attached to one of the switch's LAN ports. When the switch starts communication with an Access Port that can be adopted by the switch, it uploads the firmware appropriate for the Access Port. At this time, the Access Port becomes active. The switch also automatically adds the Access Port to the list of known ports under the left menu item, **Network Configuration --> Wireless --> Access Ports--> <Access Port Name>**.



For an Access Port to be adopted by the WS2000 Wireless Switch, three things must be configured:

- The **Country** field in the System Settings screen must be set.
- The Access Port's **MAC Address** must be set as one of the addresses that can be adopted by one of the enabled WLANs.
- A WLAN that can adopt Access Port must be associated with an enabled subnet. (See [Configuring Wireless LANs](#).)

The switch can adopt up to six Access Ports at a time, but the number of Access Ports listed can exceed six in number. A dual-radio 802.11a/b Access Port counts as one Access Port with respect to the maximum allowed; however, each radio will be listed as a separate Access Port in the list of Access Ports.

The switch creates a default name for a newly found switch consisting of “AP” and a unique number. During this detection process, the switch collects the following information from the Access Port:

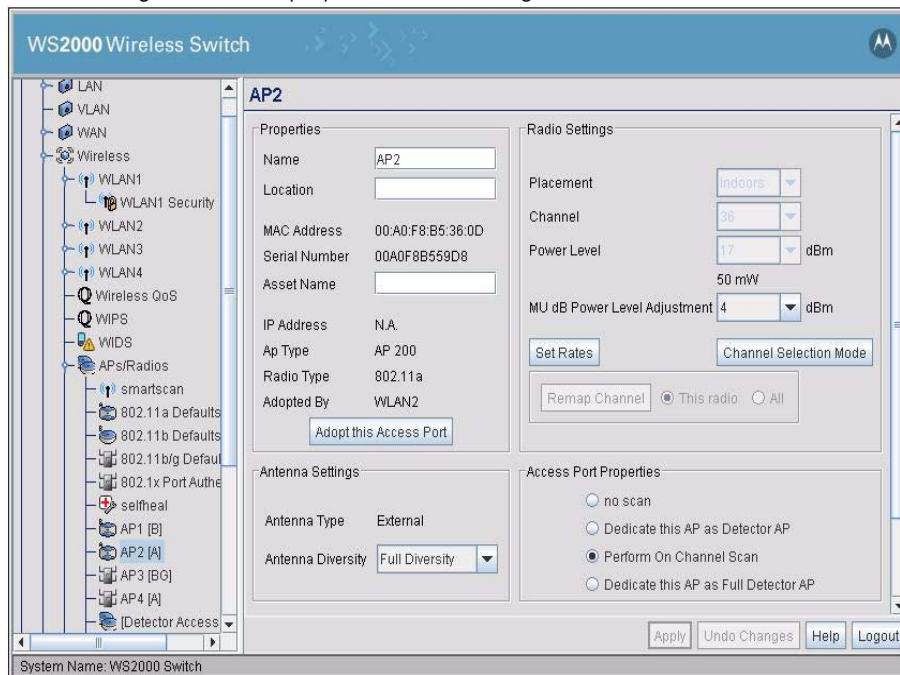
<b>MAC address</b>	Each Access Port has a unique Media Access Control (MAC) address by which it is identified. This address is burned into the ROM of the Access Port. Also, this address appears on a sticker attached to the bottom of the Access Port.
<b>Serial Number</b>	Each Access Port has a unique serial number printed on the device at the time of manufacturing. This address is burned into the ROM of the Access Port.
<b>AP Type</b>	This field lists the model number of the Access Port (i.e. AP100, AP300)
<b>Radio type</b>	This field indicates the wireless protocol that the Access Port follows. The WS2000 Wireless Switch supports 802.11b and 802.11 a/b dual-radio Access Ports.
<b>Adopted by</b>	This field contains a list of defined WLANs that have adopted this Access Port (see <a href="#">Configuring Wireless LANs and Access Port Radio Adoption List</a> for the process of adopting an Access Port).

The switch also sets several default values for the channel and the power level based upon the Location information set in the System Settings screen and upon settings in the [Access Port Default Settings](#) screen for the radio type.

The WS2000 Wireless Switch GUI also allows the administrator to refine the basic Access Port configuration that is set at the point of detection. To examine or change that information:

1. Select **Network Configuration** --> **Wireless** --> **Access Ports** from the left menu and then click the **+** to the left of the menu item. The detected Access Ports will be listed under the menu item, with the radio type listed in brackets (for example, [B]).
2. Select the Access Port item to examine or modify. There are two ways to distinguish between Access Ports when they are labeled with the default “AP#” name.
  - Look on the bottom of the Access Ports and take note of the MAC address (which looks like AA:BB:CC:DD EE:FF) and compare it with the MAC address in the Access Port windows.
  - Note the order in which Access Ports were plugged into the switch. The Access Port numbers are assigned in order, starting with AP1. When an Access Port has multiple radios, each radio is assigned an AP number.

The following screen is displayed with the settings for the selected Access Port.



3. From this screen, the administrator can change several pieces of information about each Access Port.

<b>Name</b>	Administrators can change the names of the Access Ports from Access Port# to something much more descriptive, so that they can easily identify which Access Port is being referenced in the various screens and in the left menu. The name is limited to a string of 13 characters.
<b>Location</b>	This field is a memory aid for the administrator. Enter text that describes where the Access Port is physically located. The name is limited to a string of 13 characters.
<b>Asset Name</b>	This field is also a memory aid for keeping track of the organizational asset; Enter any value that uniquely identifies this asset.
<b>Adopt this Access Port</b>	This button opens a dialogue box which allows you to adopt an Access Port into one or more WLANs.

4. In the **Radio Settings** area, the administrator can specify a number of characteristics of the radio.

<b>Placement</b>	Select either <b>Indoors</b> or <b>Outdoors</b> from the Placement pop-up menu. The setting will affect the selection available for several of the other advanced settings.
<b>Channel</b>	Specify a channel for communications between the Access Port and mobile units. The range of legally approved communications channels varies depending on the installation location. It is best to use a different channel number for each Access Port. Communications will be the clearest for nearby Access Ports if the channel numbers are 5 numbers apart (1, 6, 11).
<b>Power Level</b>	Specify a <b>Power Level</b> in milliwatts (mW) for RF signal strength. The optimal power level is best determined by a site survey prior to installation. Available settings include 1, 5, 15, 30, and 100. Consult the site survey for recommendations of the power level.  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 mobile units. Decrease the power level according to the proximity of other Access Ports. Overlapping RF coverage may cause lost packets and difficulty for roaming mobile units trying to engage an Access Port.



<b>MU dB Power Level Adjustment</b>	This is a Motorola specific feature. This value indicates the amount of power in dBm that the MU should reduce its Tx power by with respect to the Tx power of the AP. This feature is used to reduce the amount of radio noise in the environment for better reception.
-------------------------------------	--

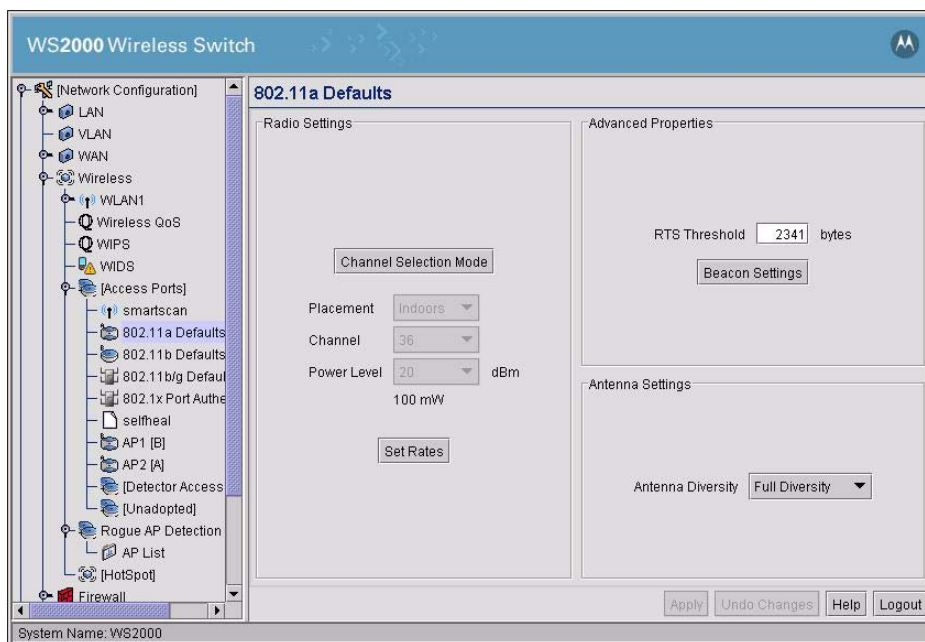
5. Click **Apply** to save changes.

This screen also provides the ability to change several advanced settings for the Access Ports. For more information, see [Advanced Access Port Settings](#).

## 5.5 Setting Default Access Port Settings

The WS2000 Network Switch can support up to six Access Port. These Access Ports can be either a 802.11a or 802.11b radio type. When an Access Port associates with the wireless switch, the initial settings for that Access Port are taken from the Default Access Port Setting for the appropriate radio type. Select **Network Configuration** --> **Wireless** --> **Access Ports** to see the list of Default radio settings. Then select the Default settings screen for the appropriate radio type: one of **802.11a Defaults**, **802.11b Defaults**, or **802.11b/g Defaults**.




This screen is the 802.11a Defaults screen.





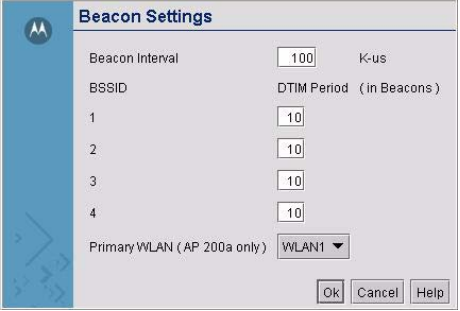


## 5.5.1 Common Settings to All Radio Types

Some of the settings are common to all three radio types.


<p><b>Channel Selection Mode</b></p>	<p>Click the <b>Channel Selection Mode</b> button to configure how channel selection for the selected AP is determined. A window will open with the following selections:</p> <p><b>User Selection</b></p> <p>Select this radio button to enable manual channel selection. With this mode, channel can be selected from a drop down list in the parent window.</p> <p><b>Uniform Spreading (AP300 Only)</b></p> <p>Select this radio button to enable the Uniform Spreading feature of the AP300. To comply with Dynamic Frequency Selection (DFS) requirements in the European Union, the 802.11a radio on AP300 Access Ports will come up on a random channel each time it is powered on.</p> <p> <b>NOTE:</b> With this mode, channel can not be manually selected.</p> <p><b>Note</b></p> <p><b>Automatic Mode (Automatic Channel Selection)</b></p> <p>Select this radio button to enable Automatic Channel Selection (ACS) feature of WS2000/ AP300. With this mode, the AP will scan the available channels and select the one in which least number of beacons is heard.</p> <p> <b>NOTE:</b> With this mode, channel can not be manually selected.</p> <p><b>Note</b></p>
<p><b>Placement</b></p>	<p>Select either <b>Indoors</b> or <b>Outdoors</b> from the Placement pop-up menu. This setting will affect the power levels and channels available for selection.</p>
<p><b>Channel</b></p>	<p>Select a channel number from the <b>Channel</b> drop-down menu on which the Access Port should communicate with associated MUs.</p> <p> <b>NOTE:</b> The available channels vary depending on the location setting of the switch.</p> <p><b>Note</b></p>
<p><b>Power Level</b></p>	<p>Select a power level from the <b>Power Level</b> drop-down menu that will be used for radio communications between the Access Port and the MUs.</p> <p>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 mobile units (MUs). Decrease the power level according to the proximity of other Access Ports. Overlapping RF coverage may cause lost packets and difficulty for roaming MUs trying to engage an Access Port.</p>

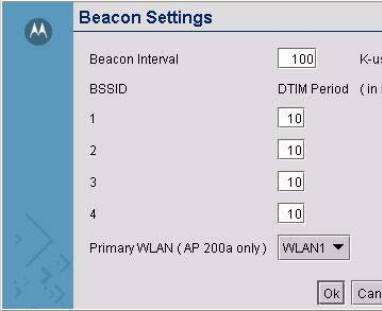
<p><b>Antenna Diversity</b></p>	<p>Use the drop-down menu to configure the Antenna Diversity settings for Access Ports that use external antennas.</p> <p><b>Full Diversity:</b> Utilizes both antennas to provide antenna diversity</p> <p><b>Primary Only:</b> Enables only the primary antenna</p> <p><b>Secondary Only:</b> Enables only the secondary antenna</p> <p> <b>NOTE:</b> Antenna Diversity should only be enabled if the Access Port has two matching external antennas.</p> <p><b>Note</b></p>																		
<p><b>RTS Threshold</b></p>	<p>Set the Request to <b>Send Threshold (RTS Threshold)</b> by specifying a number.</p> <p>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 when many mobile units (MUs) are contending for transmission time. Modifying this value allows the administrator to control the number of data collisions and thereby enhance communication with nodes that are hard to find because of other active nodes in the transmission path.</p> <p>In this field, the administrator can specify a Request To Send (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports.</p> <p>This setting initiates an RTS/CTS exchange for data frames that are larger than the threshold, and sends (without RTS/CTS) any data frames that are smaller than the threshold.</p> <p>Consider the tradeoffs 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.</p> <p>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.</p>																		
<p><b>Set Rates</b></p>	<p>Click the <b>Set Rates</b> button to open a sub-screen where the default <b>Basic Rates</b> and <b>Supported Rates</b> for 802.11b/g Access Ports can be set.</p> <p>A list of available Basic and Supported rates for the radio are listed in two columns with check boxes next to each rate. Selecting a rate as a Basic Rate automatically selects that rate as a Supported Rate and disables the option in the Supported Rates column.</p> <div data-bbox="971 1266 1414 1633" style="border: 1px solid gray; padding: 5px;">  <p><b>Set Rates</b></p> <table border="0"> <thead> <tr> <th>Basic Rates:</th> <th>Supported Rates:</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> 6</td> <td><input checked="" type="checkbox"/> 6</td> </tr> <tr> <td><input type="checkbox"/> 9</td> <td><input checked="" type="checkbox"/> 9</td> </tr> <tr> <td><input checked="" type="checkbox"/> 12</td> <td><input checked="" type="checkbox"/> 12</td> </tr> <tr> <td><input type="checkbox"/> 18</td> <td><input checked="" type="checkbox"/> 18</td> </tr> <tr> <td><input checked="" type="checkbox"/> 24</td> <td><input checked="" type="checkbox"/> 24</td> </tr> <tr> <td><input type="checkbox"/> 36</td> <td><input checked="" type="checkbox"/> 36</td> </tr> <tr> <td><input type="checkbox"/> 48</td> <td><input checked="" type="checkbox"/> 48</td> </tr> <tr> <td><input type="checkbox"/> 54</td> <td><input checked="" type="checkbox"/> 54</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Ok"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> </p> </div>	Basic Rates:	Supported Rates:	<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 6	<input type="checkbox"/> 9	<input checked="" type="checkbox"/> 9	<input checked="" type="checkbox"/> 12	<input checked="" type="checkbox"/> 12	<input type="checkbox"/> 18	<input checked="" type="checkbox"/> 18	<input checked="" type="checkbox"/> 24	<input checked="" type="checkbox"/> 24	<input type="checkbox"/> 36	<input checked="" type="checkbox"/> 36	<input type="checkbox"/> 48	<input checked="" type="checkbox"/> 48	<input type="checkbox"/> 54	<input checked="" type="checkbox"/> 54
Basic Rates:	Supported Rates:																		
<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 6																		
<input type="checkbox"/> 9	<input checked="" type="checkbox"/> 9																		
<input checked="" type="checkbox"/> 12	<input checked="" type="checkbox"/> 12																		
<input type="checkbox"/> 18	<input checked="" type="checkbox"/> 18																		
<input checked="" type="checkbox"/> 24	<input checked="" type="checkbox"/> 24																		
<input type="checkbox"/> 36	<input checked="" type="checkbox"/> 36																		
<input type="checkbox"/> 48	<input checked="" type="checkbox"/> 48																		
<input type="checkbox"/> 54	<input checked="" type="checkbox"/> 54																		

<p><b>Beacon Settings</b></p>	<p>Set the Access Port beacon settings by clicking on the <b>Beacon Settings</b> button.</p> <p>Set the following beacon values.</p> <p><b>Beacon Interval</b>—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 access-port address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM.</p> <p>Specify a beacon interval in units of 1,000 microseconds (K-us). This is a multiple of the DTIM value, for example, 100 : 10. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decreasing this value (shorten the time) to support streaming-multicast audio and video applications that are jitter-sensitive.</p>	
	<p><b>DTIM Period</b>—A DTIM is periodically included in the beacon frame that is 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 acknowledgment, so nodes sometimes miss them.</p> <p>In this field, the administrator can specify a period for the Delivery Traffic Indication Message (DTIM). This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.</p>	
	<p><b>Primary WLAN</b>—Select the primary WLAN when the 802.11a broadcast protocol is used. When a WLAN is associated with a 801.11a broadcaster, only one ESSID can be broadcast from the Access Port (even though three are supported by the switch). This field specifies which ESSID to broadcast.</p>	
	<p><b>Security Beacon</b>—Check the <b>Security Beacon</b> box if the WLAN associated with the Access Port needs to be secure. If this feature is selected, the WLAN will not broadcast the ESSID. This selection eliminates the possibility of hackers tapping in to the WLAN without authorization by “stealing” the ESSID.</p>	

## 5.5.2 Radio-Specific Settings

The fields below are only available for some radio types, as indicated in the second column.

<p><b>Uniform Spreading (AP300 only)</b></p>	<p>a</p>	<p>Check this check box to enable the Uniform Spreading feature of the AP300. To comply with Dynamic Frequency Selection (DFS) requirements in the European Union, the 802.11a radio on AP300 Access Ports will come up on a random channel each time it is powered on.</p> <p> <b>NOTE:</b> To change the channel on the 802.11a radio for an AP300 Access Port, this box <b>MUST</b> be unchecked.</p> <p><b>Note</b></p>
--	----------	--

<p><b>Support Short Preamble</b></p>	<p><b>b/g</b></p>	<p>Check the <b>Support Short Preamble</b> box to allow the Access Port to communicate with the MUs using a short 56-bit preamble.</p> <p>A preamble is the beginning part of a frame. The preamble comprises such elements as robust carrier sensing, collision detection, equalizer training, timing recovery, and gain adjustment. The administration can choose between a long or short preamble for data-frame transmission from the WLAN's adopted Access Ports.</p> <p>Use the long preamble setting (the default) for legacy wireless equipment that is not capable of dealing with short preambles. Use the short preamble setting where legacy equipment is not an issue and maximum throughput is desired, for example when streaming video or Voice-over-IP applications are used.</p>
<p><b>802.11 b/g mode</b></p>	<p><b>b/g</b></p>	<p>Use this menu to set radio rates on the Access Port to one of the following settings:</p> <p><b>B and G:</b> Clients that support 802.11b and/or 802.11g rates may associate with the Access Port.</p> <p><b>G only:</b> Only clients that support 802.11g rates may associate with the Access Port.</p> <p><b>B only:</b> Only clients that support 802.11b rates may associate with the Access Port.</p>
<p><b>DTIM per BSS (AP300 only)</b></p>	<p><b>a/b/g</b></p>	<p><b>DTIM Per BSS</b>—A DTIM is periodically included in the beacon frame that is 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 acknowledgment, so nodes sometimes miss them.</p> <p>On the AP300, the administrator can specify a period for the Delivery Traffic Indication Message (DTIM) per BSSID. This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/ beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.</p> 

Click the **Apply** button to save changes.

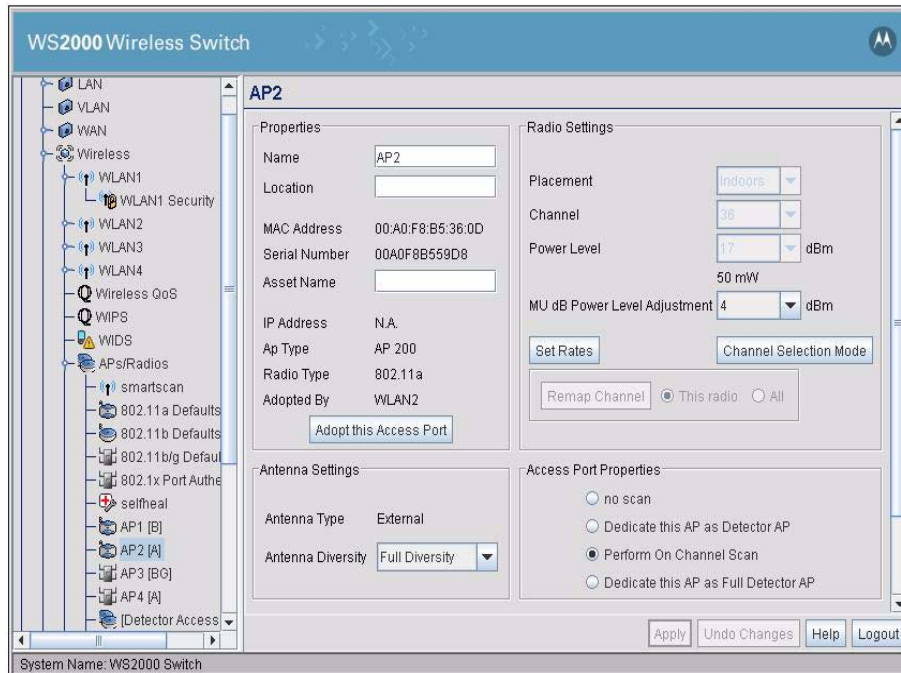
## 5.6 Advanced Access Port Settings

The WS2000 Wireless Switch GUI allows the administrator to configure the Access Port settings. To examine or change that information:

1. Select **Network Configuration** --> **Wireless** --> **Access Ports** from the left menu and then click the **+** to the left of the menu item. The detected Access Ports will be listed under the menu item.

2. Select the Access Port to examine or modify.

When the Access Port Name menu item is selected, the following screen appears:




The advanced Access Port settings are found at the bottom and right of the screen. For most installations, the default settings for the advanced settings are appropriate.

### 5.6.1 Radio Settings

<b>Placement</b>	Select either <b>Indoors</b> or <b>Outdoors</b> from the Placement pop-up menu. The setting will affect the selection available for several of the other advanced settings.
<b>Channel</b>	Select a channel number from the <b>Channel</b> drop-down menu on which the Access Port should communicate with associated MUs. (The available channels vary depending on the location setting of the switch.)
<b>Power Level</b>	Select a power level from the <b>Power Level</b> drop-down menu that will be used for radio communications between the Access Port and the MUs.
<b>MU dB Power Level Adjustment</b>	This is a Motorola specific feature. This value indicates the amount of power in dBm that the MU should reduce its Tx power by with respect to the Tx power of the AP. This feature is used to reduce the amount of radio noise in the environment for better reception.
<b>Set Rates</b>	Click the <b>Set Rates</b> button to open a sub-screen where the default Basic Rates and Supported Rates for 802.11b/g Access Ports can be set.  A list of available Basic and Supported rates for the radio are listed in two columns with check boxes next to each rate. Selecting a rate as a <b>Basic Rate</b> automatically selects that rate as a <b>Supported Rate</b> and disables the option in the Supported Rates column.

<b>Channel Selection Mode</b>	<p>Click the <b>Channel Selection Mode</b> button to open a sub-screen where you can select the modes by which channels are selected. The available options are <b>User Selection</b>, <b>Uniform Spreading</b>, and <b>Automatic Selection</b>.</p> <p>Selecting <b>Automatic Selection</b> from the sub-screen enables the <b>Remap Channel</b> button and the <b>This radio</b> and <b>All</b> options. Select the appropriate options to remap the selected channel.</p>
-------------------------------	--

## 5.6.2 Antenna Settings

<b>Internal/External Antenna</b>	Specify whether the Access Port has internal antenna or external antenna. Depending on the antenna type selected certain options in the <b>Radio Settings</b> section may be disabled.
<b>Antenna Diversity</b>	<p>Use the drop-down menu to configure the Antenna Diversity settings for Access Ports that use external antennas.</p> <p><b>Full Diversity:</b> Utilizes both antennas to provide antenna diversity.</p> <p><b>Primary Only:</b> Enables only the primary antenna.</p> <p><b>Secondary Only:</b> Enables only the secondary antenna.</p> <p> <b>NOTE:</b> Antenna Diversity should only be enabled if the Access Port has two matching external antennas.</p> <p><b>Note</b></p>

## 5.6.3 Access Port Properties

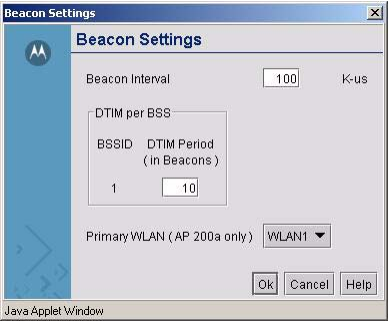
Use the options provided in this area to set the properties of the Access Port.

<b>no scan</b>	The AP does not listen to beacons
<b>Dedicate this AP as Detector AP</b>	For every configured time interval, the AP scans the channels for Rogue APs in its surroundings.
<b>Perform On Channel Scan</b>	The AP listens for beacons on the configured channels only.
<b>Dedicate this AP as a Full Detector AP</b>	For every configured time interval, the AP scans the channel for Rogue APs in its surroundings. However, MUs cannot adopt themselves to this AP.

## 5.6.4 Advanced Properties

<b>Support Short Preamble</b>	<p>Check the <b>Support Short Preamble</b> check box to allow the Access Port to communicate with the MUs using a short 56-bit preamble.</p> <p>A preamble is the beginning part of a frame. The preamble comprises such elements as robust carrier sensing, collision detection, equalizer training, timing recovery, and gain adjustment. The administrator can choose between a long or short preamble for data-frame transmission from the WLAN's adopted Access Ports.</p> <p>Use the long preamble setting (the default) for legacy wireless equipment that is not capable of dealing with short preambles. Use the short preamble setting where legacy equipment is not an issue and maximum throughput is desired, for example when streaming video or using Voice-over-IP applications.</p>
-------------------------------	--

<b>RTS Threshold</b>	<p>Set the Request to Send Threshold (<b>RTS Threshold</b>) by specifying a number.</p> <p>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 when many mobile units (MUs) are contending for transmission time. Modifying this value allows the administrator to control the number of data collisions and thereby enhance communication with nodes that are hard to find due to other active nodes in the transmission path.</p> <p>In this field, the administrator can specify a Request To Send (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports.</p> <p>This setting initiates an RTS/CTS exchange for data frames that are larger than the threshold, and sends (without RTS/CTS) any data frames that are smaller than the threshold.</p> <p>Consider the tradeoffs 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.</p> <p>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.</p>
----------------------	---

<p><b>Beacon Settings</b></p>	<p>Set the Access Port beacon settings by clicking the <b>Beacon Settings</b> button.</p> <p><b>Beacon Interval</b></p> <p>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 access-port address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM.</p> <p>Specify a beacon interval in units of 1,000 microseconds (K-us). This is a multiple of the DTIM value, for example, 100 : 10. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decreasing this value (shorten the time) to support streaming-multicast audio and video applications that are jitter-sensitive.</p> <p><b>DTIM Period</b></p> <p>A DTIM is periodically included in the beacon frame that is 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 acknowledgment, so nodes sometimes miss them.</p> <p>In this field, the administrator can specify a period for the Delivery Traffic Indication Message (DTIM). This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.</p> <p><b>DTIM Per BSS</b>— The administrator can specify a period for the Delivery Traffic Indication Message (DTIM) per BSSID. This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.</p> <p>Click <b>Ok</b> when finished setting the beacon settings.</p>	
<p><b>AP SIP Call Admission Control</b></p>	<p>Specify the number of concurrent SIP sessions allowed for this Access Port.</p> <p>SIP is the Session Initiation Protocol which controls sessions for multimedia and voice conferences.</p>	

Click **Apply** in the Access Port window to save changes.

## 5.7 Quality of Service Configuration

Disruptions in service in a wireless environment can be a significant issue in environments that have high bandwidth demands (for example, when VoIP and video broadcasts are commonplace). Wireless Internet users can also suffer disruptions due to environmental conditions, such as adverse transmission situations or a large number of wireless devices that affect radio frequency communications. The WS2000 Wireless Switch allows an administrator to adjust several parameters that can improve the quality of service (QoS) to wireless users.

Select **Wireless** --> **Wireless QoS** from the navigation menu on the left to specify how the bandwidth can be shared, how to distribute the bandwidth among the WLANs that are in service, or how to prioritize voice and multicast communications.



**WS2000 Wireless Switch**

**Wireless QoS Configuration**

Bandwidth Share Mode  
Mode: **Off**

Bandwidth Share for Each WLAN

WLAN Name	Weight	Weight (%)
WLAN1	1	50.00
WLAN2	1	50.00
WLAN3	1	0.00
WLAN4	1	0.00
WLAN5	1	0.00
WLAN6	1	0.00
WLAN7	1	0.00
WLAN8	1	0.00

Voice Prioritization and Multicast Address Settings

WLAN Name	Use Voice Prioritization	Multicast Address 1	Multicast Address 2
WLAN1	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00
WLAN2	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00
WLAN3	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00
WLAN4	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00
WLAN5	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00
WLAN6	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00
WLAN7	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00
WLAN8	<input checked="" type="checkbox"/>	01 : 00 : 5E : 00 : 00 : 00	09 : 00 : 0E : 00 : 00 : 00

System Name: DocWS2000

### 5.7.1 Setting the Bandwidth Share Mode

First, specify how the networking resources will be shared. The Bandwidth Share Mode provides three allocation options:

<b>Off</b>	Packets are served on a first-come-first-served basis. If this option is selected, the information in the <b>Bandwidth Share for Each WLAN</b> area is ignored.
<b>Round Robin</b>	Bandwidth is equally shared among all active WLANs. If this option is selected, the Weight (%) in the <b>Bandwidth Share for Each WLAN</b> area is automatically set to be the same for all active WLANs, and the values are not editable.
<b>Weighted Round Robin</b>	The bandwidth can be configured on a per WLAN basis. If <b>Weighted Round Robin</b> is the selected Bandwidth Share Mode, the weight for each WLAN can be set either using the <b>Weight</b> field or the <b>Weight (%)</b> field. When one is set, the application automatically adjusts the other field. Only the information for active WLANs can be edited.
<b>Rate Limiting</b>	The bandwidth can be configured to a maximum threshold value in Kilobytes per Second (kbps).

### **Bandwidth Share for Each WLAN Table**

The fields in this table are:

<b>WLAN Name</b>	This field lists the WLANs on the switch by name (the same name that you see in the left menu). You cannot change the name of the WLAN in this field. Go to the Wireless screen to change a WLAN name.
<b>Weight</b>	The <b>Weight</b> field specifies the relative amount of bandwidth provided to the given WLAN as compared to the other WLANs. For example, if WLAN1 has Weight set to 3 and WLAN2 has Weight set to 1, WLAN1 will get 3 times as much bandwidth as WLAN2. When the Weight field is changed, the weight percentage adjusts automatically to match.
<b>Weight (%)</b>	This field is automatically calculated and cannot be edited. This field specifies the percentage of bandwidth allocated for each of the WLANs. If the Bandwidth Share Mode is set to <b>Round Robin</b> , the Weight (%) will be the same for all active WLANs. If the Bandwidth Share Mode is set to <b>Weighted Round Robin</b> , the value is calculated based upon the Weights set for each of the WLANs. For example, if WLAN1 has Weight set to 3 and WLAN2 has Weight set to 1, the application will automatically set the weight percentage to 75% for WLAN1 and 25% for WLAN2.

### **5.7.2 Configuring Voice Prioritization and Multicast Address Settings**

To ensure better performance with Voice over IP (VoIP) broadcasts, the administrator can enable voice prioritization for particular multicast addresses within a WLAN. In the table, specify the multicast addresses by filling out the fields:

<b>WLAN Name</b>	This field lists the WLANs on the switch by name (the same name that you see in the left menu). You cannot change the name of the WLAN in this field. Go to the Wireless screen to change a WLAN name.
<b>Use Voice Prioritization</b>	Check this box to enable prioritization of voice over data for RF transmissions for the associated WLAN. This setting reduces the latency that might occur when data transmissions and VoIP transmissions compete for the same resources. Latency is usually experienced as broken or delayed speech or sound.
<b>Multicast Address #1 and Multicast Address #2</b>	Use the two <b>Multicast Address</b> fields to specify one or two MAC addresses to be used for multicast applications. Some VoIP devices make use of multicast addresses. Using this mechanism ensures that the multicast packets for these devices are not delayed by the packet queue.



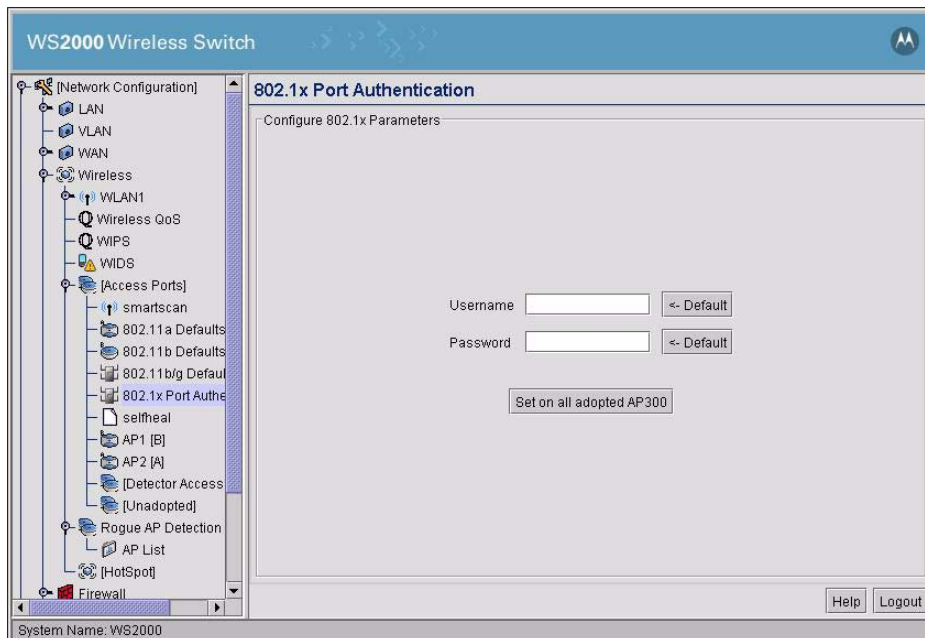
**Note**

**NOTE:** Voice prioritization and multicast addressing will only affect active WLANs. Applying these settings to an inactive WLAN will have no effect. To make a WLAN active, go to the Wireless screen.

## **5.8 Setting Up Port Authentication for AP300 Access Ports**

802.1x port authentication is used to provide security and authentication for all wired clients on a WLAN. The WS2000 Wireless Switch supports 802.1x port authentication for the AP300 Access Ports connected to it. It uses a username and password for all ports that can be configured from the wireless switch.

Select **Network Configuration** --> **[Access Ports]** --> **802.1x Port Authentication** from the navigation menu on the left.



To set up Port Authentication for all adopted AP300 Access Ports:

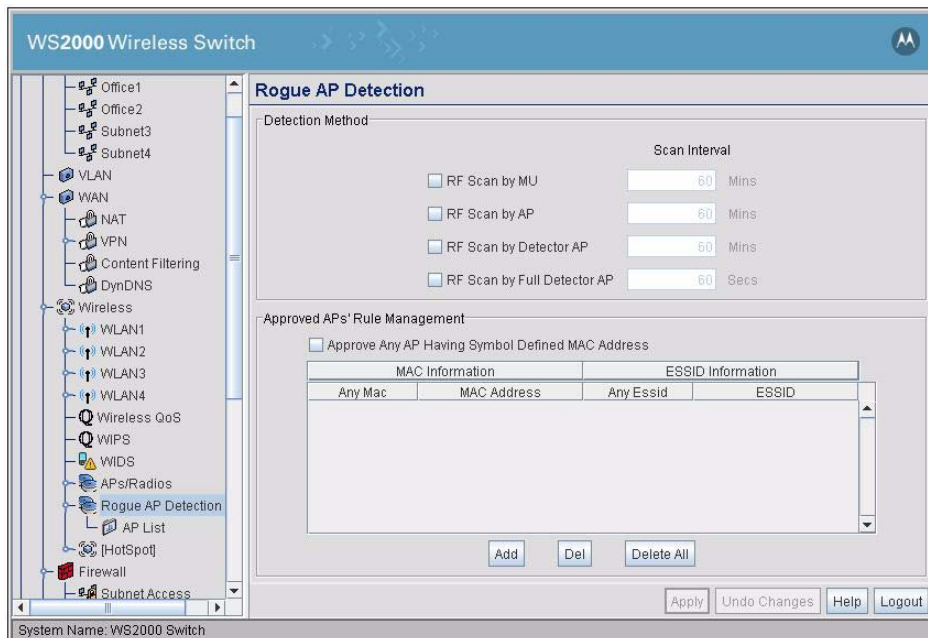
1. In the **Username** field, specify a 802.1x username for all AP300 Access Ports adopted by the switch. To use the default username click the **<- Default** button next to the **Username** field.
2. In the **Password** field, specify a 802.1x password for all AP300 Access Ports adopted by the switch. To use the default password click the **<- Default** button next to the **Password** field.
3. Click the **Set on all adopted AP300** button to set the username and password specified in the **Username** and **Password** fields on all AP300 Access Ports adopted by the switch.

## 5.9 Rogue Access Point (Port) Detection

Rogue Access Points (APs) are a hot area of concern with respect to LAN security. "Rogue AP" is a term used to describe an unauthorized access point that is connected to the production network or operating in a stand-alone mode (in a parking lot or in a neighbor's building). Rogue APs, by definition, are not under the management of network administrators and do not conform to any network security policies.

Although 802.1x security settings should completely protect the LAN, organizations are not always fully compliant with the newest wireless-security best practices. In addition, organizations want to be able to detect and disarm rogue APs. The WS2000 Wireless Switch provides a mechanism for detecting and reporting rogue APs.

Select **Network Configuration** --> **Wireless** --> **Rogue AP Detection** from the navigation menu on the left.



The Rogue AP Detection screen allows the administrator to determine how thoroughly the switch will search for rogue APs as well as list the approved APs.

### 5.9.1 Setting Up the Detection Method

The WS2000 Wireless Switch provides three methods for detecting rogue Access Points (APs). Use the top part of the Rogue AP Detection screen to set the method or methods that the switch will use to detect rogue APs.

1. Check the **RF Scan by MU** box if you want the switch to work with mobile units (MUs) to detect a rogue AP.

With this option selected, each MU reports whether it supports rogue AP detection mechanisms. If so, the switch sends WNMP requests, at regular intervals, to the MU to get a list of APs. The MU scans all the channels for APs in the vicinity. The MU then prepares a list of APs (BSSIDs) and sends it back to the switch using WNMP response message. The switch processes this information.

2. Check the **RF Scan by AP** box if you want the switch to work with the APs to detect a rogue AP. By default, this method is selected.

With this option enabled, the switch sends a WISP configuration message to each adopted AP that indicates that rogue AP detection is needed. Each AP listens for beacons in its present channel and passes the beacons to the switch without modification. The switch then processes the beacons to determine whether any of them are rogues. This method is less disruptive than the RF Scan by MU mode.

3. Check the **RF Scan by Detector AP** box if you have set up a detector AP on the LAN and want the switch to work with that AP to detect rogue APs. To set an AP as a detector AP, go to the screen for the adopted AP under APs/Radios in the navigation menu and check the appropriate box.
4. Check the **RF Scan by Full Detector AP** box if you have set up an AP on the LAN that acts exclusively as a Detector AP and want the switch to work with this AP to detect rogue APs. To set an AP to act as a full detector AP, go to the screen for that adopted AP under APs/Radios in the navigation menu and check the appropriate box. When an AP is set up as a Full Detector AP then it will not serve any data clients.



**NOTE:** Note that only some access ports have the capability of being a Detector AP, including Motorola AP100, AP200, and AP300 Access Ports.

**Note**

5. In the **Scan Interval** field, enter a time interval (in minutes) between detection RF scans. Do this for each of the selected detection methods. By default, these scans are set at one hour intervals.



**NOTE:** Scan interval for Full Detector AP is defined in seconds. For other scans, the interval is defined in minutes.

**Note**

## 5.9.2 Defining and Maintaining Approved AP List Rules

The lower half of the Rogue AP Detection screen specifies rules that determine whether a detected AP can be approved or not. Each entry in the table works as an AP evaluation rule. You can specify a particular MAC address or a particular ESSID, or you can indicate that any MAC address or ESSID will work. However, if you select **Any MAC** and **Any ESSID** on the same line, all APs will be approved. Up to 20 rules can be defined.

1. Check the **Approve Any AP Having a Symbol Defined MAC Address** box to indicate that any Symbol AP (that is, one that has a known Symbol MAC address) is an approved AP.
2. Click the **Add** button to add a line in the rule table and then fill out the following table cells:

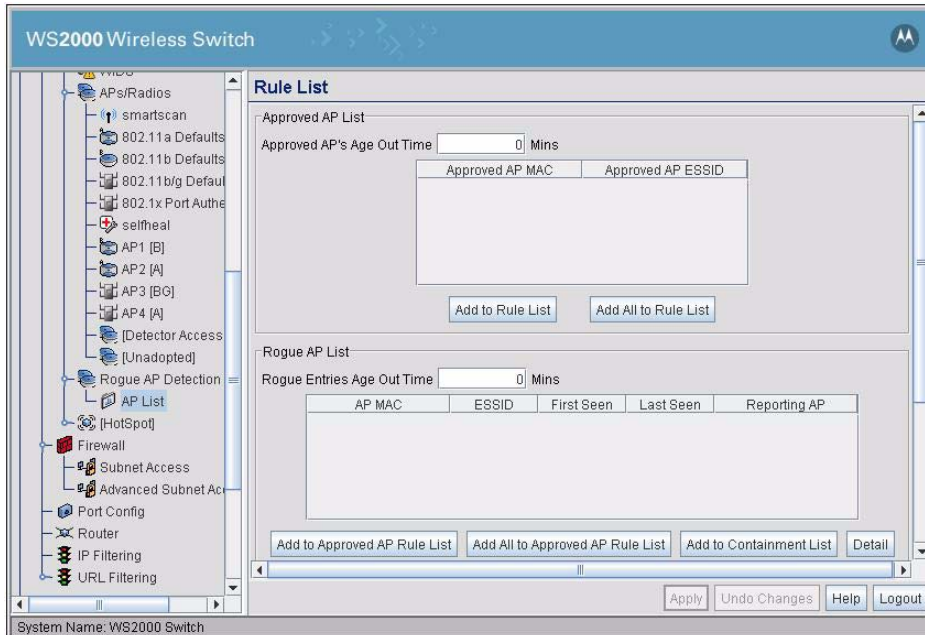
<b>Any MAC</b>	Check this box to indicate that an AP with any MAC address matches the rule.
<b>MAC Address</b>	Enter an approved MAC address to be used during the detection process. This field is only used when <b>Any MAC</b> (on the same line) is not checked.
<b>Any ESSID</b>	Check this box to indicate that an AP with any ESSID matches the rule.
<b>ESSID</b>	Enter an approved ESSID to be used during the detection process. This field is only used when <b>Any ESSID</b> (on the same line) is not checked.

3. To delete a particular rule from the table, select the rule and then click the **Del** button.
4. Click the **Delete All** button to clear the entire rule list.

### 5.9.3 Examine the Approve and Rogue Access Ports

This screen displays information about APs known to the switch. All approved APs are listed in the upper table. All rogue APs are listed in the lower table. This screen also allows the administrator to create detection rules from the information collected about approved or rogue APs.

To maintain the lists, select **Network Configuration --> Wireless --> Rogue AP Detection --> AP List** from the navigation menu on the left.



#### 5.9.3.1 The Approved AP List

Each row of this table represents an approved AP that the switch has found. For each AP, both the MAC and the ESSID for the AP are listed. Use this portion of the screen to change the age out time or to add a rule to the rule list for a particular AP:

1. Enter a number in the **Approved AP's Age Out Time** field to indicate the number of elapsed minutes before an AP will be removed from the approved list and reevaluated. A zero (0) in this field indicates that an AP can stay on the list permanently.
2. Click the **Add to Rule List** button to add a rule to the Approved APs' Rule Management table on the Rogue AP Detection screen. The generated rule will use the MAC address and ESSID of the selected AP.
3. Click the **Add All to Rule List** button to add a rule to the Approved APs' Rule Management table on the Rogue AP Detection screen for all the APs on the list. The generated rules will use the MAC addresses and ESSIDs of the APs.

#### 5.9.3.2 The Rogue AP List

Each row of this table represents a rogue AP that the switch has found. For each AP, both the MAC and the ESSID for the AP is listed as well as some information about when the AP was first and last seen:

<b>AP MAC</b>	This field is the MAC address for the rogue AP.
<b>ESSID</b>	This field is the ESSID for the rogue AP.

<b>First Seen</b>	This field indicates the number of elapsed hours since the rogue AP was first noticed on the network in hours:minutes:seconds.
<b>Last Seen</b>	This field indicates the number of elapsed hours since the rogue AP was last noticed on the network in hours:minutes:seconds.
<b>Reporting AP</b>	This field shows the MAC address of the device that detected the rogue AP.

1. Enter a number in the **Rogue Entries Age Out Time** field to indicate the number of elapsed minutes before an AP will be removed from the rogue list and reevaluated. A zero (0) in this field indicates that an AP can stay on the list permanently.
2. Click the **Add to Approved AP Rule List** button to add a rule to the Approved APs' Rule Management table of the Rogue AP Detection screen. The generated rule will use the MAC address and ESSID of the selected AP.
3. Click the **Add All to Approved AP Rule List** button to add a rule to the Approved APs' Rule Management table on the Rogue AP Detection screen for all the APs on the list. The generated rules will use the MAC addresses and ESSIDs of the APs.
4. Click the **Add to Containment List** button to add a selected Rogue AP to a containment list. The containment list is a list of APs that will not be allowed to join the network. MUs associated with APs in the containment list are de-authenticated every time interval defined in the **Deauth Interval** field.

### 5.9.3.3 Rogue AP Containment

Rogue AP Containment feature enables you to prevent rogue APs and their associated MUs from joining your network. This feature is disabled by default.

The screenshot displays the configuration page for a WS2000 Wireless Switch, specifically the 'Rogue AP Containment' section. The interface includes a navigation tree on the left with categories like Network Configuration, Wireless, and System Configuration. The main content area is titled 'Rule List' and contains the following elements:

- Rogue AP List:** A table with columns for AP MAC, ESSID, First Seen, Last Seen, and Reporting AP. Below the table are buttons for 'Add to Approved AP Rule List', 'Add All to Approved AP Rule List', 'Add to Containment List', and 'Detail'.
- Rogue AP Containment:** A section with a checkbox for 'Enable Rogue AP Containment', a 'Deauth interval' field set to '2' seconds, and a checkbox for 'Deauth all APs in Rogue List'. A 'Rogue AP MAC' input field and a 'Remove AP from Death List' button are also present.

At the bottom of the configuration area, there are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'WS2000 Switch' is visible at the bottom left of the window.



**Note**

**NOTE:** Rogue AP Containment should only be used to contain those APs that adversely impact the network and its devices.



To enable and configure Rogue AP Containment:

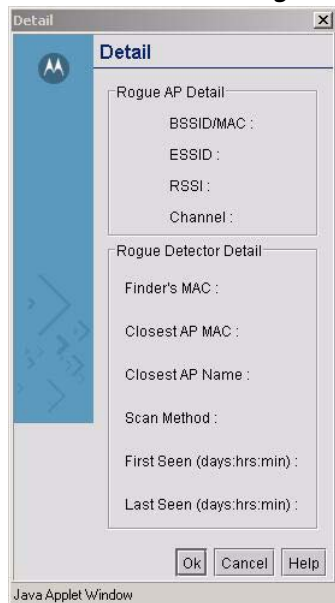
1. Check the **Enable Rogue AP Containment** box to enable this feature.
2. All MUs associated to Rogue APs in the **Rogue AP Containment list** are deauthenticated by the switch. The **Deauth Interval** value sets the time duration in seconds between two such de-authentications. For example, if the time duration is 2 seconds, the switch de-authenticates MUs associated with Rogue APs every 2 seconds. This is only available when Rogue AP Containment is enabled.
3. Check the **Deauth all APs in Rogue List** box to force de-authentication of all the APs listed in the **Rogue AP list**. This is only available when Rogue AP Containment is enabled.
4. The Rogue AP Containment list is a list of MAC addresses of APs that have been contained. Use the **Remove AP from Deauth List** button to remove a selected AP from the containment list. When removed, the AP can associate itself with the network and allow MUs to associate with it.

### 5.9.3.4 Getting Detailed Information About a Rogue AP

The Rule List screen provides a means to get detailed information about a rogue Access Point as well as its detector to help an administrator track it down. To see detailed information:

1. Select a rogue AP from the **Rogue AP List**.
2. Click the **Detail** button to open a new window to view detailed information about the rogue AP and its detector.

#### ***Details About the Rogue AP***



The top of the Rogue AP Detail screen lists information about the rogue AP:

<b>BSSID/MAC</b>	This field contains the BSSID or the MAC address for the rogue AP.
<b>ESSID</b>	This field is the ESSID for the rogue AP.
<b>RSSI</b>	This field displays the Receiver Signal Strength Indicator (RSSI) for the rogue AP. The value will be between 1 and 255. The larger the value, the better the signal strength and the closer the AP.



## Details About the Rogue Detector

The lower portion of the Rogue AP Detail screen displays information about the AP that detected the rogue. This information is provided to the administrator to help locate the rogue.

<b>Finder's MAC</b>	This is the MAC address for the AP that detected the rogue AP.
<b>Closest AP MAC</b>	This is the MAC address for the AP that is physically closest to the rogue AP.
<b>Closest AP Name</b>	This is the name of the AP that is physically closest to the rogue AP.
<b>Scan Method</b>	This is the scan method that was used to detect the rogue AP. The possible values are: <ul style="list-style-type: none"> <li>• MU (detected by a mobile unit)</li> <li>• Detector (detected by the Detector AP)</li> <li>• On Channel (detected by non-detector AP)</li> </ul>
<b>First Seen</b>	This is the number of hours:minutes:seconds since the rogue AP was first noticed on the network.
<b>Last Seen</b>	This is the number of hours:minutes:seconds since the rogue AP was last noticed on the network.



**NOTE:** The WS2000 Wireless Switch only *reports* rogue APs. It is up to the administrator to change security settings or disrupt the rogue AP's connection.

### Note

## 5.9.4 Setting SNMP Traps for Rogue APs

It is also possible to set a trap for a rogue AP.

1. Go to **[System Configuration]** --> **SNMP Access** --> **SNMP Traps** from the navigation menu.

The screenshot shows the configuration page for the WS2000 Wireless Switch, specifically the 'SNMP Traps' section. The interface includes a navigation tree on the left and a main configuration area on the right. The 'SNMP Traps' section is divided into several categories:

- System Traps:** Includes checkboxes for System Cold Start, Configuration Changes, User Login Failure, Admin Password Change, and Low Compact Flash memory. A field for 'less than' is set to 1024 KB.
- Network Traps:** Includes checkboxes for Physical port status change, Interface status change, DynDNS Update, Denial of service (DOS) attempts, and IPS Event. A field for 'Send trap every' is set to 10 secs.
- SNMP Traps:** Includes checkboxes for SNMP authentication failures and SNMP ACL violation.
- MU Traps:** Includes checkboxes for MU associated, MU unassociated, MU denied association, and MU denied authentication.
- AP Traps:** Includes checkboxes for AP adopted, AP unadopted, AP denied adoption, AP detected radar (802.11a only), and **Rogue AP** (circled in red).
- Wireless Traps:** Includes checkboxes for Hotspot MU State Change, Wids MU Event, Wids Radio Event, and Wids Switch Event.

At the bottom of the page, there are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name is identified as 'DotWS2000'.

2. Check the **Rogue AP** box (in the lower right area of the screen) to generate a trap when a rogue (unauthorized) access port (AP) is detected. The detection process is non-disruptive and will not affect the performance of the switch.

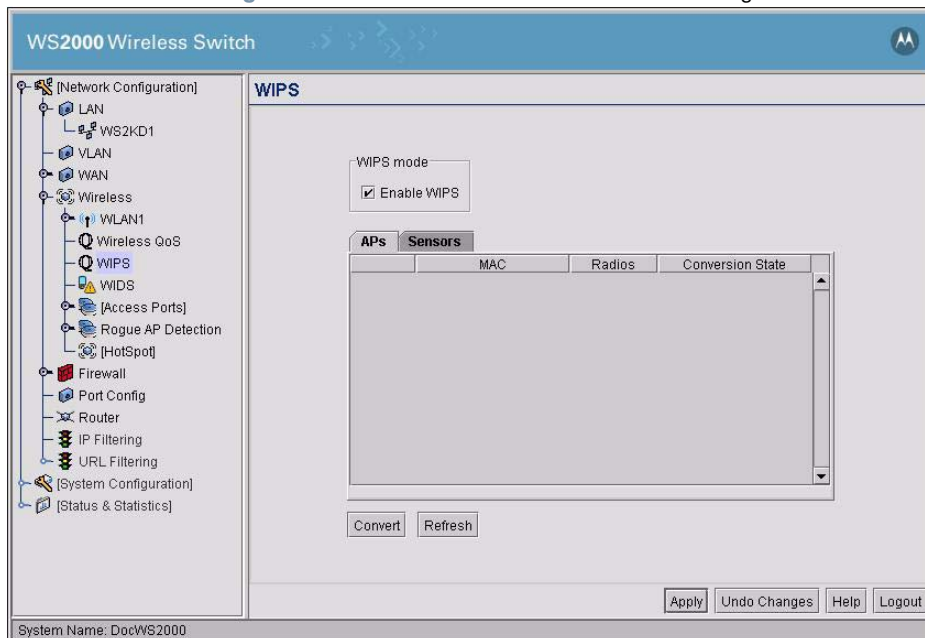
The detection functionality is greatly enhanced when the Approved AP list is filled out on the AP List screen under Rogue AP Detection.

## 5.10 Configuring Wireless Intrusion Protection System (WIPS)

The Wireless Intrusion Protection System (WIPS) provides additional wireless LAN security by monitoring the airwaves for any kind of Denial of Service (DoS) attacks. It is also able to actively suppress any rogue clients and APs in the network.

Symbol's WIPS solution utilizes AP300s that act as dedicated sensors and send out relevant information to a centralized WIPS server. The WIPS server correlates all the data and provides threat mitigation services.

Go to **Network Configuration**--> **Wireless** --> **WIPS** from the navigation menu.



1. Click the **Enable WIPS** check box in the **WIPS mode** section.
2. Check the box next to each of the APs or Sensors which you wish to convert to a dedicated detector port.
3. Once all desired APs have been checked, click the **Convert** button to begin the conversion process.



### Note

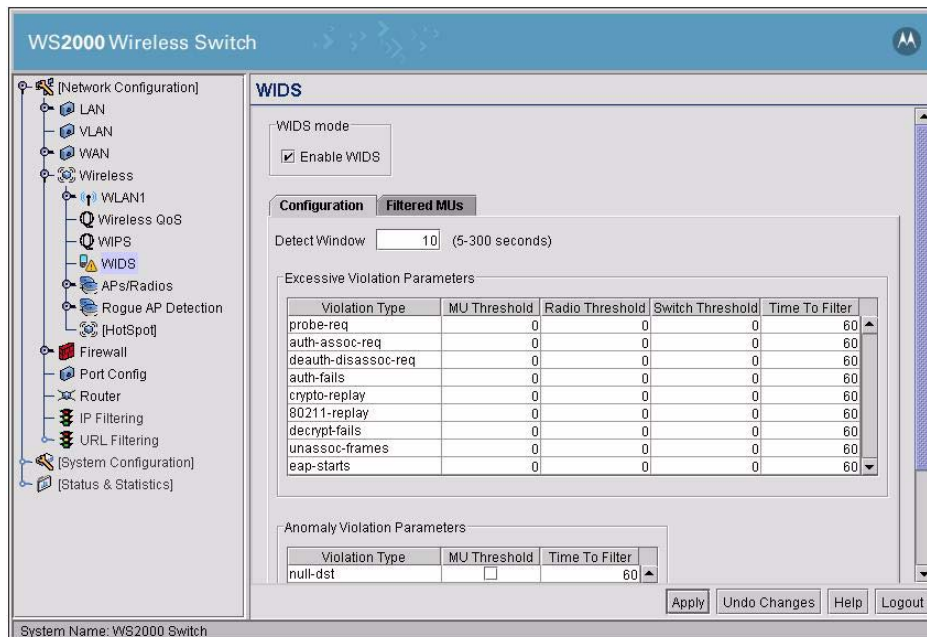
**NOTE:** If no APs or Sensors are displayed in the tables, go to the properties page for each AP you wish to use as a WIPS detector and select the **Dedicate this AP as a Detector AP** option and return the WIPS screen.

4. Click the **Apply** button to save any changes made on this screen. Navigating away from the current screen without clicking the **Apply** button results in all changes to this screen being lost.

## 5.11 Wireless Intrusion Detection System

The Motorola Wireless Intrusion Detection System (WIDS) protects against a wide range of malicious attacks on the WS2000 Wireless Switch. This feature inspects each packet that is received by the WS2000 and then based on analysis decides if an intrusion is happening on the device.

By default, WIDS is disabled. It can be enabled from the [\[Network Configuration\]](#)-->[Wireless](#)-->[WIDS](#) screen.



For WIDS a violation is when excessive numbers of packets of the same type are received.

WIDS keeps track of each packet type that is received and when a threshold value is crossed, raises a violation alarm. Appropriate action can be performed based on the alerts. WIDS provides alerts when thresholds are crossed for:

- MUs
- Radio
- Switch

WIDS keeps tracks of these violations:

- probe-req - Probe Requests
- auth-assoc-req - Authentication Association Requests
- deauth-deassoc-req - Deauthentication De-association Requests
- auth-fails - Authentication Failures
- crypto-replay - Cryptography Replays
- 802.11-replay - 802.11x Replays
- decrypt-fails - Decryption Failures
- unassoc-frames - Unassociated Frames
- eap-starts - EAP Start Frames

WIDS also keep track of anomalies. An anomaly is defined as an event which is different from the general occurrences on a WS2000. The following anomalies are tracked:

- null-dst - NULL destination
- same-src-dst - Same source and destination address
- mcast-src - Source MAC is multicast
- weak-wep-iv - Weak WEP
- tkip-cntr-meas - TKIP counter measures
- invalid-frame-len - Invalid frame length

### 5.11.1 WIDS Configuration

The WIDS parameters for violations and anomalies can be configured from the **Configuration** tab of the WIDS screen. The tab is enabled when the **Enable WIDS** check box is selected.

To configure WIDS:

1. Enter a time value in seconds for the **Detect Window**. WIPS checks for violations and anomalies every detect window value. For example, if the value is 30 seconds, WIPS checks for violations and anomalies every 30 seconds.

#### 5.11.1.1 Excessive Violation Parameters

Use the **Excessive Violation Parameters** section to set violation parameters. Violation parameters threshold values can be set for MUs, Radio, and Switch.

To set the Excessive Violation Parameter value:

1. Click on the violation that you want to monitor.
2. If you would like to monitor the MU for a violation, click under the MU Threshold column for that violation. The column becomes editable. Enter a suitable value for the threshold. You can similarly set the thresholds for the Radio as well as the Switch for the violation.
3. Use the **Time to Filter** column to set the time duration during which any packets received from the MU will be filtered out. For example, if this value is set to 135 seconds, the MU is filtered out for 135 seconds.

The **Radio Threshold** and **Switch Threshold** columns enables you to set up threshold values upon reaching which a SNMP trap is generated.

#### 5.11.1.2 Anomaly Violation Parameters

Use the Anomaly Violation Parameters section to set the parameters for Anomalies. When enabled, the MU is filtered out for the duration specified in the **Time to Filter** column.

1. Enable or disable Anomaly Violation detection by selecting the **MU Threshold** check box.
2. Use the **Time to Filter** column to set the time duration during which any packets received from the MU will be filtered out. For example, if this value is set to 135 seconds, the MU is filtered out for 135 seconds.
3. Click the **Apply** button to save any changes made on this screen. Navigating away from the current screen without clicking the **Apply** button results in all changes to this screen being lost.

### 5.11.2 Filtered MUs

The Filtered MUs screen displays a list of all MUs that have been filtered out by WIDS. You can, if required, remove any or all MUs listed in the Filtered MUs table.

The Filtered MUs table displays the following:

<b>MU MAC</b>	The MAC address of the MU that has been filtered out.
<b>Radio</b>	The Radio that has been filtered out
<b>Violation Type</b>	The violation that caused the MU to be filtered out
<b>Time Left</b>	The duration after which the MU will not be filtered out.

Use the check box to the left of each filtered MU to select it for removing it from the Filtered MUs table. Use the **Delete MU Entry** button to remove the selected MU or MUs. You can also remove all the MUs in the table by clicking the **Delete All MU Entries** button.

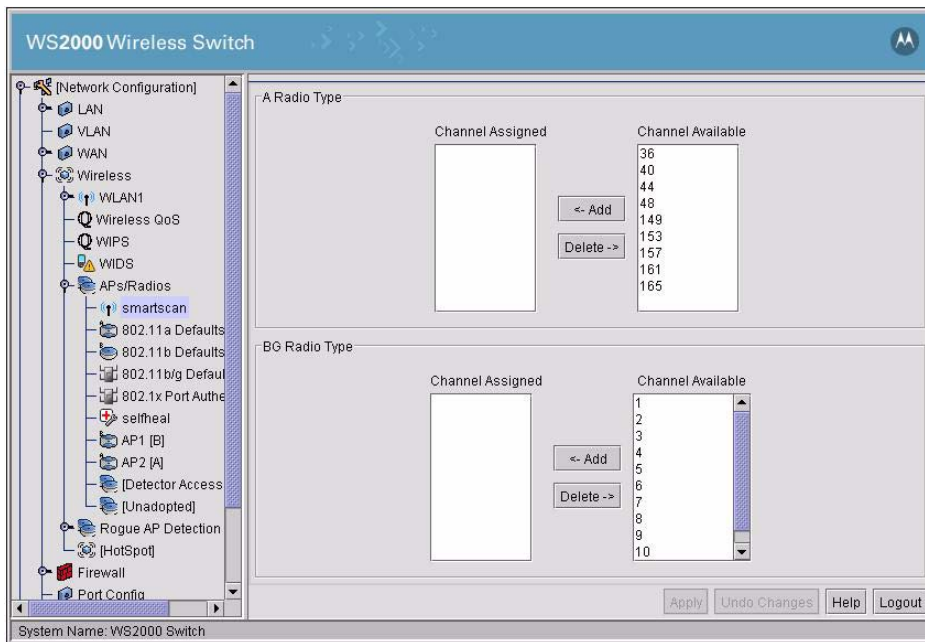
To refresh the Filtered MUs table, click the **Refresh Table** button.

## 5.12 Smart Scan

Each radio, depending on the country it is operating in, provides a large number of channels for data transmission. This means that when a MU roams from one AP to another, it has to scan all the available channels for that radio to find the WLAN it was connected to. This scan process takes time depending on the number of channels to scan.

When deploying real-time applications such as VoIP or video-streaming over wireless, this roaming latency creates a break in these application. Smart Scan allows you to select the channels to scan on a radio to reduce this latency.

To select the channels to scan, navigate to **[Network Configuration]-->Wireless-->APs/Radios-->smartscan**. The smartscan screen displays.



To select the channels to scan:

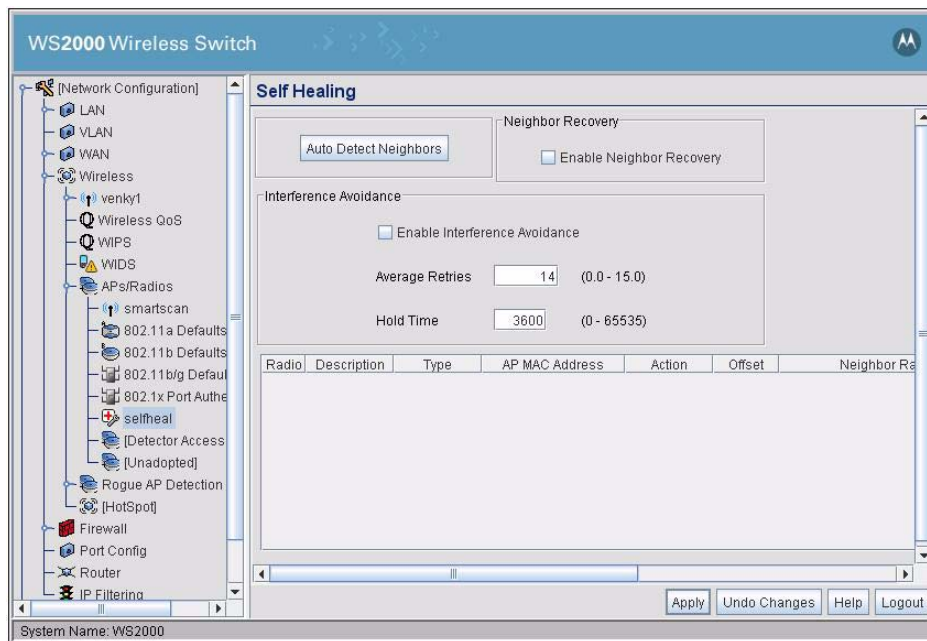
1. Select the channels to scan for each radio type. Multiple channels can be selected by using the CTRL Key+ mouse click combination.
2. Click **Add** button to move the selected channels from the **Channel Available** list to the **Channel Assigned** list. Scan will be performed only on the channels in the **Channel Assigned** list.  
Click **Delete** button to remove channels from the **Channel Assigned** list to the **Channel Available** list. The removed channels will not be scanned.

You can select the scan channels for both radio types.

## 5.13 Self Heal

A self-healing network is one that is capable of maintaining the availability of the network under all circumstances. The network can self-manage in response to the events that occur within the network. Self heal for WS2000 is provided by the device maintaining a Neighbor Table with entries for each device in its neighborhood.

Self heal can be activated from **[Network Configuration]-->Wireless-->APs/Radios-->selfheal** menu item.



Self healing consists of two different features, *Neighbor Recovery* and *Interference Avoidance*. Neighbor Recovery uses a Neighbor Table to keep track of all its immediate neighbor portals. Interference Avoidance detects interference on the channel on which the portal is operating and shifts the portal's channel to an unused channel in the channel list.

### Neighbor Recovery

When enabled, a portal listens to beacons of its neighbors configured in the Neighbor Table. The AP goes into monitoring mode once it has listened to a set number of beacons from its neighbor. After going into the monitoring mode, if the AP is not able to listen to the beacons from a neighbor, it considers that particular neighbor as being down and take appropriate neighbor recovery action as configured in the Neighbor Table.

The following actions can be performed to recover the lost neighbor.

- **none** - No action is taken to recover
- **raise-power** - The AP raises its operating power to the maximum power level less the Offset value.
- **open-rates** - The AP operates with its configured basic and supported rates.
- **both** - Both the raise-power and open-rates actions are performed.

## Interference Avoidance

When enabled, the AP keeps track of the retry count for the Tx frames and if this count exceeds the threshold limit set in Average Retries field, triggers the Interference Avoidance feature. The AP then does a Automatic Channel Selection (ACS) and shifts its channel to one where there is no interference.

The Hold Time specifies the time duration in seconds that the AP has to wait after having done a ACS before doing the next ACS.

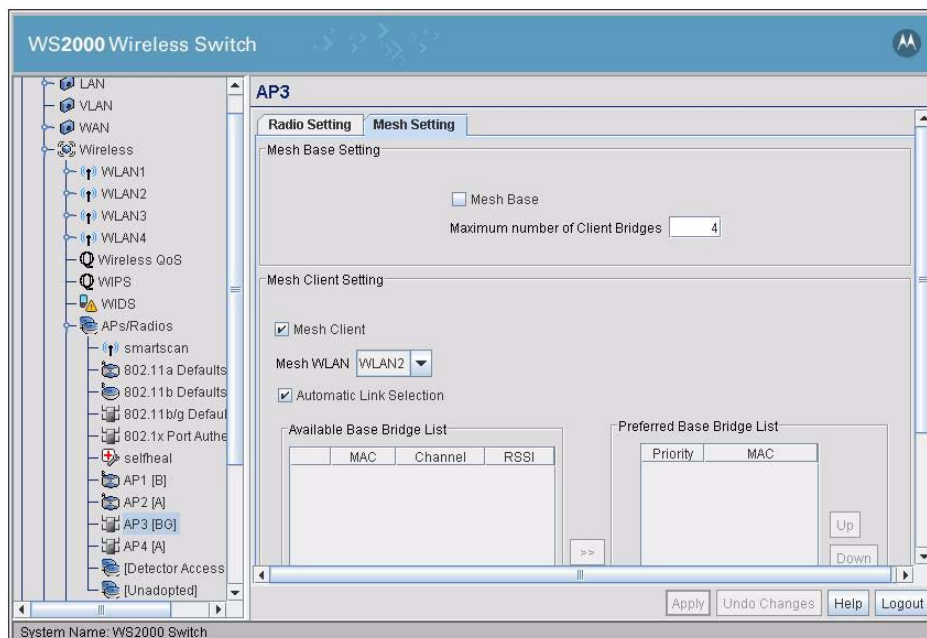
## 5.14 Mesh Settings

The WS2000 Wireless Switch provides support for creating and managing a mesh network. In a mesh network, there are more than two pathways of communication between each node. In a mesh network, each node communicates with the other nodes directly or by hops using other nodes as intermediary stops. As there are multiple paths between nodes, mesh networks provides reliability and offers redundancy.

Mesh network is supported by the WS2000 Wireless Switch through APs that have mesh network support integrated in them. AP300 from Motorola is an AP that has in built support for Mesh networks.

To create and manage a Mesh Network, select **[Network Configuration]-->Wireless-->APs/Radios--><Radio Name>**. This radio must support Mesh network. The **Radio Settings** screen is displayed.

Select the **Mesh Settings** tab on the screen to view the *Mesh Settings* screen.



A Mesh Base device is a device that allows other devices to connect to it as its client. The Mesh Base is also responsible to provide the redundancy and reliability. Each Mesh Base can support up to 6 Mesh Client devices.

A Mesh Client is a device that connects to the Mesh Base to access the network resources.



**Note**

**NOTE:** A radio can act as a Mesh Base or as a Mesh Client or as both.



### 5.14.1 Mesh Base Setting

Use the *Mesh Base Settings* area of the *Mesh Setting* screen to set up the device as a Mesh Base device. To do so:

1. Check the **Mesh Base** box to set the device as a Mesh Base.
2. Enter the maximum number of clients this Mesh Base device can handle simultaneously. The maximum number of client devices that can be handled is 6.
3. Click **Apply** button to save changes.

### 5.14.2 Mesh Client Setting

Use the *Mesh Client Setting* area of the *Mesh Setting* screen to set up the device as a Mesh Client device. To do so:

1. Check the **Mesh Client** box to set the device as a Mesh Client.
2. Select the Wireless LAN this device will connect to from the **Mesh WLAN** drop-down.
3. To enable a Mesh Client device to automatically select the best Mesh Base to connect to, check the **Automatic Base Selection** box.
4. The **Available Base Bridge List** is a list of all available Mesh Base devices with their MAC address, the channel they operate in, and the Radio Signal Strength Indicator (RSSI) value.

Use the **Refresh** button to refresh the **Available Base Bridge List**.

5. The **Preferred Base Bridge List** is a list of Mesh Bases that the device prefers to connect to. The priority of the Mesh Base can be modified by moving the device up or down the **Preferred Base Bridge List**. To change the priority of a Mesh Base, use the **Up** and **Down** buttons. These buttons are not available when **Automatic Base Selection** is enabled.
6. To add a new Mesh Base to the **Preferred Base Bridge List**, click the **Add** button. A dialog opens where you can enter the MAC address of the Mesh Base and the required priority. This button is not available when **Automatic Base Selection** is enabled.
7. To remove a Mesh Base from the **Preferred Base Bridge List**, click the **Remove** button. The device is removed from the list. This button is not available when **Automatic Base Selection** is enabled.
8. To remove all devices from the **Preferred Base Bridge List**, click the **Remove All** button. All the device are removed from the list. This button is not available when **Automatic Base Selection** is enabled.
9. Click **Apply** button to save changes made to Mesh configuration.



## ***Administrator and User Access***

6.1	Configuring Administrator Access .....	6-2
6.1.1	Selecting the Type of Admin Access .....	6-2
6.1.2	Configuring Secure Shell Connection Parameters .....	6-3
6.1.3	Admin Authentication and RADIUS Server Authentication Setup .....	6-3
6.1.4	Setting Up AirBEAM Software Access .....	6-4
6.1.5	Applet Timeout Specification .....	6-4
6.1.6	Changing the Administrator Password .....	6-4
6.2	Configuring User Authentication .....	6-5
6.2.1	Configuring the RADIUS Server .....	6-5
6.2.2	Configuring Lightweight Directory Access Protocol (LDAP) Authentication .....	6-7
6.2.3	Setting Up a Proxy RADIUS Server .....	6-8
6.2.4	Managing the User Database .....	6-9
6.2.5	Adding New Guest Users Quickly .....	6-10
6.2.6	Setting the User Access Policy .....	6-13
6.3	Managing Digital Certificates .....	6-15
6.3.1	Importing CA Certificates .....	6-15
6.3.2	Creating Self Certificates .....	6-17

## 6.1 Configuring Administrator Access

The WS2000 Network Management System allows users to log in to perform administration tasks. The switch administrator can change any settings within the WS2000 Network Management System. The default login name for the switch administrator is “**admin**” and the initial password is “**symbol**”.

The WS2000 Access screen is used to configure the access to the WS2000 Wireless Switch. This screen is used to configure the access and related parameters for the WS2000 Wireless Switch. You can also change the administrative password from this screen. This screen can be accessed from **System Configuration --> System Settings --> WS2000 Access** menu item on the left.

The screenshot shows the WS2000 Access configuration page. On the left is a navigation tree with 'WS 2000 Access' selected. The main area is titled 'WS 2000 Access' and contains several sections:

- WS 2000 Access:** A table with columns 'From LAN', 'LOG', 'From WAN', and 'LOG'. Rows include Applet HTTP (port 80), Applet HTTPS (port 443), CLI TELNET (port 23), CLI SSH (port 22), SNMP (port 161), and CF Card Access: FTP/AirBeam (port 21).
- Allow administrative access to:** A section with an 'IP Address' list box and 'Add'/'Del' buttons.
- Secure Shell:** Fields for 'Authentication Timeout' (120) and 'SSH Client Inactivity Timeout' (120).
- Admin Authentication:** Radio buttons for 'Local' (selected) and 'Radius', with a checkbox for 'Authenticate AirBEAM user using Local DB'.
- Radius Server for Admin Authentication:** Fields for 'Radius Server IP' (192.168.0.4), 'Port' (1812), and 'Shared Secret' (#####).
- AirBEAM Access:** Fields for 'AirBEAM Username' (airbeam) and 'AirBEAM Password' (#####).
- Applet Timeout:** Field for 'HTTP/S Timeout' (0) Mins.
- Administrator Access:** A button labeled 'Change Admin/Manager/Guest Admin Password'.

Buttons at the bottom include 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'WS2000' is shown at the bottom left.

### 6.1.1 Selecting the Type of Admin Access

The WS2000 Network Management System runs from a standard Web browser. By default, any individual on an enabled subnet or over the WAN can access the log screen by specifying one of the IP addresses associated with the user interface. The WS2000 Access screen allows the administrator to restrict access to the WS2000 switch from different locations. By selecting the appropriate check boxes, you, the administrator can allow or disallow specific types of access from the WAN port or from the LAN subnets.



#### Note

**NOTE:** When connected to the switch using multiple methods, for example, when connected through both SSH and HTTP, saving the configuration using one of the methods will cause a disconnect from the other method.

Choose the types of access to allow by checking the associated check box.

Access	Port	Description
Applet HTTP	80	Allows administrator access to the WS2000 Management System through a standard HTTP web browser.
Applet HTTPS	443	Allows administrator access to the WS2000 Management System through a HTTPS (secure) connection from a web browser.

Access	Port	Description
<b>CLI TELNET</b>	23	Allows administrator access to the wireless switch through TELNET. Allows the administrator to access the switch through the command line interface.
<b>CLI SSH</b>	22	Allows administrator access to the command line interface of the wireless switch through the Secure Shell (SSH) protocol of TCP/IP.
<b>SNMP</b>	161	Allows administrator access to change switch settings from an SNMP server.
<b>CF Card Access: FTP/ AirBeam</b>	21	Allows administrator access with AirBEAM using FTP to upload and download configuration data, firmware, and other software to/from the switch's CF card. The username and password used for AirBEAM is configured in the AirBEAM Access section of the screen.

**Note**

**NOTE:** If all the check boxes in this section are disabled, the administrator will not be able to access the switch through the WS2000 Management System user interface. The only way the device can then be accessed is through a direct serial connection from a PC. If this situation occurs accidentally, you can restore the settings using the command line.

### **LOG Column**

To enable logging for connections through a particular protocol, click the check box for the protocol under the **LOG** column. When logging is enabled, the first successful connection using the protocol is logged. However, every failed connection through any access protocol is logged.

### **Allow Administrative access to**

To allow administrators to access the switch from specific IPs, click the **Add** button under the **Allow Administrative access to** list. A line is created in the list where you can add the IP address from where an administrator can access this switch. However, this access is only allowed for a maximum of 4 devices.

### **Management Access across subnet**

To allow administrators to access the switch from other subnets, check this box. To disallow management access to this switch from other subnets, this check box must not be checked.

## **6.1.2 Configuring Secure Shell Connection Parameters**

If **CLI SSH (port 22)** is enabled either on WAN or LAN, set the fields in the Secure Shell area:

1. Enter a value, in seconds, when a client connected via SSH must reauthenticate in the **Authentication Timeout** field. The default is 120 seconds (2 minutes).
2. Enter the amount of time, in seconds, when an inactive client using SSH will be disconnected in the **SSH Client Inactivity Timeout** field. The default is 120 seconds (2 minutes).

## **6.1.3 Admin Authentication and RADIUS Server Authentication Setup**

There are two methods available for authenticating administrators upon connecting to the switch. Use this area to set up the desired authentication methods.

- Select the **Local** radio button to have the administrator of the switch authenticate using the built-in password authentication process (that is, using the standard admin password).
- Select the **RADIUS** radio button to have the administrator authenticate against a RADIUS database. If RADIUS is selected, then the RADIUS server information can be entered in the **RADIUS Server for Admin Authentication** area.

If the **RADIUS** button is selected, specify the **RADIUS Server IP** address, the communication port for the authentication process, and the RADIUS server's **Shared Secret** (password) to use.

### 6.1.4 Setting Up AirBEAM Software Access

Symbol's AirBEAM software suite is a comprehensive set of mobility management tools that maximize the availability, security and effectiveness of a wireless network. The fields in this section of the screen allow the administrator to enable access from the AirBEAM software suite and to set the AirBEAM password.

1. To enable AirBEAM access, check the **Enable AirBEAM** check box.
2. Specify a password for AirBEAM software access. Note that the AirBEAM login name is always "airbeam".
3. Click the **Apply** button to save changes.

### 6.1.5 Applet Timeout Specification

This screen provides a method to set a timeout for an inactive connection from either an HTTP or HTTPs connection. Specify the maximum number of inactive minutes allowed in the **HTTP/S Timeout** field. A zero (0) value indicates that an inactive administrator connection will never be timed out.

### 6.1.6 Changing the Administrator Password

Click the **Change Admin/Manager/Guest Admin Password** button (In the bottom right of the WS2000 Access screen) to open a sub-screen that allows the administrator to change the switch administrator's password.

1. Select one of *Admin*, *Manager* or *Guest* from the **User** field depending on which user's password you wish to change.
2. Enter the new admin password in both fields, and click the **Update Password Now** button. The sub-screen will close and the focus is returned to the WS2000 Access screen.



**Note**

**NOTE:** If the administrative login password is lost or forgotten, please contact Symbol Technical Support for instructions on how to resolve the issue.

## 6.2 Configuring User Authentication

The WS2000 Wireless Switch provides an integrated RADIUS server as well as the ability to work with external RADIUS and LDAP servers to provide user database information and user authentication. Several screens are available to configure the how the RADIUS server authentication works as well as set up the local user database and access policies.

- The RADIUS Server screen allows the administrator to set the data source, the authentication type, and associate digital certificates with the authentication (see [Configuring the RADIUS Server](#)).
- The LDAP screen allows the administrator to set up communication with an external LDAP server (see [Configuring Lightweight Directory Access Protocol \(LDAP\) Authentication](#)).

### 6.2.1 Configuring the RADIUS Server

The WS2000 Wireless Switch provides an integrated RADIUS server as well as the ability to work with external RADIUS and LDAP servers to provide user database information and authentication. The RADIUS Server page allows the admin to set up data sources, as well as specify authentication information for the built-in RADIUS server.

Select **[System Configuration]** --> **[User Authentication]** --> **RADIUS Server** to set up the RADIUS server configuration.

The screenshot shows the 'RADIUS Server' configuration page in the WS2000 Wireless Switch management interface. The left-hand navigation tree is expanded to 'User Authentication' > 'Radius Server'. The main configuration area is divided into three sections:

- Data Source Configuration:** A pull-down menu for 'Data Source' is set to 'LOCAL'.
- EAP Configuration:** A sub-section titled 'TTLS/PEAP Configuration' contains:
  - Checkboxes for 'TLS' (checked), 'PEAP' (checked), and 'TTLS' (unchecked).
  - 'Default Auth Type' dropdowns: 'GTC' for PEAP and 'PAP' for TTLS.
  - 'Server Certificate' and 'CA Certificate' dropdown menus, both set to 'none'.
  - A 'Create DH Param File' button.
- Radius Client Authentication:** A table with columns 'Subnet/Host', 'Netmask', and 'Shared Secret'. The table is currently empty. Below the table are 'Add' and 'Del' buttons.

At the bottom of the configuration area are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The status bar at the very bottom shows 'System Name: DocWS2000'.

1. Use the Data Source pull-down menu to select the data source for the local RADIUS server.
  - If **Local** is selected, the internal User Database will serve as the data source. Use the User Database screen to enter the user data.
  - If **LDAP** is selected, the switch will use the data in an LDAP server. Configure the LDAP server settings on the LDAP screen under RADIUS Server on the menu tree.
2. Use the **TTLS/PEAP Configuration** check boxes to specify the EAP types for the RADIUS server. TLS is selected by default and EAP and TTLS are selectable options.
  - Protected EAP (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.

- Tunneled TLS EAP (EAP-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.
3. If PEAP is selected, specify a **Default Auth Type** for PEAP to use from the pull-down menu. The options are **GTC** and **MSCHAP-V2**.
    - EAP Generic Token Card (**GTC**) is a challenge handshake authentication protocol that uses a hardware token card to provide the response string.
    - Microsoft CHAP (**MSCHAP-V2**) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
  4. If TTLS is selected, specify a **Default Auth Type** for TTLS to use from the pull-down menu. The options are **MD5, PAP and MSCHAP-V2**.
    - Message Digest 5 (**MD5**) is a secure hash function which converts a long data stream into a fixed size digest. It uses a 128-bit hash value to do the conversion.
    - Password Authentication Protocol (**PAP**) is a protocol where the user sends an identifier and password pair to the server. This information is sent un-encrypted. It is used in case a remote server does not support stronger authentication protocols such as EAP or CHAP.
    - Microsoft CHAP (**MSCHAP-V2**) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
  5. If you have a server certificate from a CA and wish to use it on the RADIUS server, select it from this pull-down menu. Only certificates imported to the switch will be available in the menu. To create a server certificate, select the **Self Certificates** screen from Certificate Mgmt in the navigation menu (see [Creating Self Certificates](#)).
  6. You can also choose an imported CA Certificate to use on the RADIUS server. If using a server certificate signed by a CA, you will need to import that CA's root certificate using the CA certificates screen from the Certificate Mgmt menu. After a valid CA root certificate has been imported, it will be available from the **CA Certificate** pull-down menu.
  7. DH Param File is required to support Cipher Suite v 0x13 (TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA) for EAP-TLS/TTLS. If this file does not exist on a WS2000, it is automatically created when the device is booted up. Use **Create DH Param File** to create the file as and when required.
  8. Use the **RADIUS Client Authentication** table to set up multiple shared secrets based on the subnet or host that is trying to authenticate against the RADIUS server. Use the **Add** button to add entries to the list.

<b>Subnet/Host</b>	This field contains the IP address of the subnet or host that will be authenticating with the RADIUS server.
<b>Netmask</b>	This field contains the netmask (subnet mask) of the subnet or host that will be authenticating with the RADIUS server.
<b>Shared Secret</b>	Set a shared secret to be used for each host or subnet that will be authenticating against the RADIUS server. The shared secret can be up to 7 characters in length.

9. Click **Apply** to save your changes.



## 6.2.2 Configuring Lightweight Directory Access Protocol (LDAP) Authentication

When the RADIUS Data Source is set to use an external LDAP server (see [Configuring the RADIUS Server](#)), the LDAP screen is used to provide information about the external LDAP server. Select **[User Authentication] --> RADIUS Server --> LDAP**. The fields on this screen are only available when LDAP or LDAPS is set as the data source for the RADIUS server.

The screenshot shows the WS2000 Wireless Switch configuration interface. The left-hand navigation tree is expanded to show the following path: [Network Configuration] > [System Configuration] > [User Authentication] > RADIUS Server > LDAP. The main configuration area is titled 'LDAP Configuration' and contains the following fields:

- Fully Qualified Domain Name: [Text Input]
- LDAP Server IP: [IP Address Input: 0 . 0 . 0 . 0]
- Port: [Text Input: 636]
- CA Certificate: [Dropdown: none]
- Client Certificate: [Dropdown: none]
- Login Attribute: [Text Input: ie:-(User-Name)]
- Password Attribute: [Text Input: userPassword]
- Bind Distinguished Name: [Text Input: Manager,o=mobion]
- Password: [Text Input]
- Base Distinguished Name: [Text Input: o=mobion]
- Group Attribute: [Text Input: cn]
- Group Filter: [Text Input: es)(uniquemember=%{Ldap-UserDn})]
- Group Membership Attribute: [Text Input: radiusGroupName]

At the bottom right of the configuration area are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'DocWS2000' is displayed at the bottom left.

1. Fill out the LDAP Configuration area to allow the switch to work with the LDAP server. Consult with the LDAP server administrator for details on how to set the values for the fields in this screen.

<b>Fully Qualified Domain Name</b>	Enter the fully qualified domain name of the external LDAP server. This server will act as the data source for the RADIUS server. This server must be accessible from the WAN port or from an active subnet on the switch.
<b>LDAP Server IP</b>	Enter the IP address of the external LDAP server that will act as the data source for the RADIUS server. This server must be accessible from the WAN port or from an active subnet on the switch.
<b>Port</b>	Enter the TCP/IP port number for the LDAP server that will act as a data source. The default port is 389.
<b>Login Attribute</b>	Enter the login attribute used by your LDAP server for authentication. In most cases, the default value in this field should work.
<b>Password Attribute</b>	Enter the password attribute used by your LDAP server for authentication.
<b>Bind Distinguished Name</b>	Specify the distinguished name to bind with the LDAP server.
<b>Password</b>	Enter a valid password for the LDAP server.
<b>Base Distinguished Name</b>	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.
<b>Group Attribute</b>	Specify the group attribute used by your LDAP server.
<b>Group Filter</b>	Specify the group filters used by your LDAP server.

<b>Group Member Attribute</b>	Specify the Group Member Attribute to be sent to the LDAP server when authenticating the users.
-------------------------------	---

The following are the additional settings that are required for the LDAPS data source.

<b>Fully Qualified Domain name</b>	Enter the fully qualified domain name of the LDAP server that provides authentication information to your RADIUS server.
<b>CA Certificate</b>	Specify the CA certificate used for authentication.
<b>Client Certificate</b>	Specify the client certificate used for authentication.

2. Click **Apply** to save your changes.

### 6.2.3 Setting Up a Proxy RADIUS Server

The WS2000 Wireless Switch provides the capability to proxy authentication requests to a remote RADIUS server based upon the suffix of the user ID (such as myisp.com or company.com). Select **[User Authentication] --> RADIUS Server --> Proxy** to go to the RADIUS Proxy Configuration screen is where the definitions of proxies are made.

The screenshot shows the 'Proxy Configuration' screen in the WS2000 Wireless Switch configuration utility. The left-hand navigation pane is expanded to 'User Authentication' > 'Radius Server' > 'Proxy'. The main configuration area is divided into two sections: 'Proxy Configuration' and 'Proxy Server Settings'. In the 'Proxy Configuration' section, there are two input fields: 'Retry Count' with a value of 3 (range 3-6) and 'Timeout' with a value of 5 (range 5-10) seconds. The 'Proxy Server Settings' section contains a table with the following columns: Suffix, RADIUS Server IP, Port, and Shared Secret. Below the table are 'Add' and 'Del' buttons. At the bottom of the screen are 'Apply', 'Undo Changes', 'Help', and 'Logout' buttons. The system name 'DocWS2000' is displayed at the bottom left.

Up to 10 proxy servers are supported.

1. Enter a value between 3 and 6 in the **Retry Count** field to indicate the number of times the switch attempts to reach a proxy server before giving up.
2. Enter a value between 5 and 10 in the **Timeout** field to indicate the number of elapsed seconds that will cause the switch to time out on a request to a proxy server.
3. Use the **Add** button to add a new entry based upon a domain suffix to the Proxy Server Settings area. Then fill in the following information for each entry:

<b>Suffix</b>	Enter the domain suffix (such as myisp.com or mycompany.com) of the users to be sent to the specified proxy server.
<b>RADIUS Server IP</b>	Enter the IP address of the RADIUS server that will be acting as a proxy server.

<b>Port</b>	Enter the TCP/IP port number for the RADIUS server that will be acting as a proxy server. The default port is 1812.
<b>Shared Secret</b>	Set a shared secret to be used for each suffix that will be used for authentication with the RADIUS proxy server.

4. Click **Apply** to save changes.

To delete a server row, select the row corresponding to that entry and click the **Del** (Delete) button.



**Note**

**NOTE:** If you are using a proxy server for RADIUS authentication, the Data Source field on the RADIUS Server screen (*Configuring the RADIUS Server*) must be set to Local. If it is set to LDAP, the proxy server will not be successful when performing the authentication.

## 6.2.4 Managing the User Database

The *User Database* screen is used to create users and groups for the local RADIUS server. This database is used when **Local** is selected as the **Data Source** from the RADIUS Server screen. The information in the database is ignored if an LDAP server is used for user authentication. Select **[User Authentication]** --> **User Database** to maintain the user entries.

Groups	Guest	VLAN ID	Start Time	End Time	Day Access
GroupOfAdmins	<input type="checkbox"/>	1	0000	2359	Mo,Tu,We,Th,Fr,Sa,Su
GroupOfLevel1Users	<input type="checkbox"/>	1	0000	2359	Mo,Tu,We,Th,Fr,Sa,Su
GroupOfLevel2Users	<input type="checkbox"/>	1	0000	2359	Mo,Tu,We,Th,Fr,Sa,Su
GroupOfGuestUsers	<input checked="" type="checkbox"/>	1	0000	2359	Mo,Tu,We,Th,Fr

Each user that is created is assigned their own password and is associated with one or more groups. Each group can be configured for its own access policy on the Access Policy configuration screen under the RADIUS Server menu.

### 6.2.4.1 Adding Groups

This Groups table displays a list of all groups in the local RADIUS server's database. The groups are listed in the order that they are added. Although groups can be added and deleted, there is no capability currently to edit the name of a group.

1. To add a new group, click the **Add** button and enter the name of the group in the new blank field in the table.

2. To set a group as a group of Guest users, click the check box in the **Guest** column, next to the Groups field.
3. To enable a group access to a particular VLAN, enter the ID in the **VLAN ID** field for the group.
4. To restrict access to set times, enter the appropriate time values in "hhmm" (24 hours) format. Enter the access start time and end time in the **Start Time** and **End Time** fields respectively.
5. To restrict access to set days in a week, select the appropriate week days from a dialog box that appears when the **Day Access** field is clicked.
6. Click **Apply** to save the changes.

### 6.2.4.2 Deleting Groups

To remove a group, select that group from the table and click the **Del** (Delete) key. A warning message will appear when you apply the change if there are users still assigned to the group. You can then remove the group from each user or add the group back to the group list.

### 6.2.4.3 Adding Users

The Users table displays the entire list of users. Up to 100 users can be entered here. The users are listed in the order that they are added. Though users can be added and deleted, there is no capability at present to edit the name of a group.

1. To add a new user, click the **Add** button at the bottom of the Users area.
2. In the new line, type a **User ID** (username).
3. Click the **Password** cell. A small window will appear. Enter a password for the user and then click **OK** to return to the User Database screen.
4. Click the **Guest** check box to make a User ID as a guest user. The **Start Date** and **Expiry Date** fields are enabled.
  - a. Click the **Start Date** cell. A dialog box appears where you can enter the date from when the user can access the network.
  - b. Click the **Expiry Date** cell. A dialog box appears where you can enter the date after which the user cannot access the network.
5. Click the **List of Groups** cell. A new screen appears that lets you associate groups with the user. A user must belong to at least one group for them to have access to the switch. When a User ID is of the type *Guest*, this list will display a list of Guest User Groups.
  - To add the user to a group, select the group in the **Available** list (on the right) and click the **<-Add** button.
  - To remove the user from a group, select the group in the **Assigned** list (on the left) and click the **Delete->** button.

Click **OK** when you are done.

6. Click **Apply** to save your changes.

## 6.2.5 Adding New Guest Users Quickly

The WS2000 also enables the administrators to add a guest user quickly. A separate screen is provided outside of the normal administrative environment for this purpose. To add a new guest user quickly:

1. Use the user name **guest** and the password **symbol** to access the switch. The **Guest User Creation** screen is displayed.

WS2000 Wireless Switch

### Guest User Creation

User Name

Password

User Group

Expiry Date

Date

Expiry Date  dd:mm:yyy

Expiry Time  hh:mm

Preset Values

System Name: TECHDOCSW

When you logon with the **guest** user name for the first time, you are forced to change the default password. Use the *Change Admin/Manager/Guest Admin Password* dialog to change the default password.

WS2000 Wireless Switch

Username:

Password:

Release 2.4

**Change Admin/Manager/Guest Admin Password**

For security purposes please change the administrator password.  
You are not allowed to keep the default password.

Enter New Password ( up to 11 chars ):

Re-Type New Password ( up to 11 chars ):

Java Applet Window



#### Note

**NOTE:** Before this screen is used to create a guest user, there must be at least one guest user group configured on the switch. To create a guest user group, see section [Adding Groups](#).

To create a guest user:

1. Enter the required username in the **User Name** text box. You can also generate a random username. To generate a random username, click the **User Generate** button. An 8 character username is generated.

2. Enter the required password in the Password text box. You can also generate a random password. To generate a random password, click the **Password Generate** button. A 10 character long password is generated.
3. Select the User Group the new user will belong to. Click on **User Group** to display a list of guest user groups. Select the appropriate guest user group.
4. Two options are available to set the life of the new guest user. You can choose to enter the expiry date and time or select a preset duration after which the user login expires.

To set a preset time for login expiry, select **Preset Values** option. A list with a range of preset values is enabled. Select the appropriate value from the list.

To set a particular date and time when the login expires, select **Date** option. The **Expiry Date** and **Expiry Time** text box are enabled. Enter the date on which the login expires in the format dd:mm:yyyy in the **Expiry Date** box. Similarly, enter the time on which the login expires in the format hh:mm in the **Expiry Time** box.

5. Click **Apply** to create the new user. Or, click **Undo Changes** to revert back the changes made to this screen.

To create multiple users, repeat the above steps and click **Apply** to create each user.



**NOTE:** RADIUS guest user accounts are removed from the database 24 hours after the user account's validity period expires.

**Note**

### 6.2.5.1 Printing Guest User Account Information

To provide each guest user details about their user account, use the print feature. This feature is provided

To print a guest account's details:

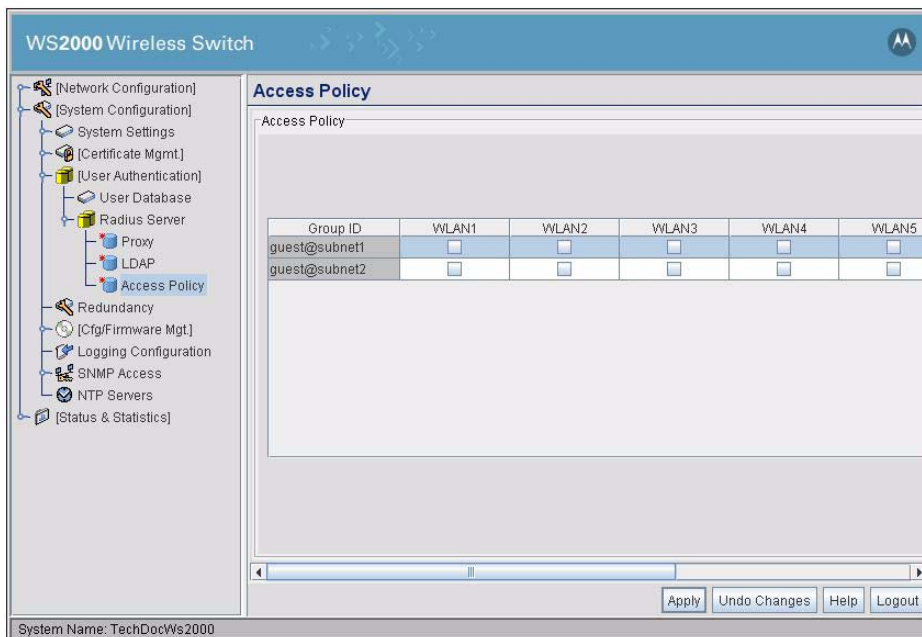
1. Click **Print**. The *PRINT* dialog appears.
2. From the **Select the User to print** drop down list, select the user to print information for. The user information is displayed in the *PRINT* dialog.



3. Click **Print**. The user information is printed. You can then provide this information to the user for reference.

## 6.2.6 Setting the User Access Policy

The RADIUS Access Policy screen allows you to set WLAN access based on a user group defined on the User Database screen. Select **[User Authentication]** --> **RADIUS Server** --> **Access Policy** to set group access.



Each Group ID defined in the User Database screen appears on the Access Policy screen as a single row in the table. Each wireless LAN represents a column in the table.

1. To enable group access to a particular WLAN, check the box for that WLAN in the row corresponding to the group. To disable access for a group, uncheck the box for the appropriate WLAN. A group must have at least one WLAN checked to have wireless access to the switch.
2. Click **Apply** when you have finished the changes.

## 6.3 Managing Digital Certificates

A digital certificate is an electronic identification card that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains a name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

The WS2000 Wireless Switch uses digital certificates for VPN access authentication and user authentication. The application provides two mechanisms for defining/importing digital certificates:

- CA certificates are those that a CA creates and signs with its own private key. These certificates are imported into the switch CA certificate library. (See [Importing CA Certificates](#) for directions.)
- Self certificates are those that an organization creates a certificate request, sends it off to a Certificate Authority (CA) to be signed, and then imports the signed certificate into the management system. (See [Creating Self Certificates](#) for directions.)

### 6.3.1 Importing CA Certificates

A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates that it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its "Trusted Root Library" so that it can trust certificates "signed" by the CA's private key.

Depending on the public key infrastructure implementation, the digital certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

The WS2000 Management System provides the means to import and maintain a set of CA certificates to be used as an authentication option for VPN access. To use the certificate for a VPN tunnel, define a tunnel and select the IKE settings to use either RSA or DES certificates.

Before you import a certificate, you need to get one. Ask a CA for a certificate. They will typically send you the certificate information in an email message. You will need to import the content of the message into the WS2000 Network Management System.



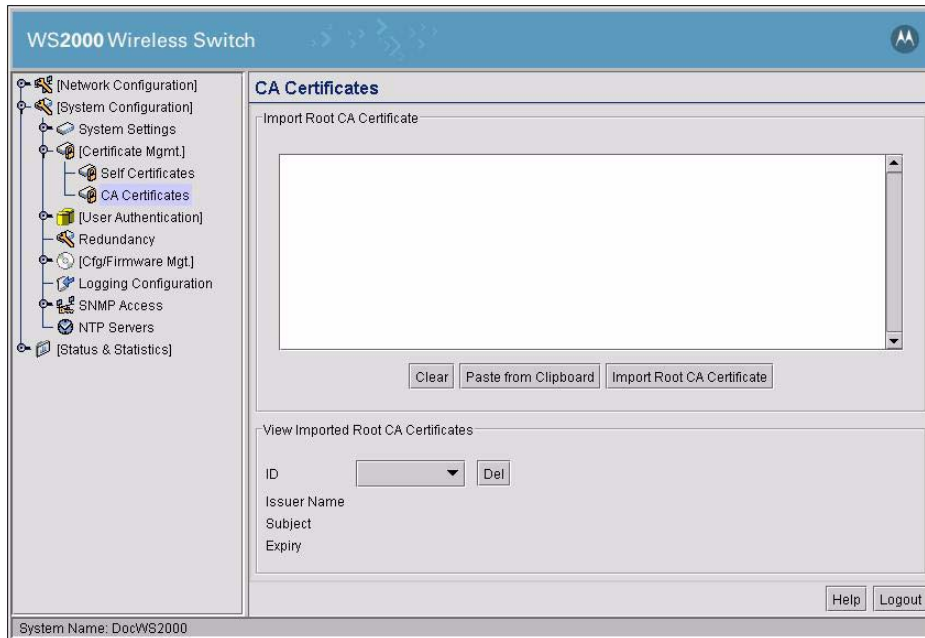
**Note**

**NOTE:** Make sure that the WS2000 is time synchronized with an NTP server before importing a certificate to avoid issues with conflicting date/time stamps.



To import a CA certificate perform the following steps:

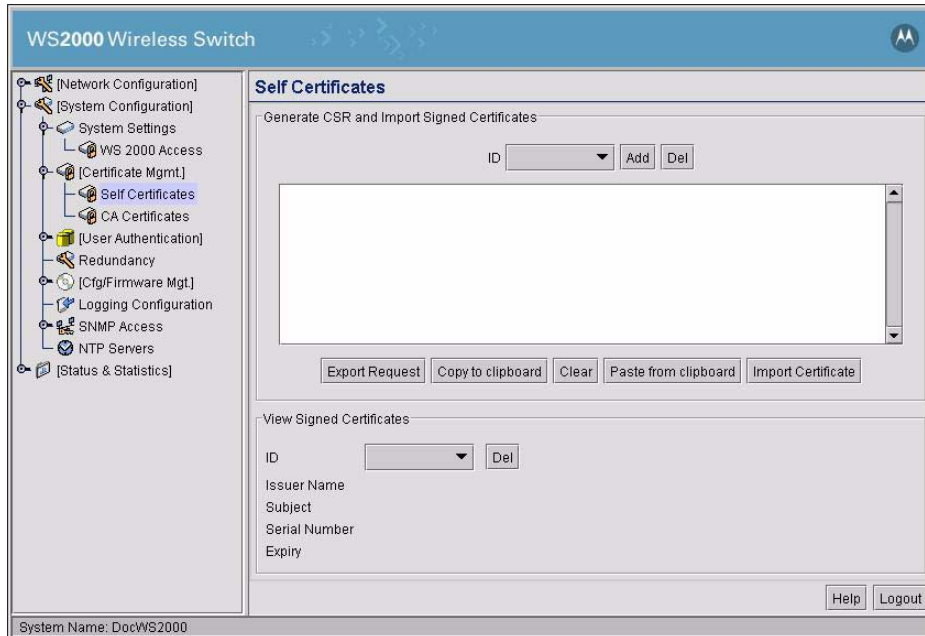
1. Select **System Configuration** --> **Certificate Mgmt** --> **CA Certificates** from the left menu. The following screen appears.



2. Copy the content of the CA Certificate message into the clipboard and then click **Paste from Clipboard**. The content of the certificate will appear in the **Import Root CA Certificate** area.
  3. Click the **Import Root CA Certificate** button to import it into the CA Certificate list.
  4. Once in the list, select the certificate ID from the **View Imported CA Certificates** area to view information, such as the issuer name, subject, serial number, and data that the certificate expires.
  5. Click the **Apply** button to save changes.
- To delete a certificate, select the Id from the menu and then click the **Del** (Delete) button.

## 6.3.2 Creating Self Certificates

Self certificates are those for which the organization creates a certificate request, sends it off to a Certificate Authority (CA) to be signed, and then imports the signed certificate into the management system. To go through this process, select **System Configuration--> Certificate Mgmt --> Self Certificates**.



1. To create the certificate request, click the **Add** button. The Certificate Request screen appears.

2. Fill out the request form with the pertinent information. Only 4 fields are required:

<b>Key ID</b>	Enter a name for the certificate to help distinguish between certificates. The name can be up to 7 characters in length.
<b>Subject</b>	This required field contains important information about the certificate. Contact the CA that will sign the certificate to determine the content of this field.

<b>Signature Algorithm</b>	Indicate the signature algorithm to use for the certificate. The selection should match the VPN tunnel settings. <ul style="list-style-type: none"> <li>• <b>MD5-RSA</b>: Message Digest 5 algorithm in combination with RSA encryption.</li> <li>• <b>SHA1-RSA</b>: Secure Hash Algorithm 1 in combination with RSA encryption.</li> </ul>
<b>Key Length</b>	Indicate the desired length of the key. Possible values are 512, 1024, and 2048.

3. Fill in as many of the optional fields as desired or as required by the CA that will sign the certificate. The contact information is for the organization who is making the certificate request. The less obvious fields are:

<b>Email</b>	Enter the email address to be used for identification purposes. Typically a CA requires either an email address, a domain name, or an IP address for identification purposes.
<b>Domain Name</b>	Enter the domain name to associate with the certificate. This field is often required by the CA.
<b>IP Address</b>	Enter the WAN IP of the WS2000 Wireless Switch. Check with your CA to determine whether this information is necessary. Often it can be omitted if either the email or domain name information is provided.

4. When finished filling out the form, click **Generate**. The Certificate Request screen disappears and the ID of the certificate request that was just generated will appear in the Requests ID list of the Self Certificates window.
5. Click the **Export Request** button. The generated certificate request appears in the large text box.
6. Click **Copy to Clipboard** and the content of request to be sent to the CA will be copied to the clipboard.
7. Create an email to your CA, paste the content into the body of the message, and send it to the CA.
8. The CA will “sign” the certificate and send it back. At this point, copy the content from the email onto the clipboard. Then, click the **Paste from Clipboard** button and the content of the email will be displayed in the window.
9. Click the **Import Certificate** button to import the certificate and make it available for use as a VPN authentication option. The certificate ID will appear in the Signed list, where you can view information about it.
10. **Apply** your changes.

To use the certificate for a VPN tunnel, first define a tunnel and select the IKE settings to use either RSA or DES certificates.



**Note**

**NOTE:** Note: If the switch is rebooted after a certificate request has been generated but before the signed certificate is imported, the import will not execute properly. Please do not reboot the switch during this interval.



## ***Switch Administration***

7.1 Overview of Administration Support .....	7-2
7.2 Restarting the Wireless Switch .....	7-2
7.3 Changing the Name of the Switch .....	7-3
7.4 Changing the Location and Country Settings of the .....	7-3
7.5 Configuring the DNS Server Information .....	7-4
7.6 Configuring the Domain Name for the switch .....	7-5
7.7 Configuring Switch Redundancy .....	7-6
7.7.1 Setting Up Switch Redundancy .....	7-6
7.7.2 Redundancy Operations Status .....	7-7
7.8 Updating the Wireless Switch's Firmware .....	7-7
7.8.1 Checking for and Downloading Firmware Updates .....	7-7
7.8.2 Performing the Firmware Update .....	7-8
7.8.3 Formatting a Compact Flash Card .....	7-9
7.8.4 Limitation of File System on the Compact Flash Card .....	7-9
7.8.5 Setting Up DHCP Options for Firmware Upload .....	7-9
7.9 Exporting and Importing Wireless Switch Settings .....	7-11
7.9.1 To Import or Export Settings to an FTP or TFTP Site .....	7-11
7.9.2 Sample Configuration File .....	7-13
7.10 Updating Sensor Firmware .....	7-47
7.10.1 Setting Sensor Firmware Update Information .....	7-47
7.10.2 Updating the Sensor Firmware .....	7-48
7.11 Configuring SNMP .....	7-48
7.11.1 Setting the SNMP Version Configuration .....	7-49
7.11.2 Setting Up the Access Control List .....	7-51
7.11.3 Setting the Trap Configuration .....	7-51
7.11.4 Setting the Trap Configuration for SNMP v1/v2c .....	7-51
7.11.5 Setting the Trap Configuration for SNMP V3 .....	7-52
7.11.6 Selecting Traps .....	7-52
7.11.7 Setting RF Traps .....	7-55
7.12 Specifying a Network Time Protocol (NTP) Server .....	7-56
7.13 Setting Up and Viewing the System Log .....	7-58
7.13.1 Viewing the Log on the Switch .....	7-58
7.13.2 Setting Up a Log Server .....	7-58
7.14 Commands to unmount a CF card .....	7-59

## 7.1 Overview of Administration Support

The WS2000 Network Management System provides several screens for administering the switch and monitoring activity on the switch. From the interface the administrator can:

- Change the general system settings, such as the name of the switch and the location of the switch
- [Restart the switch](#)
- [Restore factory settings](#)
- [Export or import the switch's configuration settings](#)
- [Find and install firmware updates](#)
- [Change the settings for who can access the switch for administration purposes](#)
- [Configure how log files are saved](#)
- View system statistics for [WAN communication](#), [subnets](#), [WLANS](#), [Access Ports](#), and [mobile units](#)

## 7.2 Restarting the WS2000 Wireless Switch

During the normal course of operations, the administrator might need to restart or reset the switch. For example, changing certain configuration settings can require restarting the switch for those settings to take effect. To restart the WS2000:

1. Select **System Configuration** --> **System Settings** from the left menu.-

The screenshot shows the 'System Settings' page of the WS2000 Wireless Switch. The left sidebar contains a navigation tree with the following items: [Network Configuration], [System Configuration], [System Settings] (selected), [WS 2000 Access], [Certificate Mgmt], [User Authentication], Redundancy, [Cfg/Firmware Mgt], Logging Configuration, [SNMP Access], [NTP Servers], and [Status & Statistics]. The main content area is titled 'System Settings' and contains the following fields:

- System Name: WS2000 Switch
- System Location: Doc Team Area
- Domain Name: docteam.motorola.com
- Admin Email Address: (empty)
- DNS Server IP Address: 192 . 168 . 0 . 1
- Country: United States - us (dropdown menu)
- WS 2000 Version: 2.4.0.0-018B
- System Uptime: 15 days 22 hours 56 minutes
- Hardware Address: 00:15:70:00:C2:10

Below the fields are two sections: 'Factory Defaults' with buttons for 'Restore Default Configuration' and 'Restore Partial Default Configuration', and 'Restart WS 2000' with a 'Restart WS 2000' button. At the bottom of the page are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The status bar at the very bottom shows 'System Name: WS2000 Switch'.

2. Click the **Restart** button to restart the switch. A second window appears, asking for confirmation.
3. Select the **Restart** button. Upon confirming the restart, the switch reboots. Typically, normal communications with the switch are restored within a minute or two.

## 7.3 Changing the Name of the Switch

When the administrator first logs into the WS2000 Network Management System, the System Settings screen appears. One of the fields in this screen is the System Name field. In this field, the administrator can specify the name of the switch. This name is used to distinguish the switch from others that are on the network and it is also used to set the device name in SNMP.

To examine and change the current name for the switch:

1. Select **System Configuration** --> **System Settings** from the left menu.

2. Find the **System Name** field and type a string of alphanumeric characters to create a name.
3. Select the **Apply** button to save the change.

## 7.4 Changing the Location and Country Settings of the WS2000

When the administrator first logs into the WS2000 Network Management System, the System Settings screen appears. One of the fields in this screen is the Country field. This field is set to the country in which the switch is installed. Setting this field appropriately ensures compliance with national and local laws concerning electromagnetic emissions and the power level of Access Port radio transmissions.

To examine and change the location setting for the switch:

1. Select **System Configuration** --> **System Settings** from the left menu.

The screenshot displays the 'System Settings' page for a WS2000 Wireless Switch. The left-hand navigation pane includes options such as [Network Configuration], [System Configuration], [System Settings], WS 2000 Access, [Certificate Mgmt], [User Authentication], Redundancy, [Cfg/Firmware Mgt], Logging Configuration, SNMP Access, NTP Servers, and [Status & Statistics]. The 'System Settings' section is active, showing the following configuration details:

- System Name: WS2000 Switch
- System Location: Doc Team Area
- Domain Name: docteam.motorola.com
- Admin Email Address: (empty field)
- DNS Server IP Address: 192 . 168 . 0 . 1
- Country: United States - us (dropdown menu)
- WS 2000 Version: 2.4.0.0-018B
- System Uptime: 15 days 22 hours 56 minutes
- Hardware Address: 00:15:70:00:C2:10

At the bottom of the settings area, there are two sections: 'Factory Defaults' with buttons for 'Restore Default Configuration' and 'Restore Partial Default Configuration', and 'Restart WS 2000' with a 'Restart WS 2000' button. A status bar at the very bottom indicates 'System Name: WS2000 Switch'. At the bottom right of the main content area are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'.

2. Type in a description of the physical location of the switch within your facility into the **Location** field.
3. Find the **Country** field and use the drop down menu to select the correct country from the list.
4. Click **Apply** to save changes. The interface asks you to confirm any changes you make to the **Country** selection.

## 7.5 Configuring the DNS Server Information

The DNS Server is used by the Network Time Protocol (NTP) feature to synchronize the switch time with time servers on the world wide web. This enables switches in the network to maintain the same time. The DNS Server IP address is used by the NTP to resolve addresses of the time servers.

To provide the DNS server information,

1. Select **System Configuration** --> **System Settings** from the left menu.



WS2000 Wireless Switch

**System Settings**

WS 2000 System Settings

System Name: WS2000 Switch

System Location: Doc Team Area

Domain Name: docteam.motorola.com

Admin Email Address:

DNS Server IP Address: 192 . 168 . 0 . 1

Country: United States - us

WS 2000 Version: 2.4.0.0-018B

System Uptime: 15 days 22 hours 56 minutes

Hardware Address: 00:15:70:00:C2:10

Factory Defaults

Restart WS 2000

Restore Default Configuration

Restore Partial Default Configuration

Restart WS 2000

Apply Undo Changes Help Logout

System Name: WS2000 Switch

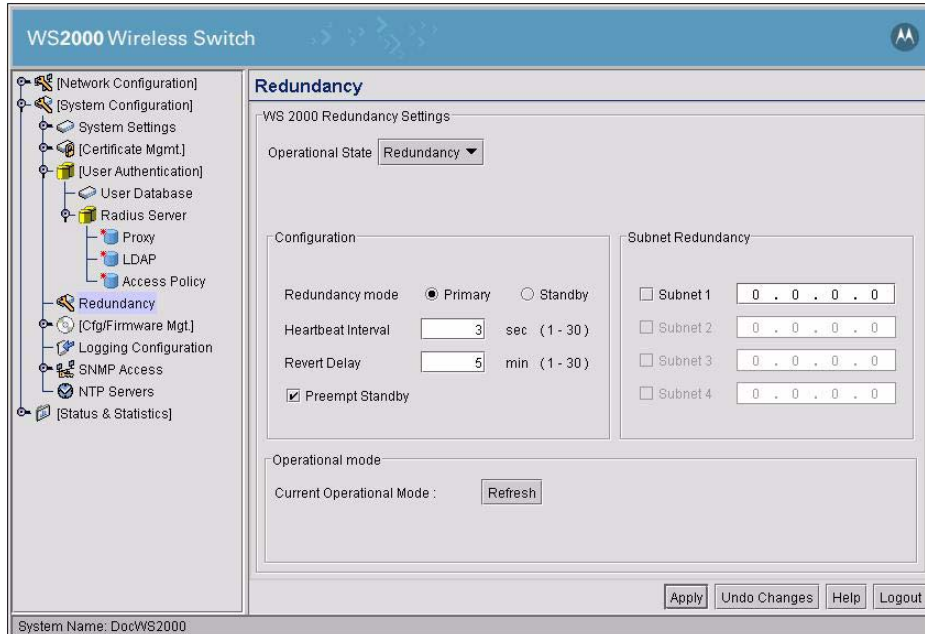
2. Enter the IP address of the DNS server in the **DNS Server IP Address** field.
3. Click **Apply** to save changes.

## 7.6 Configuring the Domain Name for the switch

The **Domain Name** field provides domain information for reverse DNS queries. The name of the WS2000 as entered in the **System Name** field and the device's domain name as entered in the **Domain Name** field is returned for the reverse DNS query.

## 7.7 Configuring Switch Redundancy

The WS2000 Wireless Switch supports redundancy between two WS2000 Wireless Switch, allowing a standby switch to take over if the primary switch stop responding. Use the WS2000 Redundancy settings to configure the Operational State and Redundancy Mode for the switch.



### 7.7.1 Setting Up Switch Redundancy

For each of the two switches, use the following procedure to set up redundancy.

1. Choose the redundancy mode in which the WS2000 Wireless Switch will operate in.

<b>Stand-alone</b>	The switch has no redundancy capabilities and operates independently of any other WS2000 switches on the network. This is the default setting.
<b>Redundancy</b>	Two WS2000 switches are connected, with one set as a primary and the other as a standby. The primary switch will send heartbeat packets to the specified port of the standby switch at a specified interval. If the standby switch doesn't receive a heartbeat packet in a specified amount of time, it will take over as the primary switch.

2. When redundancy is selected as the operational state, specify whether the current switch is the primary or standby switch by selecting the appropriate **Redundancy mode** radio button.
3. When redundancy is selected as the operational state, in the **Heartbeat Interval** field specify the amount of time between heartbeat packets being sent or received between the two switches.
4. When redundancy is selected as the operational state, in the **Revert Delay** field specify the amount of time after not receiving a heartbeat packet before the standby switch will take over.
5. When redundancy is selected as the operational state, check the **Preempt Standby** box to prevent system standby on the redundant switches.
6. Click the check boxes in the **Subnet Redundancy** to select which subnets are enabled for redundancy.
7. Click **Apply** to save changes.

## 7.7.2 Redundancy Operations Status

To see the Operational Mode status for switch redundancy, look at the bottom of the Redundancy screen. Click the **Refresh** button to update the **Operational Mode** status.

## 7.8 Updating the WS2000 Wireless Switch's Firmware

From time to time, Motorola releases updates to the WS2000 Wireless Switch's firmware. These updates include:

- Information about how to communicate with newly released Access Ports
- Updates for security issues that have been identified
- Fixes to any software problems that have been identified

### 7.8.1 Checking for and Downloading Firmware Updates

The switch administrator should check for firmware updates for the WS2000 Wireless Switch on a monthly basis, as follows:

1. Select **System Configuration --> Cfg/Firmware Mgt. --> Firmware Update** from the menu on the left.

The screenshot shows the 'Firmware Update' configuration page for a WS2000 Wireless Switch. The left sidebar contains a tree view with 'Firmware Update' selected. The main content area is titled 'Firmware Update' and contains the following fields and controls:

- Update Firmware** section:
- WS 2000 Version: 2.4.0.0-018B
- Filename:
- Filepath(optional):
- Boot Device:
- CF Active Partition:
- Get Firmware file from:
- FTP Server on 
  - IP Address:
  - Username:
  - Password:
- TFTP Server on 
  - IP Address:
- CF Card
  - 
  -
- 
- Status:
- Buttons at the bottom:

2. Examine the **Version** field to record the version number of the currently loaded software. It should be something like 2.0.0.0-20
3. Go to the web site <http://www.symbol.com/services/downloads/> and select the link to the WS2000 Wireless Switch.
4. Compare the WS2000 Version value with the most recent version listed on the site. All updates will be listed along with a description of what the update contains.
5. Check to see if an administrator has already downloaded the file. It might already be on an FTP server at the site. If not, download the update from <http://www.symbol.com/services/downloads/>. Put the file on

an FTP server, on a system with a TFTP server, or on a CompactFlash card that is compatible with the switch.

## 7.8.2 Performing the Firmware Update

To perform the update, the update file must be available from an FTP or TFTP site, or it must be on the CompactFlash card in the CF slot of the switch. The administrator supplies the site information and the WS2000 Network Management System will perform the update for the administrator.

1. Save the WS2000 Wireless Switch's current configuration settings (**System Configuration** --> **Config Import/Export**)
2. Select **System Configuration** --> **Firmware Update** from the left menu to view the Firmware Update screen.
3. Specify the **Filename** of the firmware file with the update (such as WS\_22343.bin).
4. Specify the **Boot Device** for the WS2000. The WS2000 boots from the selected Boot Device. Select the option from one of *Onboard Flash* or *CF Card*.
5. Specify a folder pathname for an FTP login, if necessary.
6. Select one of the **FTP**, **TFTP**, or **CP Card** radio buttons, as appropriate.

### If FTP is selected:

1. Specify whether the FTP server is on the WAN or is on one of the subnets associated with the switch by selecting the appropriate choice from the **FTP Server on** drop-down menu to the right of the radio button.
2. Specify the **IP Address** of the FTP server that has the update.
3. Specify a **Username** and **Password** that will allow the FTP login and access to the file.

### If TFTP is selected:

1. Specify whether the TFTP server is on the WAN or is on one of the subnets associated with the switch by selecting the appropriate choice from the **TFTP Server on** drop-down menu to the right of the radio button.
2. Specify the **IP Address** of the TFTP server that has the update.



**Note**

**NOTE:** When using TFTP as the upgrade method, be sure the TFTP server you are using supports files larger than 16MB. The WS2000's firmware files are over 20MB in size and will cause the upgrade to fail if your TFTP server does not support files larger than 16MB.

### If CF Card is selected:

1. Click the **Display CF** button to open a dialogue where you can browse the Compact Flash card's file system to find or verify the firmware file and path.  
Click the **Format CF** button to format the compact flash card before storing the firmware file on it.

### To complete the update:

1. Click the **Perform Update** button to initiate the firmware update for the switch. The update process will take a few minutes.

2. After the switch reboots, return to the **Firmware Update** screen. Read the **Status** field to verify that the firmware update completed successfully. The **Version** number at the top of the screen should have been updated.
3. Confirm that the wireless switch's configuration settings are the same as prior to the update. If not, restore the settings.

### 7.8.3 Formatting a Compact Flash Card

If you need to erase the contents of a Compact Flash card you can do so on the **Firmware Update** screen.



**WARNING! Formatting a Compact Flash card will erase all data on the card. There is no undo option for formatting cards. Be sure that you do not need any data on the Compact Flash card before formatting it.**

To format a Compact Flash card:

1. Navigate to **System Configuration--> Cfg/Firmware Mgt--> Firmware Update** screen.
2. Verify that the Compact Flash card is firmly seated in the WS2000's Compact Flash slot.
3. Click the **Format CF** button.
4. Click **Yes** to continue formatting the card.



**WARNING! Sometimes you might encounter an issue with mounting CF cards that have been formatted on a Windo/XP machine. To resolve this issue, reset the WS2000 with the CF card inserted. Go to the boot prompt. From the boot prompt enter the following commands:**

```
cf fill 0 0
cf fill 100 0
cf fill 200 0
```

**You can then take the card and format it using a Windows machine using FAT32.**

**Any card formatted on a Linux machine does not have this issue.**

### 7.8.4 Limitation of File System on the Compact Flash Card

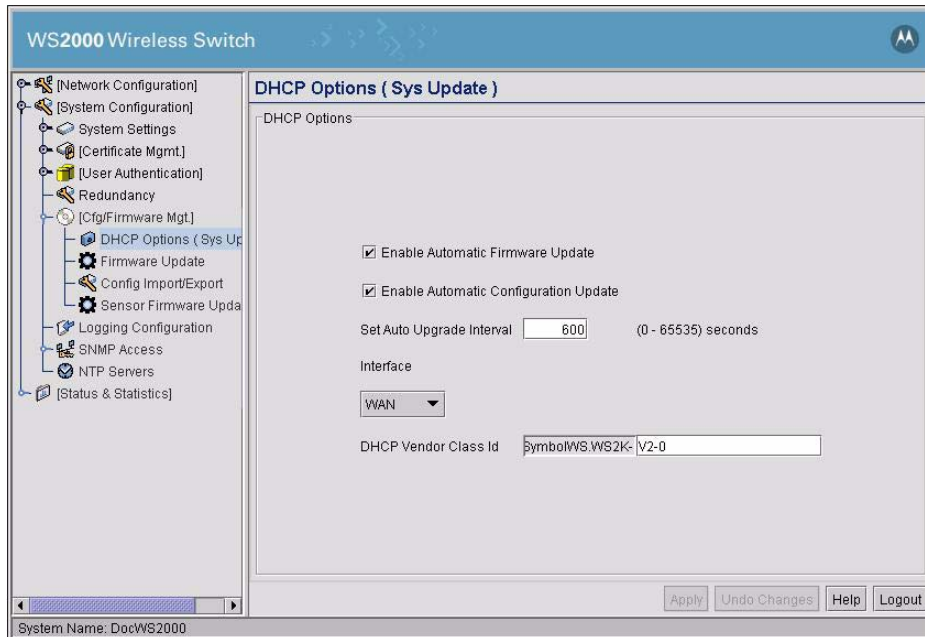
The Compact Flash (CF) card uses VFAT (FAT16) file system. This file system can at the most support 512 root directory entries, where each directory entry can either be a file or a folder (directory). If long file names are used (other than xxxxxxxx.xxx (<filename>.<ext>) format), then the number of entries are less than 512. Once the limit of 512 is reached, no more files or directories can be added.

If the 512 entry limit is reached, it can be overcome by deleting a file and creating a folder (directory). However, it is suggested to keep number of files or folders (directories) in the root folder of the CF card low. The limit of 512 entries is applicable to every directory created.

### 7.8.5 Setting Up DHCP Options for Firmware Upload

It is also possible to configure the switch to receive firmware and configuration files automatically from a server using the Dynamic Host Configuration Protocol (DHCP). This feature allows quick and automatic rollouts of new configurations or firmware updates across the network without manually updating each switch.

Select **[System Configuration]** --> **[Cfg/Firmware Mgt]** --> **DHCP Options (Sys Update)** to configure the switch to accept DHCP downloads.



### 7.8.5.1 Setting Up the Switch

1. Check **Enable Automatic Firmware Update** to allow the WS2000 Wireless Switch to automatically receive firmware updates from a server using the DHCP protocol. By default this option is disabled.
2. Check **Enable Automatic Configuration Update** to allow the WS2000 to automatically receive configuration file updates from a server using DHCP. By default this option is disabled.
3. Set the **Auto Upgrade Interval** (in seconds) for the WS2000 to check the server for automatic updates.
4. Use the **Interface** menu to select the interface from which Firmware and Configuration updates will be received. This interface can be either the WAN port or any of the configured subnets on the switch. By default this value is set to **WAN**.
5. Optional: If you wish to change or specify a **DHCP Vendor Class Id** enter it here.

**DHCP Vendor class ID** is used by the onboard DHCP clients as a unique identifier for Firmware/Config upgrade parameters. The external DHCP server which handles the DHCP client needs to be configured with this option to provide TFTP/FTP server IP, firmware file name and config file to facilitate WS2000 for Auto FW/Config upgrade. Any string provided in the text field will be prefixed with a "SymbolWS.WS2K" string.

6. Navigate to the **Firmware** or **Config Import/Export** screen depending on whether you are setting up the automatic firmware download or configuration settings download. Set the TFTP server IP address to the IP address of the server what will do the download. Also set the name of the file to download.

### 7.8.5.2 Setting Up the DHCP Server

The external DHCP server will also needs to be configured appropriately. On a Windows server, you will need to select the appropriate options in the server setup. For a Linux server, edit the /etc/dhcpd.conf file to have the appropriate settings.

## 7.9 Exporting and Importing Wireless Switch Settings

All of the configuration settings for the WS2000 Wireless Switch can be saved to a configuration file and then either imported back into the same switch or transferred to another switch. This file-based configuration saving feature provides several benefits:

- It can speed the switch setup process significantly at sites using multiple WS2000 wireless switches.
- It allows an administrator to “backup” the current switch configuration before making significant changes, before restoring the default configuration, or for precautionary measures.

Select **[System Configuration]** --> **[Cfg/Firmware Mgt]** --> **Config Import/Export** from the left menu to import or export the switch configuration settings.

The screenshot shows the 'Config Import/Export' window for a WS2000 Wireless Switch. The left sidebar contains a tree view with 'Config Import/Export' selected. The main area is titled 'Config Import/Export' and is divided into three sections:

- FTP and TFTP Import/Export:** This section contains fields for 'Server Options' (Filename: cfg.txt, Server IP: 192.168.0.100, Username: root, Password: #####, Filepath(optional):, Bind Interface: None) and buttons for 'Import' (Default Before Applying, Get from server and Apply the file -> FTP Import, TFTP Import) and 'Export' (Generate and Put the file onto server -> FTP Export, TFTP Export).
- HTTP Import/Export:** This section contains buttons for 'Import' (1.) Upload A File, 2.) Apply Uploaded File and 'Export' (1.) Generate File, 2.) Download File.
- Status:** This section shows a message: [5] File transfer failed.

At the bottom of the window, there are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'WS2000' is visible at the bottom left.

### 7.9.1 To Import or Export Settings to an FTP or TFTP Site

Use the Config Import/Export screen to provide information used to import or export WS2000 switch configuration settings. This screen is divided into areas that take settings for importing and exporting configuration using FTP/TFTP and HTML.

Import or Export settings u

#### Export/Import configuration settings using FTP/TFTP

To import or export configuration settings using FTP/TFTP:

1. Enter the name of the file used to import or export configuration in the **Filename** field.
2. Enter the IP address of the server where the file is exported to or imported from in the **Server** field.
3. Enter the user name of the account in the **Username** field that is used to access the FTP/TFTP server specified in the **Server** field.
4. Enter the password in the **Password** field. This is for the user account in **Username** field and is used to access the FTP/TFTP server.
5. Enter the fully qualified path to the file on the FTP/TFTP server in the **Filepath (optional)** field.



- If required, select **Default Before Applying** to reset the WS2000 device to default settings before an imported configuration file is applied on it.
- To import a file from the FTP server and apply it, click **FTP Import**. Similarly, to import a file from the TFTP server, click **TFTP Import**.

To export a file a server using FTP, click **FTP Export**. Similarly, to export to a server using TFTP, click **TFTP Export**.

### Export/Import configuration settings using HTTP

To import configuration settings using HTTP, you have to first upload a configuration file to the WS2000 and then apply it. Similarly, to export a WS2000's configuration setting, you have to first generate the configuration file and then download it to your PC.

#### To import a configuration file using HTTP:

- Click **Upload A File**. The *Upload a WS2000 Configuration File* dialog displays.

- Enter the administrative password for this WS2000 in the **Administrator Password** field. This allows you to upload a file to the WS2000.
- Use the **Browse** button to search for a configuration file to import to the WS2000.
- Click **Submit** to upload/import the configuration file to the WS2000. Once the file is uploaded to the WS2000, the *Upload a WS2000 Configuration File* dialog closes and you are returned to the *Config Import/Export* screen.
- Click **Apply Uploaded File** to apply the new configuration settings to the device.

#### To export a configuration file using HTTP

- Click **Generate File**. This creates the configuration file with the WS2000's current settings on it.
- Click **Download File**. The *Download WS2000 Configuration File* dialog displays.





3. Enter the administrative password for this WS2000 in the **Administrator Password** field. This allows you to download the configuration file from the WS2000.
4. Click **Get File**. The *Opening cfg.txt* dialog displays.



If you want to view the downloaded file, click **Open with** option to select it. If you want to save the file, click **Save to Disk**. Click **Ok** to do the selected task.



**NOTE:** When importing configuration settings, the system displays a confirmation window indicating that you must log out of the switch after the operation completes for the changes to take effect.

- Note**
5. After exporting, check the **Status** field for messages about the success or errors in executing the specified operation.

## 7.9.2 Sample Configuration File

All the configuration settings for the WS2000 Wireless Switch can be saved to a configuration file and then either imported back into the same switch or transferred to other switches.

Below is a sample configuration file that has been annotated using comment lines. All comment lines begin with // and are blue in color. The configuration file is organized by function area, and most areas correspond directly to a menu item.

```
//
// WS2000 Configuration Command Script
// System Firmware Version: 2.3.1.0-003X
//
system
ws2000
// WS2000 menu
set name WS2000
set loc \0
set email \0
set cc us
set airbeam mode disable
set airbeam enc-passwd a11e00942773
set applet lan enable
set applet wan enable
set applet slan enable
set applet swan enable
set cli lan enable
set cli wan enable
set snmp lan enable
set snmp wan enable
set workgroup name WORKGROUP
set workgroup mode disable
set ftp lan disable
set ftp wan disable
set ssh lan enable
set ssh wan enable
set timeout 0
set airbeam logging disable
set ftp wan logging disable
set ssh lan logging disable
set ssh wan logging disable
set applet lan logging disable
set applet wan logging disable
set applet slan logging disable
set applet swan logging disable
set cli lan logging disable
set cli wan logging disable
set snmp lan logging disable
set snmp wan logging disable
set limited-access disable
set dns-ip 192.168.0.1
set domain-name ws2ksymbol.com
delete administrator all
/
system
config
// Config menu
set server 192.168.0.100
set user root
set enc-passwd a0061b9f782f
set file cfg.txt
set fw file mesh.client.tc.yang.fix.bin
set fw path /home/ftp/adi/2k/
set import-enc-password disable
```

```

set fw boot on-board-flash
set fw active-partition primary
set bind-interface none
/
system
logs
// Logs menu
set mode disable
set level L6
set cf_logging_mode disable
/
system
ntp
// NTP menu
set mode enable
set server 1 157.235.205.31
set server 2 \0
set server 3 \0
set port 1 123
set port 2 123
set port 3 123
set intrvl 15
set zone 206
/
system
snmp
access
// SNMP ACL configuration
delete acl all
// SNMP v1/v2c configuration
delete v1v2c all
add v1v2c public ro 1.3.6.1
add v1v2c private rw 1.3.6.1
// SNMP v3 user definitions
delete v3 all
/
system
snmp
traps
// SNMP trap selection
set cold disable
set cfg disable
set lowcf disable
set port disable
set dos-attack disable
set snmp-auth disable
set snmp-acl disable
set mu-assoc disable
set mu-unassoc disable
set mu-deny-assoc disable
set mu-deny-auth disable
set ap-adopt disable
set ap-unadopt disable
set ap-denied-adopt disable
set ap-radar disable
set cf-thresh 1024
set min-pkt 1000
set dos-rate-limit 10
set rate pkts switch 0.00

```

```
set rate pkts wlan 0.00
set rate pkts ap 0.00
set rate pkts mu 0.00
set rate mbps switch 0.00
set rate mbps wlan 0.00
set rate mbps ap 0.00
set rate mbps mu 0.00
set rate avg-bps wlan 0.00
set rate avg-bps ap 0.00
set rate avg-bps mu 0.00
set rate pct-nu wlan 0.00
set rate pct-nu ap 0.00
set rate pct-nu mu 0.00
set rate avg-signal wlan 0.00
set rate avg-signal ap 0.00
set rate avg-signal mu 0.00
set rate avg-retries wlan 0.00
set rate avg-retries ap 0.00
set rate avg-retries mu 0.00
set rate pct-dropped wlan 0.00
set rate pct-dropped ap 0.00
set rate pct-dropped mu 0.00
set rate pct-undecrypt wlan 0.00
set rate pct-undecrypt ap 0.00
set rate pct-undecrypt mu 0.00
set rate assoc-mus switch 0
set rate assoc-mus wlan 0
set rate assoc-mus ap 0
set rogue-ap disable
set hotspot-mu-state disable
set user-login-failure enable
set interface enable
set admin-passwd-change enable
set dyndns-update disable
// SNMP v1/v2c trap configuration
delete v1v2c all
// SNMP v3 trap configuration
delete v3 all
/
system
ssh
// SSH configuration
set auth-timeout 120
set inactive-timeout 120
/
system
authentication
set mode local
set auth-loc radius
/
system
authentication
radius
// AUTHENTICATION RADIUS configuration
set auth-server-ip 192.168.0.4
set auth-server-port 1812
set enc-shared-secret alle00942773
/
system
```

```
userdb
user
// clear userdb user configuration
clearall
/
system
userdb
group
// clear userdb group configuration
clearall
/
system
userdb
user
enc-add EVLtwLcU a8342499045d7431bbb5
enc-add jzoniBdO 95252ea206553419ff9d
enc-add ssmzhpIC bd0539c4102c0b16cb9c
/
system
userdb
group
create Guests 1
add EVLtwLcU Guests
add jzoniBdO Guests
add ssmzhpIC Guests
set guest-group Guests
set start-time Guests 0000
set end-time Guests 2359
set day-access Guests mo tu we th fr sa su
/
system
radius
// radius server configuration
set database local
/
system
radius
eap
// radius EAP configuration
set auth peap
import server none
import cacert none
/
system
radius
eap
peap
// radius EAP PEAP configuration
set auth gtc
/
system
radius
eap
ttls
// radius EAP TTLS configuration
set auth pap
/
system
radius
```

```

policy
// radius access policy configuration
  set Guests
/
system
radius
ldap
// radius LDAP configuration
set domain \0
set port 389
set binddn cn=Manager,o=mobion
set basedn o=mobion

set login (uid=%{Stripped-User-Name:-%{User-Name}})
set pass_attr userPassword
set groupname cn
set filter (|(&(objectClass=GroupOfNames)(member=%{Ldap-UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))
set membership radiusGroupName
import client none
import cacert none
set admin-uname \\0
set pri-domain \\0
set admin-pass \\0
set adagent disable
/
system
radius
proxy
// radius proxy server configuration
set delay 5
set count 3
// radius proxy realm configuration
clearall
/
system
radius
client
// radius client configuration
/
system
http
// system http configuration
import self default
/
network
wlan
// WLAN 1 configuration
set mode 1 enable
set ess 1 101
set enc 1 none
set auth 1 none
set wep-mcm index 1 1
set wep-mcm enc-key 1 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 1 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 1 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 1 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 1 \0

```

```
set kerb realm 1 \0
set kerb port 1 1 88
set kerb port 1 2 88
set kerb port 1 3 88
set eap port 1 1 1812
set eap port 1 2 1812

set eap reauth mode 1 disable
set eap reauth retry 1 2
set eap reauth period 1 3600
set eap adv mu-quiet 1 10
set eap adv mu-tx 1 5
set eap adv mu-timeout 1 10
set eap adv mu-retry 1 2
set eap adv server-timeout 1 5
set eap adv server-retry 1 2
set eap rad-acct mode 1 disable
set eap rad-acct timeout 1 10
set eap rad-acct retry-count 1 2
set tkip type 1 phrase
set tkip enc-phrase 1 a11e00942773343deb84
set tkip enc-key 1
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 1 86400
set tkip rotate-mode 1 disable
set tkip wpa2 1 disable
set tkip preauth 1 disable
set tkip pmk 1 enable
set ccmp type 1 phrase
set ccmp enc-phrase 1 a11e00942773343deb84
set ccmp enc-key 1
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 1 86400
set ccmp rotate-mode 1 disable
set ccmp mixed-mode 1 disable
set ccmp preauth 1 disable
set ccmp opp-pmk 1 enable
set name 1 WLAN1
set no-mu-mu 1 disable
set vop 1 enable
set bcast 1 disable
set adopt 1 allow
set acl 1 allow
set mcast 1 1 01005E000000
set mcast 1 2 09000E000000
set eap syslog mode 1 disable
set vlan-id 1 1
set secure-beacon 1 disable
delete 1 all
// WLAN 2 configuration
set mode 2 disable
set ess 2 102
set enc 2 none
set auth 2 none
set wep-mcm index 2 1
set wep-mcm enc-key 2 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 2 2 f2464fd56c3a667fa0c53a09b9
```

```

set wep-mcm enc-key 2 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 2 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 2 \0

set kerb realm 2 \0
set kerb port 2 1 88
set kerb port 2 2 88
set kerb port 2 3 88
set eap port 2 1 1812
set eap port 2 2 1812

set eap reauth mode 2 disable
set eap reauth retry 2 2
set eap reauth period 2 3600
set eap adv mu-quiet 2 10
set eap adv mu-tx 2 5
set eap adv mu-timeout 2 10
set eap adv mu-retry 2 2
set eap adv server-timeout 2 5
set eap adv server-retry 2 2
set eap rad-acct mode 2 disable
set eap rad-acct timeout 2 10
set eap rad-acct retry-count 2 2
set tkip type 2 phrase
set tkip enc-phrase 2 alle00942773343deb84
set tkip enc-key 2
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 2 86400
set tkip rotate-mode 2 disable
set tkip wpa2 2 disable
set tkip preauth 2 disable
set tkip pmk 2 enable
set ccmp type 2 phrase
set ccmp enc-phrase 2 alle00942773343deb84
set ccmp enc-key 2
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 2 86400
set ccmp rotate-mode 2 disable
set ccmp mixed-mode 2 disable
set ccmp preauth 2 disable
set ccmp opp-pmk 2 enable
set name 2 WLAN2
set no-mu-mu 2 disable
set vop 2 enable
set bcast 2 disable
set adopt 2 allow
set acl 2 allow
set mcast 2 1 01005E000000
set mcast 2 2 09000E000000
set eap syslog mode 2 disable
set vlan-id 2 2
set secure-beacon 2 disable
delete 2 all
// WLAN 3 configuration
set mode 3 disable
set ess 3 103
set enc 3 none

```



```
set auth 3 none
set wep-mcm index 3 1
set wep-mcm enc-key 3 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 3 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 3 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 3 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 3 \0

set kerb realm 3 \0
set kerb port 3 1 88
set kerb port 3 2 88
set kerb port 3 3 88
set eap port 3 1 1812
set eap port 3 2 1812

set eap reauth mode 3 disable
set eap reauth retry 3 2
set eap reauth period 3 3600
set eap adv mu-quiet 3 10
set eap adv mu-tx 3 5
set eap adv mu-timeout 3 10
set eap adv mu-retry 3 2
set eap adv server-timeout 3 5
set eap adv server-retry 3 2
set eap rad-acct mode 3 disable
set eap rad-acct timeout 3 10
set eap rad-acct retry-count 3 2
set tkip type 3 phrase
set tkip enc-phrase 3 a11e00942773343deb84
set tkip enc-key 3
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 3 86400
set tkip rotate-mode 3 disable
set tkip wpa2 3 disable
set tkip preauth 3 disable
set tkip pmk 3 enable
set ccmp type 3 phrase
set ccmp enc-phrase 3 a11e00942773343deb84
set ccmp enc-key 3
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 3 86400
set ccmp rotate-mode 3 disable
set ccmp mixed-mode 3 disable
set ccmp preauth 3 disable
set ccmp opp-pmk 3 enable
set name 3 WLAN3
set no-mu-mu 3 disable
set vop 3 enable
set bcast 3 disable
set adopt 3 allow
set acl 3 allow
set mcast 3 1 01005E000000
set mcast 3 2 09000E000000
set eap syslog mode 3 disable
set vlan-id 3 3
set secure-beacon 3 disable
delete 3 all
```

```
// WLAN 4 configuration
set mode 4 disable
set ess 4 104
set enc 4 none
set auth 4 none
set wep-mcm index 4 1
set wep-mcm enc-key 4 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 4 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 4 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 4 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 4 \0

set kerb realm 4 \0
set kerb port 4 1 88
set kerb port 4 2 88
set kerb port 4 3 88
set eap port 4 1 1812
set eap port 4 2 1812

set eap reauth mode 4 disable
set eap reauth retry 4 2
set eap reauth period 4 3600
set eap adv mu-quiet 4 10
set eap adv mu-tx 4 5
set eap adv mu-timeout 4 10
set eap adv mu-retry 4 2
set eap adv server-timeout 4 5
set eap adv server-retry 4 2
set eap rad-acct mode 4 disable
set eap rad-acct timeout 4 10
set eap rad-acct retry-count 4 2
set tkip type 4 phrase
set tkip enc-phrase 4 a11e00942773343deb84
set tkip enc-key 4
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 4 86400
set tkip rotate-mode 4 disable
set tkip wpa2 4 disable
set tkip preauth 4 disable
set tkip pmk 4 enable
set ccmp type 4 phrase
set ccmp enc-phrase 4 a11e00942773343deb84
set ccmp enc-key 4
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 4 86400
set ccmp rotate-mode 4 disable
set ccmp mixed-mode 4 disable
set ccmp preauth 4 disable
set ccmp opp-pmk 4 enable
set name 4 WLAN4
set no-mu-mu 4 disable
set vop 4 enable
set bcast 4 disable
set adopt 4 allow
set acl 4 allow
set mcast 4 1 01005E000000
set mcast 4 2 09000E000000
```

```

set eap syslog mode 4 disable
set vlan-id 4 4
set secure-beacon 4 disable
delete 4 all
// WLAN 5 configuration
set mode 5 disable
set ess 5 105
set enc 5 none
set auth 5 none
set wep-mcm index 5 1
set wep-mcm enc-key 5 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 5 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 5 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 5 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 5 \0

set kerb realm 5 \0
set kerb port 5 1 88
set kerb port 5 2 88
set kerb port 5 3 88
set eap port 5 1 1812
set eap port 5 2 1812

set eap reauth mode 5 disable
set eap reauth retry 5 2
set eap reauth period 5 3600
set eap adv mu-quiet 5 10
set eap adv mu-tx 5 5
set eap adv mu-timeout 5 10
set eap adv mu-retry 5 2
set eap adv server-timeout 5 5
set eap adv server-retry 5 2
set eap rad-acct mode 5 disable
set eap rad-acct timeout 5 10
set eap rad-acct retry-count 5 2
set tkip type 5 phrase
set tkip enc-phrase 5 alle00942773343deb84
set tkip enc-key 5
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 5 86400
set tkip rotate-mode 5 disable
set tkip wpa2 5 disable
set tkip preauth 5 disable
set tkip pmk 5 enable
set ccmp type 5 phrase
set ccmp enc-phrase 5 alle00942773343deb84
set ccmp enc-key 5
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 5 86400
set ccmp rotate-mode 5 disable
set ccmp mixed-mode 5 disable
set ccmp preauth 5 disable
set ccmp opp-pmk 5 enable
set name 5 WLAN5
set no-mu-mu 5 disable
set vop 5 enable
set bcast 5 disable

```

```

set adopt 5 allow
set acl 5 allow
set mcast 5 1 01005E000000
set mcast 5 2 09000E000000
set eap syslog mode 5 disable
set vlan-id 5 5
set secure-beacon 5 disable
delete 5 all
// WLAN 6 configuration
set mode 6 disable
set ess 6 106
set enc 6 none
set auth 6 none
set wep-mcm index 6 1
set wep-mcm enc-key 6 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 6 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 6 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 6 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 6 \0

set kerb realm 6 \0
set kerb port 6 1 88
set kerb port 6 2 88
set kerb port 6 3 88
set eap port 6 1 1812
set eap port 6 2 1812

set eap reauth mode 6 disable
set eap reauth retry 6 2
set eap reauth period 6 3600
set eap adv mu-quiet 6 10
set eap adv mu-tx 6 5
set eap adv mu-timeout 6 10
set eap adv mu-retry 6 2
set eap adv server-timeout 6 5
set eap adv server-retry 6 2
set eap rad-acct mode 6 disable
set eap rad-acct timeout 6 10
set eap rad-acct retry-count 6 2
set tkip type 6 phrase
set tkip enc-phrase 6 a11e00942773343deb84
set tkip enc-key 6
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 6 86400
set tkip rotate-mode 6 disable
set tkip wpa2 6 disable
set tkip preauth 6 disable
set tkip pmk 6 enable
set ccmp type 6 phrase
set ccmp enc-phrase 6 a11e00942773343deb84
set ccmp enc-key 6
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 6 86400
set ccmp rotate-mode 6 disable
set ccmp mixed-mode 6 disable
set ccmp preauth 6 disable
set ccmp opp-pmk 6 enable

```

```

set name 6 WLAN6
set no-mu-mu 6 disable
set vop 6 enable
set bcast 6 disable
set adopt 6 allow
set acl 6 allow
set mcast 6 1 01005E000000
set mcast 6 2 09000E000000
set eap syslog mode 6 disable
set vlan-id 6 6
set secure-beacon 6 disable
delete 6 all
// WLAN 7 configuration
set mode 7 disable
set ess 7 107
set enc 7 none
set auth 7 none
set wep-mcm index 7 1
set wep-mcm enc-key 7 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 7 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 7 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 7 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 7 \0

set kerb realm 7 \0
set kerb port 7 1 88
set kerb port 7 2 88
set kerb port 7 3 88
set eap port 7 1 1812
set eap port 7 2 1812

set eap reauth mode 7 disable
set eap reauth retry 7 2
set eap reauth period 7 3600
set eap adv mu-quiet 7 10
set eap adv mu-tx 7 5
set eap adv mu-timeout 7 10
set eap adv mu-retry 7 2
set eap adv server-timeout 7 5
set eap adv server-retry 7 2
set eap rad-acct mode 7 disable
set eap rad-acct timeout 7 10
set eap rad-acct retry-count 7 2
set tkip type 7 phrase
set tkip enc-phrase 7 a11e00942773343deb84
set tkip enc-key 7
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 7 86400
set tkip rotate-mode 7 disable
set tkip wpa2 7 disable
set tkip preauth 7 disable
set tkip pmk 7 enable
set ccmp type 7 phrase
set ccmp enc-phrase 7 a11e00942773343deb84
set ccmp enc-key 7
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 7 86400

```

```
set ccmp rotate-mode 7 disable
set ccmp mixed-mode 7 disable
set ccmp preauth 7 disable
set ccmp opp-pmk 7 enable
set name 7 WLAN7
set no-mu-mu 7 disable
set vop 7 enable
set bcast 7 disable
set adopt 7 allow
set acl 7 allow
set mcast 7 1 01005E000000
set mcast 7 2 09000E000000
set eap syslog mode 7 disable
set vlan-id 7 7
set secure-beacon 7 disable
delete 7 all
// WLAN 8 configuration
set mode 8 disable
set ess 8 108
set enc 8 none
set auth 8 none
set wep-mcm index 8 1
set wep-mcm enc-key 8 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 8 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 8 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 8 4 92262fb50c5a061fc0a55a69d9
set mu-inact 10
set kerb user 8 \0

set kerb realm 8 \0
set kerb port 8 1 88
set kerb port 8 2 88
set kerb port 8 3 88
set eap port 8 1 1812
set eap port 8 2 1812

set eap reauth mode 8 disable
set eap reauth retry 8 2
set eap reauth period 8 3600
set eap adv mu-quiet 8 10
set eap adv mu-tx 8 5
set eap adv mu-timeout 8 10
set eap adv mu-retry 8 2
set eap adv server-timeout 8 5
set eap adv server-retry 8 2
set eap rad-acct mode 8 disable
set eap rad-acct timeout 8 10
set eap rad-acct retry-count 8 2
set tkip type 8 phrase
set tkip enc-phrase 8 alle00942773343deb84
set tkip enc-key 8
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set tkip interval 8 86400
set tkip rotate-mode 8 disable
set tkip wpa2 8 disable
set tkip preauth 8 disable
set tkip pmk 8 enable
set ccmp type 8 phrase
```

```

set ccmp enc-phrase 8 a11e00942773343deb84
set ccmp enc-key 8
c2767fe55c0a564fa8cd3201b1984a33f986e7872572740a80c6dcff32905735
set ccmp interval 8 86400
set ccmp rotate-mode 8 disable
set ccmp mixed-mode 8 disable
set ccmp preauth 8 disable
set ccmp opp-pmk 8 enable
set name 8 WLAN8
set no-mu-mu 8 disable
set vop 8 enable
set bcast 8 disable
set adopt 8 allow
set acl 8 allow
set mcast 8 1 01005E000000
set mcast 8 2 09000E000000
set eap syslog mode 8 disable
set vlan-id 8 8
set secure-beacon 8 disable
delete 8 all
set wep_shared disable
/
// Rogue AP Scan configuration
network
wlan
rogueap
set muscan mode disable
set muscan interval 60
set apscan mode disable
set apscan interval 60
set detscan mode disable
set detscan interval 60
set fullapscan mode disable
set fullapscan interval 60
rulelist
delete all
authsymbolap disable
..
approvedlist
ageout 0
..
roguelist
set RAP-Containment enable
ageout 0
set deauth-interval 2
set deauth-all disable
deauth remove-from-list all
set RAP-Containment disable
/
network
ap
default
// Default 802.11a radio configuration
set reg 802.11a in 36 17
set rate 802.11a 6,12,24 6,9,12,18,24,36,48,54
set div 802.11a full
set ch_mode 802.11a random
set beacon intvl 802.11a 100
set rts 802.11a 2341

```

```
set primary 802.11a 1
set dtim 802.11a 1 10
set dtim 802.11a 2 10
set dtim 802.11a 3 10
set dtim 802.11a 4 10
// Default 802.11b radio configuration
set reg 802.11b in/out 1 20
set rate 802.11b 1,2 1,2,5.5,11
set div 802.11b full
set ch_mode 802.11b fixed
set beacon intvl 802.11b 100
set rts 802.11b 2341
set short-pre 802.11b disable
set dtim 802.11b 1 10
set dtim 802.11b 2 10
set dtim 802.11b 3 10
set dtim 802.11b 4 10
// Default 802.11b/g radio configuration
set reg 802.11b/g in/out 1 20
set rate 802.11b/g 1,2,5.5,11 1,2,5.5,6,9,11,12,18,24,36,48,54
set div 802.11b/g full
set ch_mode 802.11b/g fixed
set beacon intvl 802.11b/g 100
set rts 802.11b/g 2341
set short-pre 802.11b/g disable
set dtim 802.11b/g 1 10
set dtim 802.11b/g 2 10
set dtim 802.11b/g 3 10
set dtim 802.11b/g 4 10
set sensor-img def
set ap4131-img def
set ap4121-img def
/
// Access Port configuration
network
ap
delete 1 all
delete 2 all
delete 3 all
delete 4 all
delete 5 all
delete 6 all
delete 7 all
delete 8 all
// Set each ap to the default
// copydefaults 1
// copydefaults 2
// copydefaults 3
// copydefaults 4
// copydefaults 5
// copydefaults 6
// copydefaults 7
// copydefaults 8
// copydefaults 9
// copydefaults 10
// copydefaults 11
// copydefaults 12
// Individual AP settings exported for, static AP configuration
forget all
```



```
set mac 1 00A0F860C858
set ap_type 1 AP200
set radio_type 1 802.11b
set beacon intvl 1 100
set dtim 1 1 10
set dtim 1 2 10
set dtim 1 3 10
set dtim 1 4 10
set ch_mode 1 fixed
set short-pre 1 disable
set div 1 full
set reg 1 in/out 1 20
set mu-power-adjustment 1 0
set rts 1 2341
set name 1 AP1
set loc 1 \0
set ap_scan 1 on-chan
set rate 1 1,2 1,2,5.5,11
set allowed_sip_session 1 10
set mac 2 00A0F860BE2B
set ap_type 2 AP200
set radio_type 2 802.11a
set beacon intvl 2 100
set dtim 2 1 10
set dtim 2 2 10
set dtim 2 3 10
set dtim 2 4 10
set ch_mode 2 random
set primary 2 1
set div 2 full
set reg 2 in 36 17
set mu-power-adjustment 2 0
set rts 2 2341
set name 2 AP2
set loc 2 \0
set ap_scan 2 on-chan
set rate 2 6,12,24 6,9,12,18,24,36,48,54
set allowed_sip_session 2 10
set mac 3 00A0F8B54D68
set ap_type 3 AP200
set radio_type 3 802.11b
set beacon intvl 3 100
set dtim 3 1 10
set dtim 3 2 10
set dtim 3 3 10
set dtim 3 4 10
set ch_mode 3 fixed
set short-pre 3 disable
set div 3 full
set reg 3 in/out 1 20
set mu-power-adjustment 3 0
set rts 3 2341
set name 3 AP3
set loc 3 \0
set ap_scan 3 on-chan
set rate 3 1,2 1,2,5.5,11
set allowed_sip_session 3 10
set mac 4 00A0F8B5360D
set ap_type 4 AP200
```

```
set radio_type 4 802.11a
set beacon intvl 4 100
set dtim 4 1 10
set dtim 4 2 10
set dtim 4 3 10
set dtim 4 4 10
set ch_mode 4 random
set primary 4 1
set div 4 full
set reg 4 in 36 17
set mu-power-adjustment 4 0
set rts 4 2341
set name 4 AP4
set loc 4 \0
set ap_scan 4 on-chan
set rate 4 6,12,24 6,9,12,18,24,36,48,54
set allowed_sip_session 4 10
set mac 5 00A0F8BFF144
set ap_type 5 AP300
set radio_type 5 802.11b/g
set beacon intvl 5 100
set dtim 5 1 10
set dtim 5 2 10
set dtim 5 3 10
set dtim 5 4 10
set ch_mode 5 fixed
set short-pre 5 disable
set div 5 full
set reg 5 in/out 1 20
set mu-power-adjustment 5 0
set rts 5 2341
set name 5 AP5
set loc 5 \0
set ap_scan 5 on-chan
set rate 5 1,2,5.5,11 1,2,5.5,6,9,11,12,18,24,36,48,54
set allowed_sip_session 5 10
set mac 6 00A0F8BFEE3C
set ap_type 6 AP300
set radio_type 6 802.11a
set beacon intvl 6 100
set dtim 6 1 10
set dtim 6 2 10
set dtim 6 3 10
set dtim 6 4 10
set ch_mode 6 random
set primary 6 1
set div 6 full
set reg 6 in 36 17
set mu-power-adjustment 6 0
set rts 6 2341
set name 6 AP6
set loc 6 \0
set ap_scan 6 on-chan
set rate 6 6,12,24 6,9,12,18,24,36,48,54
set allowed_sip_session 6 10
set sip_cac_mode disable
set legacy-mode enable
set force-13 disable
denyap
```

```
// AP Deny List menu
delete all
// Self-Healing configuration
/
network
ap
selfheal
// Self-Heal Interference Avoidance Configuration
set interference-avoidance mode disable
set interference-avoidance max-retries 14
set interference-avoidance hold-time 3600

// Self-Heal Neighbor Recovery Configuration
set neighbor-recovery mode disable
set neighbor-recovery offset 1 default
set neighbor-recovery offset 2 default
set neighbor-recovery offset 3 default
set neighbor-recovery offset 4 default
set neighbor-recovery offset 5 default
set neighbor-recovery offset 6 default
set neighbor-recovery offset 7 default
set neighbor-recovery offset 8 default
set neighbor-recovery offset 9 default
set neighbor-recovery offset 10 default
set neighbor-recovery offset 11 default
set neighbor-recovery offset 12 default

set neighbor-recovery action 1 none
set neighbor-recovery action 2 none
set neighbor-recovery action 3 none
set neighbor-recovery action 4 none
set neighbor-recovery action 5 none
set neighbor-recovery action 6 none
set neighbor-recovery action 7 none
set neighbor-recovery action 8 none
set neighbor-recovery action 9 none
set neighbor-recovery action 10 none
set neighbor-recovery action 11 none
set neighbor-recovery action 12 none

del all all

/
network
ap
smartscan
// smartscan configuration
delete 11a
delete 11bg
/
/
// Access Port Mesh configuration
network
ap
mesh
set client 1 disable
```

```
set wlan 1 1
set auto 1 enable
del 1 all
set base 1 disable
set max-clients 1 6
set client 2 disable
set wlan 2 1
set auto 2 enable
del 2 all
set base 2 disable
set max-clients 2 6
set client 3 disable
set wlan 3 1
set auto 3 enable
del 3 all
set base 3 disable
set max-clients 3 6
set client 4 disable
set wlan 4 1
set auto 4 enable
del 4 all
set base 4 disable
set max-clients 4 6
set client 5 disable
set wlan 5 1
set auto 5 enable
del 5 all
set base 5 disable
set max-clients 5 6
set client 6 disable
set wlan 6 1
set auto 6 enable
del 6 all
set base 6 disable
set max-clients 6 6
set client 7 disable
set wlan 7 1
set auto 7 enable
del 7 all
set base 7 disable
set max-clients 7 6
set client 8 disable
set wlan 8 1
set auto 8 enable
del 8 all
set base 8 disable
set max-clients 8 6
set client 9 disable
set wlan 9 1
set auto 9 enable
del 9 all
set base 9 disable
set max-clients 9 6
set client 10 disable
set wlan 10 1
set auto 10 enable
del 10 all
set base 10 disable
set max-clients 10 6
```

```
set client 11 disable
set wlan 11 1
set auto 11 enable
del 11 all
set base 11 disable
set max-clients 11 6
set client 12 disable
set wlan 12 1
set auto 12 enable
del 12 all
set base 12 disable
set max-clients 12 6
/
// LAN configuration
network
lan
set mode 1 enable
set name 1 Subnet1
set ipadr 1 192.168.0.1
set mask 1 255.255.255.0
set dgw 1 192.168.0.1
set mode 2 enable
set name 2 Subnet2
set ipadr 2 192.168.1.1
set mask 2 255.255.255.0
set dgw 2 192.168.1.1
set mode 3 enable
set name 3 Subnet3
set ipadr 3 192.168.2.1
set mask 3 255.255.255.0
set dgw 3 192.168.2.1
set mode 4 enable
set name 4 Subnet4
set ipadr 4 192.168.3.1
set mask 4 255.255.255.0
set dgw 4 192.168.3.1
// Port To Subnet Map configuration
set port 1 s1
set port 2 s1
set port 3 s1
set port 4 s1
set port 5 s1
set port 6 s1
// WLAN To Subnet Map configuration
set wlan 1 s1
set wlan 2 s2
set wlan 3 s3
set wlan 4 s4
set wlan 5 none
set wlan 6 none
set wlan 7 none
set wlan 8 none
/
// LAN DHCP configuration
network
lan
dhcp
set mode 1 server
set ddnsmode 1 disable
```

```
set ddnsusrcls 1 single
set dgw 1 192.168.0.1
set dns 1 1 192.168.0.1
set dns 1 2 192.168.0.1
set wins 1 192.168.0.254
set lease 1 86400
set domain 1 \0
set fwdzone 1 \0
set tftp-server 1 0.0.0.0
set bootfile 1 \0
set option-189 1 \0
set option-43 1 \0
set mode 1 server
set range 1 192.168.0.100 192.168.0.254
set mode 2 server
set ddnsmode 2 disable
set ddnsusrcls 2 single
set dgw 2 192.168.1.1
set dns 2 1 192.168.1.1
set dns 2 2 192.168.1.1
set wins 2 192.168.1.254
set lease 2 86400
set domain 2 \0
set fwdzone 2 \0
set tftp-server 2 0.0.0.0
set bootfile 2 \0
set option-189 2 \0
set option-43 2 \0
set mode 2 server
set range 2 192.168.1.100 192.168.1.254
set mode 3 server
set ddnsmode 3 disable
set ddnsusrcls 3 single
set dgw 3 192.168.2.1
set dns 3 1 192.168.2.1
set dns 3 2 192.168.2.1
set wins 3 192.168.2.254
set lease 3 86400
set domain 3 \0
set fwdzone 3 \0
set tftp-server 3 0.0.0.0
set bootfile 3 \0
set option-189 3 \0
set option-43 3 \0
set mode 3 server
set range 3 192.168.2.100 192.168.2.254
set mode 4 server
set ddnsmode 4 disable
set ddnsusrcls 4 single
set dgw 4 192.168.3.1
set dns 4 1 192.168.3.1
set dns 4 2 192.168.3.1
set wins 4 192.168.3.254
set lease 4 86400
set domain 4 \0
set fwdzone 4 \0
set tftp-server 4 0.0.0.0
set bootfile 4 \0
set option-189 4 \0
```

```
set option-43 4 \0
set mode 4 server
set range 4 192.168.3.100 192.168.3.254
delete 1 all
delete 2 all
delete 3 all
delete 4 all
/
// LAN Bridge configuration
network
lan
bridge
set priority 1 32768
set hello 1 2
set msgage 1 20
set fwddelay 1 15
set ageout 1 300
set wireless-trunking 1 disable
set priority 2 32768
set hello 2 2
set msgage 2 20
set fwddelay 2 15
set ageout 2 300
set wireless-trunking 2 disable
set priority 3 32768
set hello 3 2
set msgage 3 20
set fwddelay 3 15
set ageout 3 300
set wireless-trunking 3 disable
set priority 4 32768
set hello 4 2
set msgage 4 20
set fwddelay 4 15
set ageout 4 300
set wireless-trunking 4 disable
/
network
lan
set mode 1 enable
set mode 2 disable
set mode 3 disable
set mode 4 disable
set stp disable
/
// Port configuration
network
port
// LAN Port configuration
set auto-negotiation port1 enable
set speed port1 100M
set duplex port1 full

set auto-negotiation port2 enable
set speed port2 100M
set duplex port2 full

set auto-negotiation port3 enable
set speed port3 100M
```

```
set duplex port3 full

set auto-negotiation port4 enable
set speed port4 100M
set duplex port4 full

set auto-negotiation port5 enable
set speed port5 100M
set duplex port5 full

set auto-negotiation port6 enable
set speed port6 100M
set duplex port6 full

// WAN Port configuration
set auto-negotiation wan enable
set speed wan 100M
set duplex wan full

/
system
redundancy
//Redundancy menu
set op_state redundancy
set redundancy s1 disable
set virtualip s1 0.0.0.0
set redundancy s2 disable
set virtualip s2 0.0.0.0
set redundancy s3 disable
set virtualip s3 0.0.0.0
set redundancy s4 disable
set virtualip s4 0.0.0.0
set mode primary
set heartbeat 5
set revertdelay 5
set preempt enable
set op_state standalone

/
// WAN configuration
network
wan
set dhcp enable
set mask 255.255.255.0
set pppoe mode disable
set pppoe user \0

set pppoe idle 600
set pppoe ka disable
set pppoe type pap/chap
set pppoe mss 1452
set mode 1 enable
set mode 2 enable
set mode 3 disable
set ipadr 3 4.4.4.4
set mode 4 disable
set ipadr 4 3.3.3.3
set mode 5 disable
set mode 6 disable
```



```
set mode 7 disable
set mode 8 disable
/
network
wan
nat
// NAT configuration
set type 1 1-to-many
set inb mode 1 disable
set type 2 none
set inb mode 2 disable
set type 3 none
set inb mode 3 disable
set type 4 none
set inb mode 4 disable
set type 5 none
set inb mode 5 disable
set type 6 none
set inb mode 6 disable
set type 7 none
set inb mode 7 disable
set type 8 none
set inb mode 8 disable
// Outbound 1-To-Many NAT configuration
set outb map s1 1
set outb map s2 1
set outb map s3 1
set outb map s4 1
// Inbound NAT configuration
delete inb 1 all
delete inb 2 all
delete inb 3 all
delete inb 4 all
delete inb 5 all
delete inb 6 all
delete inb 7 all
delete inb 8 all
/
network
wan
app
// Content Filtering configuration
delcmd web proxy
delcmd web activex
delcmd smtp helo
delcmd smtp mail
delcmd smtp rcpt
delcmd smtp data
delcmd smtp quit
delcmd smtp send
delcmd smtp saml
delcmd smtp rset
delcmd smtp vrfy
delcmd smtp expn
delcmd ftp put
delcmd ftp get
delcmd ftp ls
delcmd ftp mkdir
delcmd ftp cd
```

```
delcmd ftp pasv
delcmd web file all
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
addcmd web file \0
/
// Firewall configuration
network
fw
set override disable
submap
// Subnet map configuration
set default s1 w allow
set default s1 s2 allow
set default s1 s3 allow
set default s1 s4 allow
set default s2 w allow
set default s2 s1 allow
set default s2 s3 allow
set default s2 s4 allow
set default s3 w allow
set default s3 s1 allow
set default s3 s2 allow
set default s3 s4 allow
set default s4 w allow
set default s4 s1 allow
set default s4 s2 allow
set default s4 s3 allow
delete s1 all
delete s2 all
delete s3 all
delete s4 all
set subnet-logging s1 w disable
set subnet-logging s1 s2 disable
set subnet-logging s1 s3 disable
set subnet-logging s1 s4 disable
set subnet-logging s2 w disable
set subnet-logging s2 s1 disable
set subnet-logging s2 s3 disable
set subnet-logging s2 s4 disable
set subnet-logging s3 w disable
set subnet-logging s3 s1 disable
set subnet-logging s3 s2 disable
set subnet-logging s3 s4 disable
set subnet-logging s4 w disable
set subnet-logging s4 s1 disable
set subnet-logging s4 s2 disable
set subnet-logging s4 s3 disable
/
// Advanced Subnet configuration
network
fw
```

```
set override enable
policy
inbound
// Inbound policy configuration
delete all
/
network
fw
set override enable
policy
outbound
// Outbound policy configuration
delete all
/
network
fw
set mode enable
set override disable
set syn enable
set src enable
set win enable
set ftp enable
set ip enable
set seq enable
set mime filter enable
set mime len 8192
set mime hdr 16
set timeout 10
set spoof enable
set rst enable
set range enable
set fin 20
timerdel all
/
// Router configuration
network
router
set type off
set dir both
set auth none

set id 1 1
set enc-key 1 e2565fc57c2a766fb0d55160d6f92952
set id 2 1
set enc-key 2 e2565fc57c2a766fb0d55160d6f92952
set dgw-if wan
delete all
/
// QOS configuration
network
qos
set bw-share mode weighted
set bw-share weight 1 1
set bw-share weight 2 1
set bw-share weight 3 1
set bw-share weight 4 1
set bw-share weight 5 1
set bw-share weight 6 1
set bw-share weight 7 1
```

```
set bw-share weight 8 1
set bw-share mode rate-limit
set bw-share mode none
/
// VLAN configuration
network
vlan
set assign-mode port
set default 1
// Subnet to VLAN configuration
set vlan-id s1 1
set vlan-id s2 2
set vlan-id s3 3
set vlan-id s4 4
/
// VLAN Trunk configuration
network
vlan
set trunk-port none
set allow vlans 1-4094
/
// Hotspot configuration
// Hotspot configuration
network
wlan
hotspot
// Wlan 1 - Hotspot configuration
set mode 1 disable
set page-loc 1 default
set exturl 1 login \0
set exturl 1 welcome \0
set exturl 1 fail \0
set http-mode 1 https
// Wlan 2 - Hotspot configuration
set mode 2 disable
set page-loc 2 default
set exturl 2 login \0
set exturl 2 welcome \0
set exturl 2 fail \0
set http-mode 2 https
// Wlan 3 - Hotspot configuration
set mode 3 disable
set page-loc 3 default
set exturl 3 login \0
set exturl 3 welcome \0
set exturl 3 fail \0
set http-mode 3 https
// Wlan 4 - Hotspot configuration
set mode 4 disable
set page-loc 4 default
set exturl 4 login \0
set exturl 4 welcome \0
set exturl 4 fail \0
set http-mode 4 https
// Wlan 5 - Hotspot configuration
set mode 5 disable
set page-loc 5 default
set exturl 5 login \0
set exturl 5 welcome \0
```

```
set exturl 5 fail \0
set http-mode 5 https
// Wlan 6 - Hotspot configuration
set mode 6 disable
set page-loc 6 default
set exturl 6 login \0
set exturl 6 welcome \0
set exturl 6 fail \0
set http-mode 6 https
// Wlan 7 - Hotspot configuration
set mode 7 disable
set page-loc 7 default
set exturl 7 login \0
set exturl 7 welcome \0
set exturl 7 fail \0
set http-mode 7 https
// Wlan 8 - Hotspot configuration
set mode 8 disable
set page-loc 8 default
set exturl 8 login \0
set exturl 8 welcome \0
set exturl 8 fail \0
set http-mode 8 https
/
// Hotspot Radius configuration
network
wlan
hotspot
radius
// Wlan 1 - Hotspot Radius configuration
set acct-mode 1 disable
set acct-timeout 1 10
set acct-retry 1 3
set port 1 primary 1812

set port 1 secondary 1812

// Wlan 2 - Hotspot Radius configuration
set acct-mode 2 disable
set acct-timeout 2 10
set acct-retry 2 3
set port 2 primary 1812

set port 2 secondary 1812

// Wlan 3 - Hotspot Radius configuration
set acct-mode 3 disable
set acct-timeout 3 10
set acct-retry 3 3
set port 3 primary 1812

set port 3 secondary 1812

// Wlan 4 - Hotspot Radius configuration
set acct-mode 4 disable
set acct-timeout 4 10
set acct-retry 4 3
set port 4 primary 1812
```

```
set port 4 secondary 1812

// Wlan 5 - Hotspot Radius configuration
set acct-mode 5 disable
set acct-timeout 5 10
set acct-retry 5 3
set port 5 primary 1812

set port 5 secondary 1812

// Wlan 6 - Hotspot Radius configuration
set acct-mode 6 disable
set acct-timeout 6 10
set acct-retry 6 3
set port 6 primary 1812

set port 6 secondary 1812

// Wlan 7 - Hotspot Radius configuration
set acct-mode 7 disable
set acct-timeout 7 10
set acct-retry 7 3
set port 7 primary 1812

set port 7 secondary 1812

// Wlan 8 - Hotspot Radius configuration
set acct-mode 8 disable
set acct-timeout 8 10
set acct-retry 8 3
set port 8 primary 1812

set port 8 secondary 1812

/
// Hotspot Whitelist configuration
network
wlan
hotspot
white-list
clear rule all
// Hotspot Whitelist 1 configuration
// Hotspot Whitelist 2 configuration
// Hotspot Whitelist 3 configuration
// Hotspot Whitelist 4 configuration
// Hotspot Whitelist 5 configuration
// Hotspot Whitelist 6 configuration
// Hotspot Whitelist 7 configuration
// Hotspot Whitelist 8 configuration
/
/
network
dhcp
// network->dhcp menu
set firmwareupgrade 1
set configupgrade 1
set interface w
set dhcpvendorclassid V2-0
set autoupgradeinterval 600
```

```
/
network
wips
// WIPS menu
set mode enable
defaults
set mode client
set ipaddr 192.168.0.10
set mask 255.255.255.0
set dgw 192.168.0.1
set pwips 192.168.0.20
set swips 192.168.0.21
..
set mode disable
/
/
network
// WLAN IP Filter Configuration
wlan
wlanipfpolicy
set ipf-mode 1 enable
del 1 all
set ipf-mode 2 enable
del 2 all
set ipf-mode 3 enable
del 3 all
set ipf-mode 4 enable
del 4 all
set ipf-mode 5 enable
del 5 all
set ipf-mode 6 enable
del 6 all
set ipf-mode 7 enable
del 7 all
set ipf-mode 8 enable
del 8 all
/
/
network
// TRUNK IP Filter Configuration
wan
trunkipfpolicy
set ipf-mode enable
del all
/
/
network
ipfilter
del all
/
// Global IP Filter Configuration
/
network
ipfilter
/
// WLAN IP Filter Configuration
/
network
wlan
```

```
wlanipfpolicy
set ipf-mode 1 enable

set ipf-mode 1 disable
set default incoming 1 allow
set default outgoing 1 allow
set ipf-mode 2 enable

set ipf-mode 2 disable
set default incoming 2 allow
set default outgoing 2 allow
set ipf-mode 3 enable

set ipf-mode 3 disable
set default incoming 3 allow
set default outgoing 3 allow
set ipf-mode 4 enable

set ipf-mode 4 disable
set default incoming 4 allow
set default outgoing 4 allow
set ipf-mode 5 enable

set ipf-mode 5 disable
set default incoming 5 allow
set default outgoing 5 allow
set ipf-mode 6 enable

set ipf-mode 6 disable
set default incoming 6 allow
set default outgoing 6 allow
set ipf-mode 7 enable

set ipf-mode 7 disable
set default incoming 7 allow
set default outgoing 7 allow
set ipf-mode 8 enable

set ipf-mode 8 disable
set default incoming 8 allow
set default outgoing 8 allow
/
// TRUNK IP Filter Configuration
/
network
wan
trunkipfpolicy
set ipf-mode enable

set ipf-mode disable
set default incoming allow
set default outgoing allow
/
/
network
wan
dyndns
// DynDNS menu
set mode disable
```



```

set username \0
set password \0
set hostname \0
/
// WIDS Configuration
network
wids
set mode disable
set detect-window 10
/
network
wids
set excess-op threshold mu probe-req 0
set excess-op threshold radio probe-req 0
set excess-op threshold switch probe-req 0
set excess-op filter-ageout probe-req 60
set excess-op threshold mu auth-assoc-req 0
set excess-op threshold radio auth-assoc-req 0
set excess-op threshold switch auth-assoc-req 0
set excess-op filter-ageout auth-assoc-req 60
set excess-op threshold mu deauth-disassoc-req 0
set excess-op threshold radio deauth-disassoc-req 0
set excess-op threshold switch deauth-disassoc-req 0
set excess-op filter-ageout deauth-disassoc-req 60
set excess-op threshold mu auth-fails 0
set excess-op threshold radio auth-fails 0
set excess-op threshold switch auth-fails 0
set excess-op filter-ageout auth-fails 60
set excess-op threshold mu crypto-replay-fails 0
set excess-op threshold radio crypto-replay-fails 0
set excess-op threshold switch crypto-replay-fails 0
set excess-op filter-ageout crypto-replay-fails 60
set excess-op threshold mu 80211-replay-fails 0
set excess-op threshold radio 80211-replay-fails 0
set excess-op threshold switch 80211-replay-fails 0
set excess-op filter-ageout 80211-replay-fails 60
set excess-op threshold mu decrypt-fails 0
set excess-op threshold radio decrypt-fails 0
set excess-op threshold switch decrypt-fails 0
set excess-op filter-ageout decrypt-fails 60
set excess-op threshold mu unassoc-frames 0
set excess-op threshold radio unassoc-frames 0
set excess-op threshold switch unassoc-frames 0
set excess-op filter-ageout unassoc-frames 60
set excess-op threshold mu eap-starts 0
set excess-op threshold radio eap-starts 0
set excess-op threshold switch eap-starts 0
set excess-op filter-ageout eap-starts 60
/
network
wids
set anomaly-detect mode null-dst disable
set anomaly-detect filter-ageout null-dst 60
set anomaly-detect mode same-src-dst disable
set anomaly-detect filter-ageout same-src-dst 60
set anomaly-detect mode mcast-src disable
set anomaly-detect filter-ageout mcast-src 60
set anomaly-detect mode weak-wep-iv disable
set anomaly-detect filter-ageout weak-wep-iv 60

```

```
set anomaly-detect mode tkip-cntr-meas disable
set anomaly-detect filter-ageout tkip-cntr-meas 60
set anomaly-detect mode invalid-frame-len disable
set anomaly-detect filter-ageout invalid-frame-len 60
/
/
// Enhanced Rogue AP Scan configuration
network
wlan
enhancedrogueap
set mode disable
set scaninterval 10
set scanduration 100
/
// Mu Probe Table configuration
network
wlan
muprobe
set mode disable
set size 200
/
/
passwd enc-admin b3
passwd enc-manager a11e00942773
/
save
```

## 7.10 Updating Sensor Firmware

WS2000 provides support for setting up AP300s as dedicated sensors. This feature enables updating the firmware for these APs without disturbing the switch settings. The following must be noted with respect to sensor firmware update:

- The switch need not be restarted after a successful sensor firmware update.
- APs that are converted as sensors after a sensor firmware update receive the new firmware.
- APs that are sensors when the sensor firmware update is performed have to be reverted and re-converted.

Select **System Configuration --> Cfg/Firmware Mgt. --> Sensor Firmware Update** from the left menu to set parameters to update the sensor firmware.

The screenshot shows the 'Sensor Firmware Update' configuration page in the WS2000 Wireless Switch management console. The left sidebar contains a tree view with 'Sensor Firmware Update' selected. The main area has the following fields and options:

- Server Options:**
  - Filename:
  - Server IP:
  - Username:
  - Password:
  - Filepath(optional):
  - Bind Interface:
  - Max size of sensor fw file:
- Sensor FW upgrade mode ->**
  - 
  -
- Status:**
  -

At the bottom right, there are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'WS2000' is visible at the bottom left.

### 7.10.1 Setting Sensor Firmware Update Information

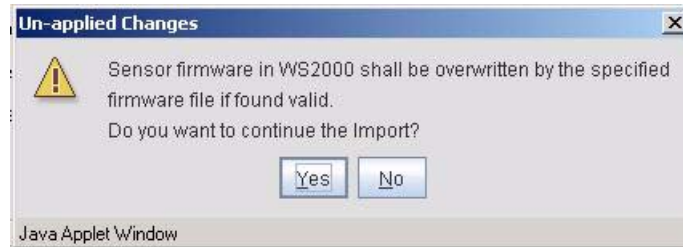
To update the sensor firmware, perform the following steps:

1. Enter the sensor firmware file name in the **Filename** box. This is the name of the file that contains the sensor firmware.
2. Enter the IP address of the server where the sensor firmware is stored. Enter this IP address in the **Server IP** field.
3. Enter the user name for authentication with the file server. Enter this in the **Username** field.
4. Similarly, enter the password for the user name for authentication. Enter this in the **Password** field.
5. Optionally, provide the complete path to the sensor firmware file on the server. Enter the path in the **Filepath(optional)** field.
6. Select the bind interface from the **Bind Interface** drop down list. This interface is used to reach the FTP/TFTP server for firmware update. Select, as the bind interface, the subnet that is configured as the local subnet for the VPN tunnel and on which the FTP/TFTP server resides.

7. To restrict the maximum size of the sensor firmware image, use the **Max size of sensor file**. Use this value to restrict the file size for the sensor firmware file.

### 7.10.2 Updating the Sensor Firmware

To update the sensor firmware, use the **FTP** or **TFTP** buttons on the screen. Select the appropriate server to update the sensor firmware from. A warning dialog appears.



Click **Yes** to proceed with sensor firmware update.

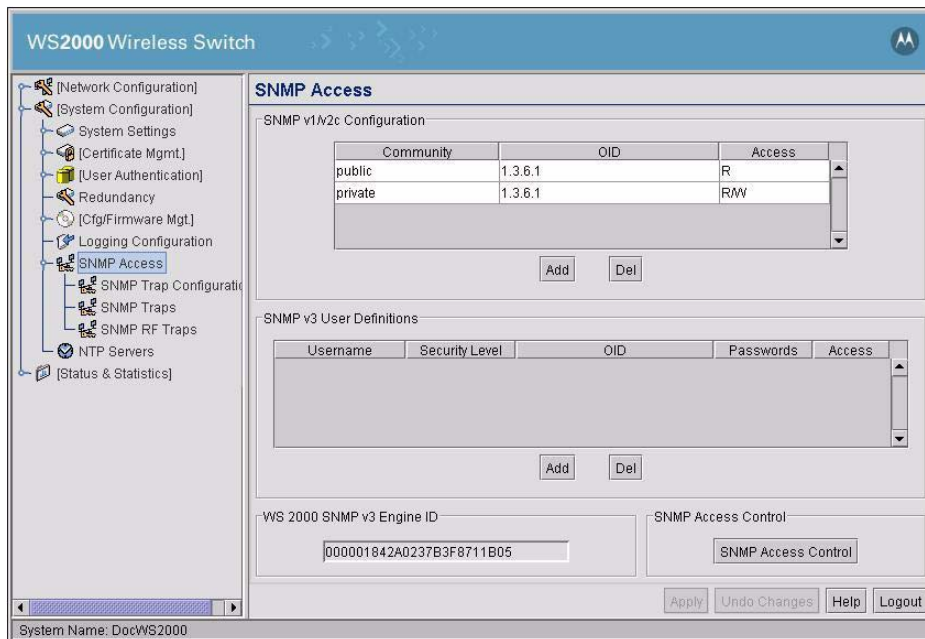
Once the sensor firmware is updated, a status is shown in the *Sensor Firmware Update* screen.

## 7.11 Configuring SNMP

The Simple Network Management Protocol (SNMP) facilitates the exchange of management information between network devices. SNMP allows an administrator to manage network performance, find and solve network problems, and plan for network growth. The WS2000 Wireless Switch includes SNMP management functions for gathering information from its network components, and communicating that information to specific users. There are four different SNMP screens.

- Use the SNMP Access screen to define SNMP v1/v2c community definitions and SNMP v3 user definitions associated with access.
- Use the SNMP Trap Configuration screen to configure to define SNMP v1/v2c community definitions and SNMP v3 user definitions associated with the traps themselves. Trap configuration depends on the network machine that receives the generated traps.
- Use the SNMP Traps screen to enable system, network, SNMP, mobile unit, and Access Port traps.
- Use the SNMP Rate Traps screen to enable traps by setting RF Rate thresholds.

Select **System Configuration** --> **SNMP Access** from the left menu to set up SNMP service.



## 7.11.1 Setting the SNMP Version Configuration

The SNMP Access screen allows the administrator to define SNMP v1/v2c community definitions and SNMP v3 user definitions. SNMP v1 and v2c provide a strong network management system, but their security is relatively weak. SNMP v3 provides greatly enhanced security protocols. SNMP v3 encrypts transmissions and provides authentication for users generating requests.

### 7.11.1.1 Setting Up SNMP v1/v2c Community Definitions

SNMP v1/v2c community definitions allow read-only or read/write access to switch-management information, as appropriate. The SNMP community, in this case, includes users whose IP addresses are specified on the SNMP Access Control subscreen. A read-only community string allows a remote device to retrieve information, while a read/write community string also allows a remote device to modify settings. Set up a read/write definition to facilitate full access by the administrator.

1. To create a new community definition, click the **Add** button in the SNMP v1/v2c Community Configuration area.
2. Type in a site-appropriate name for the community.
3. Click in the **OID** cell of the table. Either use the OID (Object Identifier) pull-down menu to select the default OID or type in an OID number into the field. (The format is in a numerical dot notation, and valid numbers can be found within the MIB.)

If is selected, the community will have access to all the OIDs (SNMP parameters) in the SNMP Management Information Base (MIB) file. If a custom OID is entered, the administrator can allow access to specific OIDs in the MIB to certain communities.

4. Use the **Access** pull-down menu to specify read-only (R) access or read/write (RW) access for the community. Read-only access allows a remote device to retrieve switch information, while read/write access also allows a remote device to modify switch settings.
5. Continue to the [Setting Up the Access Control List](#) section in this document.

### 7.11.1.2 Setting Up SNMP v3 Community Definitions

Setting up the v3 user definition is very similar to the v1/v2c community definitions. The difference is the addition of a user security level and a user password.

1. To create a new SNMP v3 user definition, click the **Add** button in the SNMP v3 User Definitions area.
2. Specify a user name in the **Username** field.
3. Select a security level from the Security pull-down menu. Select from the following choices:

<b>noAuth</b>	(no authorization) Allows the user to access SNMP without authorization or encryption
<b>AuthNoPriv</b>	(authorization without privacy) Requires the user to login, however no encryption is used
<b>AuthPriv</b>	(authorization with privacy) Requires the user to login and encryption is used

4. Click in the **OID** cell of the table. Either use the OID (Object Identifier) pull-down menu to select the default OID or type in an OID number into the field. (The format is in a numerical dot notation, and valid numbers can be found within the MIB.)

If is selected, the community will have access to all the OIDs (SNMP parameters) in the SNMP Management Information Base (MIB) file. If a custom OID is entered, the administrator can allow access to specific OIDs in the MIB to certain communities.

5. Click the **Password** button in the cell and the **Password Settings** screen appears.


1. Select an **Authentication Algorithm** from the drop-down menu, either **MD5** or **SHA1**.
2. Type in an **Authentication Password**.
3. Select a Privacy Algorithm from the drop-down menu. The options include:
  - **DES**
  - **AES 128-bit**
4. Type in a **Privacy Password** that matches the algorithm.
5. Click **Ok**, when done.

6. Use the **Access** pull-down menu to specify read-only (R) access or read/write (RW) access for the community. Read-only access allows a remote device to retrieve switch information, while read/write access also allows a remote device to modify switch settings.
7. Follow the directions for setting up the Access Control List (below).

### 7.11.2 Setting Up the Access Control List

To set up the Access Control list as specified by a range of IP addresses, click the **SNMP Access Control** button at the bottom of the SNMP Access screen. The SNMP Access Control screen appears:

1. Click the **Add** button to create a new entry in the Access Control table.
2. Specify the IP address for the user(s) that have access. Enter an IP address only in the **Starting IP Address** column to specify an address for a single SNMP user. Enter both the **Starting IP Address** and **Ending IP Address** columns to specify a range of addresses for SNMP users.
3. Click **Ok** to save changes and return to the SNMP Access screen.

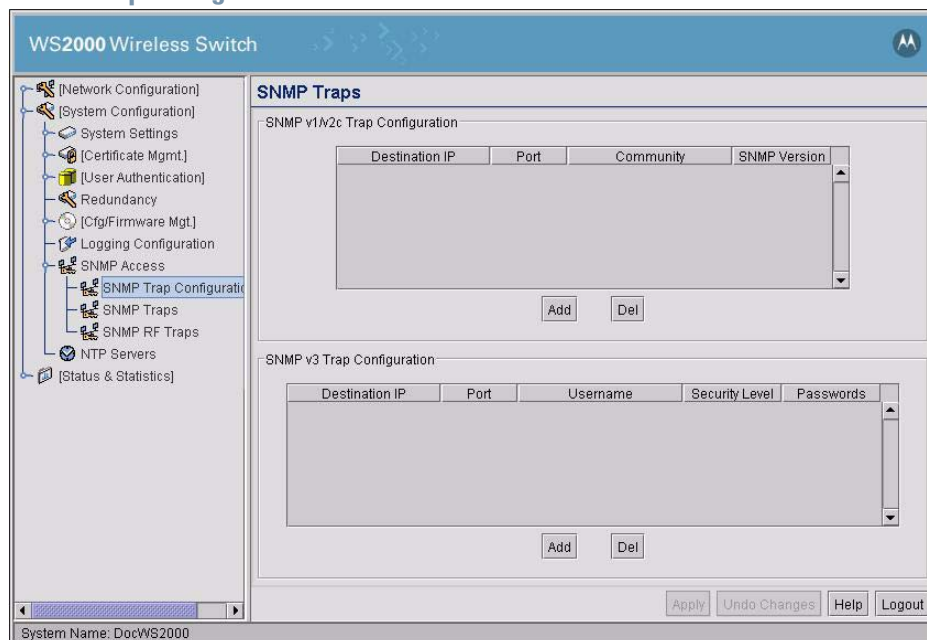


The dialog box titled "SNMP Access Control" contains the following elements:

- Instruction: "Enter IP Address Ranges to allow. (Leave the table blank to allow any IP)"
- Table with columns: Start IP, End IP
- Table content: 0 . 0 . 0 . 0, 0 . 0 . 0 . 0
- Buttons: Add, Del, Ok, Cancel, Help

### 7.11.3 Setting the Trap Configuration

To set the trap notification destination for SNMP, select **System Configuration --> SNMP Access --> SNMP Trap Configuration** from the left menu.



The "SNMP Traps" configuration screen shows the following structure:

- Left menu: WS2000 Wireless Switch > SNMP Access > SNMP Trap Configuration
- SNMP v1/v2c Trap Configuration table:
 

Destination IP	Port	Community	SNMP Version
- SNMP v3 Trap Configuration table:
 

Destination IP	Port	Username	Security Level	Passwords
- Buttons: Add, Del, Apply, Undo Changes, Help, Logout
- System Name: DocWS2000

### 7.11.4 Setting the Trap Configuration for SNMP v1/v2c

To set the trap notification destination for the SNMP v1/v2c servers, add one or more entries to SNMP v1/v2c Trap Configuration table.

1. Click the **Add** button to add a new entry to the table.
2. Specify a **Destination IP** addresses for the systems that will receive notification when an SNMP trap is generated.

3. Specify a destination User Datagram Protocol (UDP) port for receiving the traps that are sent by SNMP agents. UDP offers direct connection for sending and receiving datagrams over an IP network.
4. Specify a **Community** name that matches one of the community names added on the SNMP Access screen.
5. Select the appropriate **SNMP Version (v1 or v2)** from the pull-down menu for this particular SNMP server.
6. Click the **Apply** button to save the entries.

### 7.11.5 Setting the Trap Configuration for SNMP V3

To set the trap notification destination for the SNMP v3 servers, add one or more entries to SNMP v3 Trap Configuration table.

1. Click the **Add** button to add a new entry to the table.
2. Specify a **Destination IP** addresses for the systems that will receive notification when an SNMP trap is generated.
3. Specify a destination User Datagram Protocol (UDP) port for receiving the traps that are sent by SNMP agents. UDP offers direct connection for sending and receiving datagrams over an IP network.
4. Specify a **Username** that matches one of the user names added on the SNMP Access screen.
5. Specify a **Security** level from **noAuth** (no authorization required), **AuthNoPriv** (authorization without encryption), or **AuthPriv** (authorization with encryption).
6. Specify a password for the user.



**NOTE:** When entering the same username on the SNMP Traps and SNMP Access screens, the password entered on the SNMP Traps page will overwrite the password entered on the SNMP Access page. To avoid this problem enter the same password on both pages.

**Note**

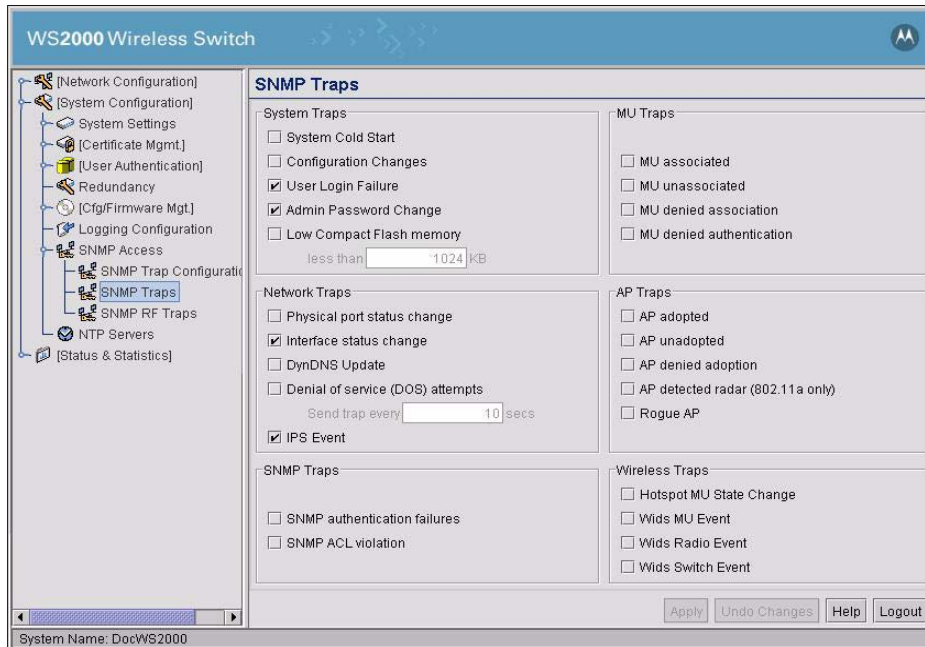
7. Click the **Apply** button to save changes

### 7.11.6 Selecting Traps

The SMNP Trap screen allow you to specify the types of network events that generate traps, and who to notify regarding the events. SNMP traps are generated according to predefined types of network events that are considered important to manage. This information is asynchronously reported to the switch's SNMP network-management system by switch-managed entities. Notification is sent to the responsible individuals whose IP addresses are listed for trap notification.



- To set the SNMP traps, select **System Configuration --> SNMP Access --> SNMP Traps** from the left menu.



- Check the type of traps to enable the generation of notification events.

Trap Category	Trap Name	Generates a Trap whenever...
System Traps	System Cold Start	The switch's router reinitializes while transmitting, possibly altering the agent's configuration or protocol entity implementation.
	Configuration Changes	SNMP access or management functions are reconfigured.
	User Login Failure	A user fails to successfully login from the CLI or Applet.
	Admin Password Change	A change is made to the Admin user password.
	Low Compact Flash Memory	The memory in the Compact Flash card in the system falls below the amount specified.
Network Traps	Physical port status change	The status changes for one of the ports on the front of the WS2000, such as if a device is plugged into or unplugged from the switch, or if the link is lost between the switch and the connected device.
	Interface Status Change	An interface on the switches status changes from its configured state.
	DynDNS Update	If Dynamic DNS services are configured on the WAN a new trap is set when there is a Dynamic DNS update.
	Denial of service (DOS) attempts	A Denial of Service attack is detected by the switch's firewall. A new trap will be sent at the interval specified until the attack has stopped.

<b>Trap Category</b>	<b>Trap Name</b>	<b>Generates a Trap whenever...</b>
	<b>IPS Event</b>	An Intrusion Prevention System event is detected by the switch's firewall. IPS Event traps are sent until the attack stops. These traps are internally rate-limited to prevent flooding of traps in case of heavy attack traffic on the network.
<b>SNMP Traps</b>	<b>SNMP authentication failures</b>	An SNMP-capable client is denied access to the switch's SNMP management functions or data. This may result from incorrect login
	<b>SNMP ACL violation</b>	An SNMP client cannot access SNMP management functions or data due to an Access Control List (ACL) violation
<b>MU Traps</b>	<b>MU associated</b>	An MU becomes associated with one of the switch's Wireless Local Area Networks (WLANs)
	<b>MU unassociated</b>	An MU becomes unassociated with (or gets dropped from) one of the switch's WLANs
	<b>MU denied association</b>	An MU cannot associate with the switch-managed network, for example due to an absent or incorrectly specified MAC address on a WLAN Security screen.
	<b>MU denied authentication</b>	An MU is denied authentication on one of the switch's WLANs, which can be caused by the MU being set for the wrong authentication type for the WLAN or by an incorrect key or password.
<b>AP Traps</b>	<b>AP adopted</b>	Any of the switch's Wireless Local Area Networks (WLANs) adopts an AP.
	<b>AP unadopted</b>	Any of the switch's WLANs unadopts (or drops) an AP.
	<b>AP denied adoption</b>	Any of the switch's WLANs deny the adoption of an AP.
	<b>AP detected radar (802.11a only)</b>	An 802.11a AP300 Access Port detects radar during its startup or ongoing radar scans. This trap only applies to the 802.11a radio of an AP300 Access Port operating with Dynamic Frequency Selection and Transmit Power Control (DFS/TPC).
	<b>Rogue AP</b>	A rogue (unauthorized) access port (AP) is detected. Several methods for rogue AP detection are employed by the switch. The detection process is non-disruptive and will not affect the performance of the switch. The detection functionality is greatly enhanced when the Approved AP list is filled out on the AP List screen under Rogue AP Detection.
<b>Wireless Traps</b>	<b>Hotspot MU State Change</b>	An MU using the switch's Hotspot feature is authenticated, unauthenticated or dropped.
	<b>WIDS MU Event</b>	A WIDS violation event is generated by a MU. For a list of WIDS violations, see <CROSS REFERENCE HERE>
	<b>WIDS Radio Event</b>	A WIDS violation event is generated by a radio. For a list of WIDS violations, see <CROSS REFERENCE HERE>
	<b>WIDS Switch Event</b>	A WIDS violation event is generated by the switch. For a list of WIDS violations, see <CROSS REFERENCE HERE>

3. Click the **Apply** button to save the trap settings.
4. It is necessary to tell the switch where to send the notifications. Make sure to set the trap configuration to indicate where to send the trap notifications.

### 7.11.7 Setting RF Traps

A screen is also available to specify traps caused when certain rates of activities either exceed or drop below a specified threshold. To set rate traps, select **System Configuration** --> **SNMP Access** --> **SNMP RF Traps** from the left menu.

		Switch	Wlan	Ap	Mu	
Pkts/s	greater than	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Pps
Throughput	greater than	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Mbps
Average Bit Speed	less than	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Mbps
% Non-Unicast	greater than	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	%
Average Signal	worse than	- <input type="text"/>	- <input type="text"/>	- <input type="text"/>	- <input type="text"/>	dBm
Average Retries	greater than	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Retries
% Gave Up	greater than	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	%
% Undecryptable	greater than	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	%
Associated Mus	greater than	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	

Minimum Packets

Minimum number of packets required for a trap to fire :

Apply Undo Changes Help Logout

System Name: DocWS2000

1. Select the threshold type for which you want a rate trap, such as Pkts/sec.
2. Determine whether you want the rate to apply to **Switch** (the switch as a whole), **Wlan** (for each WLAN enabled), **Ap** (each associated Access Port), or **Mu** (each mobile unit connected to the switch).
3. Type in the threshold rate into the field associated with the selected object.
4. Traps are only generated for those field where numbers exist. Explanation of the different threshold types are listed below.

<b>Pkts/s</b>	The maximum threshold for the number of packets per second before a trap is sent.
<b>Throughput</b>	The maximum threshold for the total throughput in Mbps (Megabits per second) for each of the devices before a trap is sent.
<b>Average Bit Speed</b>	The minimum threshold for the average bit speed in Mbps (Megabits per second) for each of the devices before a trap is sent.
<b>% Non-Unicast</b>	The maximum threshold for the total percentage of packets that are non-unicast for each of the devices before a trap is sent. Non-unicast packets include broadcast and multi-cast traffic.
<b>Average Signal</b>	The minimum threshold for the average signal strength in dBm for each of the devices before a trap is sent.

- Average Retries** The maximum threshold for the average number of retries for each of the devices before a trap is sent.
- % Gave Up** The maximum threshold for the total percentage of packets that are given up for each of the devices before a trap is sent.
- % Dropped** The maximum threshold for the total percentage of packets that are dropped for each of the devices before a trap is sent.
- % Undecryptable** The maximum threshold for the total percentage of packets that are undecryptable for each of the devices before a trap is sent. Undecryptable packets can be the result of corrupt packets, bad CRC checks, or incomplete packets.
- Associated MUs** The maximum threshold for the total number of MUs associated with each of the devices before a trap is sent.

Enter the minimum number of packets that must pass through the device before an SNMP rate trap will be sent. It is recommended to set this value no less than 1000.

## 7.12 Specifying a Network Time Protocol (NTP) Server

Network Time Protocol (NTP) manages time and clock synchronization in a network environment. The switch, which acts as an NTP client, periodically synchronizes its clock with a master clock on an NTP server. Time synchronization is typically optional (although recommended) for the switch's network operations; however, for sites using Kerberos authentication, time synchronization is required. Kerberos must synchronize the clocks of its Key Distribution Center (KDC) server(s).

Select **System Configuration** --> **NTP Servers** from the left menu to enable NTP. The NTP Server screen appears.

The screenshot shows the 'NTP Servers' configuration page in the WS2000 Wireless Switch web interface. On the left is a navigation menu with 'NTP Servers' selected. The main content area is divided into three sections: 'Current Time' showing 'Mon 1970-Jan-05 00:18:52 +0000 UTC (UTC)' with a 'Refresh' button; 'Manual Time Settings' with a 'Set Date/Time' button; and 'Server Configuration' which includes a checked 'Enable NTP on WS 2000' checkbox, a 'Time Zone' dropdown menu (currently showing 'UTC'), and three rows for time servers (Preferred, First Alternate, and Second Alternate) with IP Address and Port (default: 123) fields. A 'Synchronization Interval' of 15 minutes is also set. At the bottom are 'Apply', 'Undo Changes', 'Help', and 'Logout' buttons.

1. The field on the left of the Current Time area displays what the switch believes is the current time. Click the **Refresh** button to update that time. If an NTP server is configured, the switch will go out to the network to update its current time.
2. Specify a time zone by selecting the appropriate zone from the **Time Zone** list.

3. To set the time manually, click the **Set Date/Time** button. A sub-window displays where you can set the WS2000's time.

**Note**

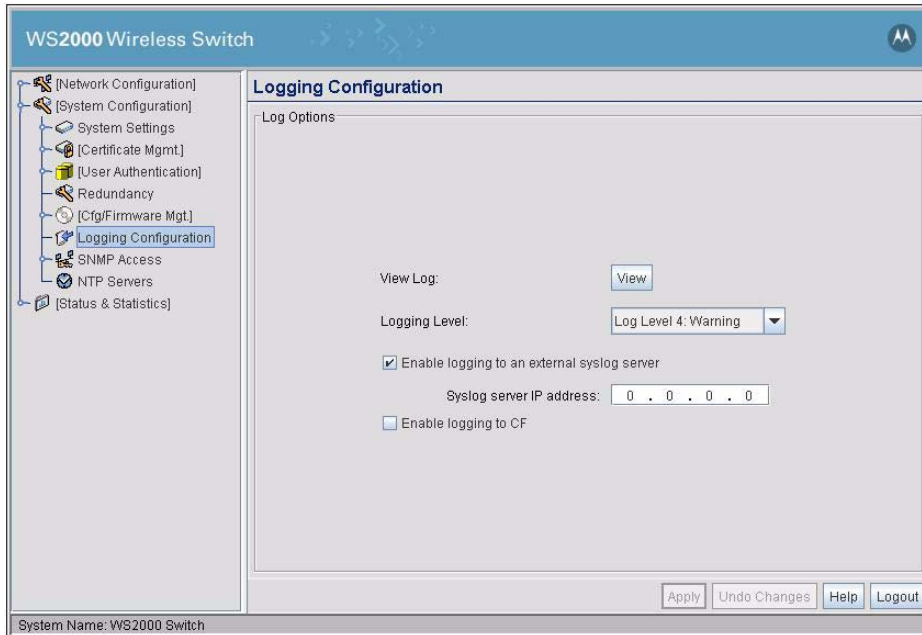
**NOTE:** When NTP is enabled on the WS2000, you will not be able to set time manually.

4. To enable time service on the switch, check the **Enable NTP on** check box and continue with the rest of the steps below.
5. Specify a **Preferred Time Server**, and optionally a **First Alternate Time Server** and a **Second Alternate Time Server** by specifying the IP address and Port for the time service for each server. The default port is 123. The more NTP servers specified, the greatest assurance there is of uninterrupted time synchronization.
6. Specify a **Synchronization Interval** (in minutes). By default, the switch will synchronize the time every 15 minutes.
7. Click the **Apply** button to save any changes made on this screen.

## 7.13 Setting Up and Viewing the System Log

The WS2000 Network Management System keeps a log of the events that happen on the switch. The switch has a modest amount of memory to store events. If the administrator wishes to keep a more complete event history, the administrator needs to enable a log server.

To view the log or set up a log server, select **System Configuration --> Logs** from the left menu.



### 7.13.1 Viewing the Log on the Switch

To save a log of the most recent events that are retained on the switch, click the **View** button. The system will display a prompt asking for the administrator password. After the password has been entered, click the **Get File** button and a dialogue will be displayed with buttons to **Open** or **Save** the log.txt file. Click **Save** and specify a location to save the file.

To view the saved log.txt file on a Microsoft Windows based computer use the WordPad application. Viewing the log file with Notepad, the default text file view on most Windows based computers, will not properly display the formatting of the log file.

### 7.13.2 Setting Up a Log Server

To keep a complete history of the events that are logged by the switch, the administrator needs to set up an external system log on a server. The server listens for incoming switch-generated syslog messages on a UDP port (514 by default), and then decodes the messages into a log file appropriate for viewing and printing. Events are categorized into eight levels (0 through 7), with the lowest numbers representing the most critical issues.

1. Set the level of the errors to be logged from the **Logging Level** drop-down menu. All events associated with the selected level and events with levels lower than the selection will be recorded.
2. Check the **Enable** logging in to an external syslog server check box to enable logging.
3. Specify the Syslog server IP address for the server that will store the log.

4. Check the **Enable logging to CF** check box to enable logging of events to a CF card on the switch. This is useful when the connection to the Syslog server is lost due to network disturbances or any other cause. When enabled, the event log is written to the CF card when the Syslog server is not available for any reason. When the Syslog server comes back on line, the logging is automatically done to the server.
5. Select **Apply** to save the changes.
6. Select **Network Configuration** --> **Subnet Access**. Work through all the combinations of subnet-to-WAN accesses to ensure that DNS communications are allowed. (UDP must be enabled to save the log entries.)

## 7.14 Commands to unmount a CF card

To unmount a CF card used to load firmware use these commands from the console.

```
admin> system
admin(system)> exec cfumount
```

To see the contents of the CF card use these commands from the console.

```
admin> system
admin(system)> cf
admin(system.cf)> ls
```

```
.
..
mf12.bin
mf_02020200003R.bin
admin(system.cf)>
```

You can also use these commands to view the contents of the CF card.

```
admin(system)> exec df -h /mnt/cf
```





## Configuring HotSpot

8.1 Overview .....	8-2
8.1.1 Requirements .....	8-2
8.2 Configuring Hotspot .....	8-2
8.2.1 Enabling Hotspot on a WLAN .....	8-3
8.2.2 Set Hotspot Configuration .....	8-4
8.2.3 Setting the User Access Policy .....	8-7
8.2.4 Defining the Hotspot State of a Mobile Unit .....	8-7
8.2.5 Handling log-in and redirection .....	8-8
8.2.6 Authentication (RADIUS) .....	8-8
8.2.7 Accounting (RADIUS) .....	8-8

## 8.1 Overview

The hotspot feature enables the WS2000 Wireless Switch to act as a single on-site solution to provide wireless LAN hotspots and management.

The hotspot access controller enables hotspot operators to provide user authentication and accounting without a special client application. It enables a web browser as a secure authentication device. Instead of relying on the built-in security features of 802.11 to control privileges to an access port, you can configure a WLAN as an open network with hotspot authentication. The WS2000 Wireless Switch provides an IP address to the user through its built-in DHCP server, authenticates the user, and enables the user to access the Internet.

### 8.1.1 Requirements

The hotspot feature requires the following:

HTTP redirection	Redirects unauthenticated users to a specific page specified by the Hotspot provider.
User authentication	Authenticates users using a RADIUS server.
Walled garden support	Enables a list of IP address (not domain names) to be accessed without authentication.
Billing system integration	Sends accounting records to a RADIUS accounting server.

## 8.2 Configuring Hotspot

To configure the hotspot access controller on the WS2000 Wireless Switch:

1. Configure a subnet as outlined in the LAN/Subnet Configuration chapter and enable hotspot on that WLAN.
2. Create a set of allowed destination IP addresses. These allowed destination IP addresses are also called a white list.

## 8.2.1 Enabling Hotspot on a WLAN

To enable hotspot on a WLAN:

1. Click **[Network Configuration]** --> **Wireless**. The *Wireless* screen is displayed.

WS2000 Wireless Switch

Wireless

WLAN Summary | AP Adoption Configuration

Enable	HotSpot	Name	ESSID	Subnet	Access Ports Adopted
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	OfficeN	OfficeNew	OfficeN	3,4
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Office	Office	Office	3,4
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Printer	Printer	Printer	3,4
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Guests	Guests	Guests	3,4
<input type="checkbox"/>	<input type="checkbox"/>	WLAN5	105		
<input type="checkbox"/>	<input type="checkbox"/>	WLAN6	106		
<input type="checkbox"/>	<input type="checkbox"/>	WLAN7	107		
<input type="checkbox"/>	<input type="checkbox"/>	WLAN8	108		

Miscellaneous

WEP Shared Mode

SIP CAC Mode

Legacy mode (AP300)

MU Inactivity Timeout:  Mins

HotSpot Session Timeout:  Mins

Apply Undo Changes Help Logout

System Name: TECHDOCSW

2. Select the **Hotspot** check box for the WLAN that will support Hotspot.
3. Click **Apply** to apply the changes made to this screen. Click **Undo Changes** to revert back to the previous settings.

This enables hotspot on the particular WLAN.



**Note**

**NOTE:** The **HotSpot Session Timeout** value controls the duration of inactivity after which the user is timed out of the hotspot. The default value for **HotSpot Session Timeout** is 20 minutes. You can enter a maximum of 1440 (1 day) minutes for this field.

## 8.2.2 Set Hotspot Configuration

Hotspots can be configured from the <WLAN Name> **Hotspot Config** screen. This screen allows you to configure the different parameters to enable users to use the hotspots.

The screenshot shows the 'WLAN3 Hotspot Config' screen on a WS2000 Wireless Switch. The left sidebar contains a navigation tree with categories like [Network Configuration], [System Configuration], and [Status & Statistics]. The main content area is divided into several panels:

- HTTP Redirection mode:** Radio buttons for 'https' (selected) and 'http'.
- Files Location:** Radio buttons for 'Use Default Files' (selected), 'Use CF Card', and 'Use External URL'.
- Radius Accounting:** A checkbox for 'Enable Accounting (Save to CF Card)' is unchecked. Below it are input fields for 'Timeout' (set to 1) and 'Retries' (set to 1).
- CF Card Files:** A section with the text 'Get the files and Press Apply.' and three buttons: 'Login', 'Welcome', and 'Fail'.
- External URL:** Input fields for 'Login Page URL', 'Welcome Page URL', and 'Fail Page URL'.
- WhiteList Configuration:** A button labeled 'White List Entries'.
- Radius Configuration:** Fields for 'Pri Server IP' (0.0.0.0), 'Pri Port' (1812), 'Pri Secret' (empty), 'Bind Intf (for Pri Server)' (NONE), 'Sec Server IP' (0.0.0.0), 'Sec Port' (1812), 'Sec Secret' (empty), and 'Bind Intf (for Sec Server)' (NONE). There is a 'Use Local Radius' button and a 'Radius auth-mode' dropdown set to 'PAP'.

At the bottom right, there are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name 'WS2000' is displayed at the bottom left.

To configure the hotspot for a WLAN:

1. Set the HTTP Redirection mode to either **http** or **https** by selecting the appropriate option. When a user successfully logs on using the hotspot, the user is redirected to a welcome screen. This selection decides the redirection mode.
2. Set the location of the files the user is redirected to by selecting one of the **Use Default Files**, **Use CF Card**, or **Use External URL** options.

To use the standard redirect HTML files, select the **Use Default Files** option.

To use redirect HTML files stored on a CF card loaded to the switch, use **Use CF Card** option. When selected, the **CF Card Files** area is enabled.

To use redirect HTML files stored on a different location on the local network, use the **Use External URL** option. When this option is selected, the **External URL** area is enabled.

### Radius Server Configuration

3. By default, hotspot user authentication is performed using a RADIUS server. This server could be on the network or you can use the onboard/local RADIUS server.

To use a RADIUS server located on the network, enter the appropriate information in the **Radius Configuration** area. You must enter the **IP Address**, **Port**, and the **Common Secret** for at least the

primary RADIUS server. To authenticate a hotspot user with a RADIUS server through a VPN tunnel select the bind interface from the **Bind Intf (for Pri Server)** drop down.

If the RADIUS server is on a network accessible through a VPN tunnel, then the tunnel must be configured. The bind interface should be the same as the Local Subnet configured for the VPN tunnel.

Entering information for the secondary RADIUS server is optional.

To authenticate a hotspot user with a RADIUS server, select the authentication mode from the **Radius auth-mode** drop down. You can use either **PAP** or **CHAP** as the authentication mode.

To use the RADIUS server located on the WS2000, click the **Use Local Radius** button. This sets the value of the Primary RADIUS Server IP to 127.0.0.1, the port to 1812. Enter the common secret for access in the **Pri Secret** field. You can also provide information for an external secondary RADIUS server.

### Radius Accounting Logs

4. The Radius Accounting area provides a feature by which user logins and logouts can be logged. This user accounting information can be sent to an external RADIUS server or to the installed CF card. using the onboard RADIUS server.

To enable logging of RADIUS accounting to the CF card, select the **Enable Accounting (Save to CF Card)** option.

Enter the **Timeout** value which is the duration (in seconds) for retransmitting the accounting request to the RADIUS server if no response is received from the server. The timeout value should be between 1-255 sec.

Enter the Retries value which is the number of times the accounting request is sent to the RADIUS server if no response is received, before logging is done on to the CF Card. The value should be between 1-10.

### White List Entries

5. The White List is a list of URLs the hotspot users can access without authentication. A maximum of 10 URLs can be created for each WLAN.

Click **White List Entries** button to enter and manage White List entries for the WLAN.



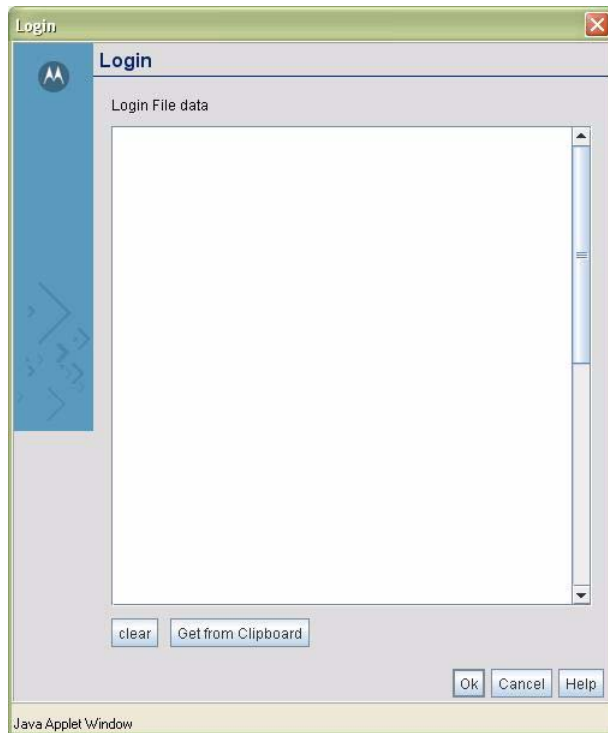
### Redirect Pages

Hotspot uses HTML pages to provide login and login status to the user. Three files are used. They are

- Login page
- Welcome page
- Fail page

When selecting **Use CF Card** to set the location where these files can be found, the **CF Card Files** area enables.

Use the **Login**, **Welcome**, and **Fail** buttons to enter the HTML files. This screen is displayed when **Login** button is clicked. Similar screens are displayed when **Welcome** and **Fail** buttons are clicked.



Type in the HTML code for the appropriate page. You can also paste the code from the clipboard by clicking the **Get from Clipboard** button.

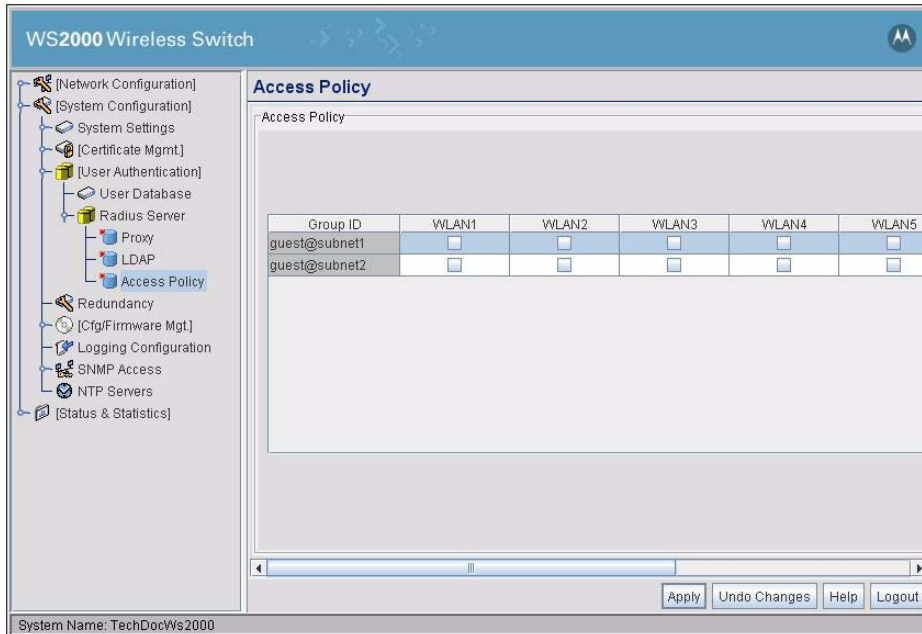
When selecting **Use External URL** to set the location where the files are located, the **External URL** area is enabled. Enter the fully qualified URL to the appropriate file in its text box.

### Creating Hotspot users

To create a new hotspot user quickly, see [Adding New Guest Users Quickly](#).

### 8.2.3 Setting the User Access Policy

The RADIUS Access Policy screen allows you to set WLAN access based on a user group defined on the User Database screen. Select **[User Authentication]** --> **RADIUS Server** --> **Access Policy** to set group access.



Each Group ID defined in the User Database screen appears on the Access Policy screen as a single row in the table. Each wireless LAN represents a column in the table.

1. To enable group access to a particular WLAN, check the box for that WLAN in the row corresponding to the group. To disable access for a group, uncheck the box for the appropriate WLAN. A group must have at least one WLAN checked to have wireless access to the switch.
2. Click **Apply** when you have finished the changes.

### 8.2.4 Defining the Hotspot State of a Mobile Unit

When configured as a hotspot, the switch tracks the hotspot-state of each mobile unit associated with the hotspot. The server maintains a list of all mobile units associated and tracks the state of these mobile units.

Mobile Units in a hotspot have one the following two states:

- **REDIRECT state**—The associated mobile unit enters the REDIRECT state after 802.11 authentication and association. The mobile unit remains in this state until it successfully authenticates through the RADIUS server. After the mobile unit logs-off from the hotspot, it moves into the REDIRECT State.
- **RADIUS AUTHENTICATED state**—The mobile unit moves into the RADIUS AUTHENTICATED state after it successfully authenticates through the RADIUS server.

The RADIUS server provides the trigger to move the state of the mobile unit from REDIRECT to RADIUS AUTHENTICATED. There is a dedicated socket connection between the wireless switch and an the RADIUS server for this purpose.

After the RADIUS server successfully authenticates the mobile unit, it sends a trigger to the wireless switch to change the hotspot-state of the mobile unit to RADIUS-AUTHENTICATED.



When the mobile unit requests the RADIUS server to log out, the RADIUS server again sends a trigger to the wireless switch to change the state of the mobile unit to REDIRECT.

## 8.2.5 Handling log-in and redirection

When a client requests a URL from a web server, the login handler returns an HTTP redirection status code in the range 300-399 (for example, **301 Moved Permanently**), which indicates to the browser that it should look for the page at another URL.

This other URL can be a local or remote login page (based on the hotspot configuration). The login page URL is specified in the location HTTP header.

After the response with status code **301 Moved Permanently**, the client's browser issues a request for the URL specified in the response header. The client's browser, then displays the WS2000 login page.

To host a login page on the external web server, the IP address of that web server should be in the White list (list of IP addresses that are allowed to access the server) configuration. Ensure that the login page is designed so that the submit action always posts the login data on the WS2000 Wireless Switch.

When the login information is submitted to the WS2000 Wireless Switch, the login handler runs a CGI script that uses this data as input and sends the user the response from the CGI script.

## 8.2.6 Authentication (RADIUS)

The CGI script has a RADIUS client built in it, which receives the posted login data and initiates RADIUS authentication.

If the RADIUS authentication for that user is successful, the CGI script does the following:

1. Sends a command to wireless switch to change the MU state from REDIRECT to RADIUS-AUTHENTICATED.
2. Replies back to the login handler to generate an HTTP redirection response for Welcome page.
3. Starts the RADIUS accounting for the user.

The Welcome page will contain **Logout** button, which user can click at any point to logout from the system. Again the Remote Welcome page needs to be setup such that the logout request should be sent to WS2000.

If the RADIUS authentication for that user is failed the CGI script will reply back to the Login Handler to generate an HTTP redirection response for Fail page.

4. Click the **Logout** button on the Welcome page to log out of the switch at any point.

Upon logout another CGI script is executed. The CGI script will use REMOTE\_ADDR environment variable to get the IP address of the requester and verify its MAC address from ARP table. Then CGI script will stop the RADIUS accounting for that client and sends a command to wireless switch to change the MU state back to REDIRECT.

To create new guest hotspot users see [Chapter 6, Adding New Guest Users Quickly](#).

## 8.2.7 Accounting (RADIUS)

Upon successful login a CGI script will generate an Accounting Start packet describing the type of service being delivered and the client. The script will then send that information to the RADIUS Accounting server, which will reply with an acknowledgement that the packet has been received.

If a client logs out or an MU is dis-associated, an Accounting Stop packet will be generated describing the type of service that was delivered, the statistics, and the elapsed time. That packet will be sent to the RADIUS accounting server, which replies with an acknowledgement that the packet has been received.

## Using DDNS

9.1 Overview .....	9-2
9.2 Enabling DDNS .....	9-2
9.3 Updating DNS Entries using DDNS .....	9-4
9.3.1 Updating DNS Entries for a Single Subnets .....	9-4
9.3.2 Updating DNS Entries for All Active Subnets .....	9-5

## 9.1 Overview

When browsing web sites or sending E-mail messages a domain name is used. For example, the URL [www.yahoo.com](http://www.yahoo.com) and the e-mail address [user@yahoo.com](mailto:user@yahoo.com) contains the domain name yahoo.com. Domain names allow users to remember the address to a site without knowing the IP address. For traffic to be routed on a network those domain names must first be converted to an IP address. When a domain name is entered the domain is translated to an IP address by a Domain Name Server (DNS).

DNS translation poses the following challenges:

- There are a limited number of IP addresses currently available.
- Domain names and IP addresses are created and changed everyday.

Dynamic Domain Name System (DDNS) enables you to link a domain name to a changing IP address. When you connect to the Internet, your Internet service provider uses Dynamic Host Configuration Protocol (DHCP) and assigns the domain an unused IP address from a set pool of IP addresses. This IP address is only used for the duration of this specific connection. This method of dynamically assigning addresses, increases the pool of available IP addresses.

The DDNS service maintains a database to connect a domain name to an IP address on the Internet. Because the IP addresses change, it is necessary to update the DNS database with the current IP address for a given domain name. The DDNS service performs these updates.

Enabling Dynamic DNS will allow domain name information to be updated when the IP address associated with that domain changes. When a MU associates and gets an IP address from the DHCP server the DHCP server then updates the DNS server with the IP allocated to the corresponding hostname.

## 9.2 Enabling DDNS

Dynamic DNS is configured on a per-subnet basis and requires the subnet to be configured as a DHCP Server. DDNS is then enabled and configured in the Advanced DHCP Server screen for the corresponding subnet.

1. From the Subnet screen for the desired subnet select the **This interface is a DHCP Server** option.

The screenshot shows the configuration interface for a WS2000 Wireless Switch. The main window is titled "WS2000 Wireless Switch" and "WS2K1". The left sidebar shows a navigation tree with options like LAN, VLAN, WAN, Wireless, Firewall, Port Config, Router, IP Filtering, URL Filtering, System Configuration, and Status & Statistics. The main area is divided into "Subnet Config" and "Bridge Config" tabs. The "Subnet Config" tab is active, showing the following fields:

- Name:** WS2K1
- IP Parameters:**
  - IP Address: 192 . 168 . 0 . 1
  - Network Mask: 255 . 255 . 255 . 0
  - Default Gateway: 192 . 168 . 0 . 1
- Interfaces:**
  - Assigned: Port1, Port2, Port3, Port4, Port5, Port6, WLAN1
  - Available: WLAN5, WLAN6, WLAN7, WLAN8
  - Buttons: <- Add, Delete ->
- DHCP:**
  - This interface does not use DHCP
  - This interface is a DHCP Client
  - This interface is a DHCP Server
  - Address Assignment Range: 192 . 168 . 0 . 100 to 192 . 168 . 0 . 254
  - Buttons: Advanced DHCP Server, Update DNS
  - This interface is a DHCP Relay
  - Relay server IP: 0 . 0 . 0 . 0

At the bottom of the interface, there are buttons for "Apply", "Undo Changes", "Help", and "Logout". The status bar at the very bottom indicates "System Name: DocWS2000".

2. Enter a range of IPs in the **Address Assignment Range** fields.
3. Click the **Advanced DHCP Server** button to open the Advanced DHCP window.

The screenshot shows the 'Advanced DHCP Server' configuration window. The 'Enable Dynamic DNS' checkbox is unchecked. The 'Single User Class Option' radio button is selected. The 'Multiple User Class Option' radio button is unselected. The 'Primary DNS Server', 'Secondary DNS Server', and 'Default Gateway' fields all contain the IP address '192.168.0.1'. The 'WINS Server' field contains '192.168.0.254'. The 'DHCP Lease Time (sec)' field contains '86400'. The 'Domain Name', 'DNS Forward Zone', 'TFTP Server Address', 'Bootfile', 'Option 189', and 'Option 43' fields are empty. The 'Static DHCP Mappings' table is empty. The 'Add', 'Del', 'Ok', 'Cancel', and 'Help' buttons are visible at the bottom.

4. In the Advanced DHCP Server window check the box next to **Enable Dynamic DNS**.
5. Select either **Single User Class Option** or **Multiple User Class Option** depending on the settings of your DHCP clients.

Any DHCP client can send the User Class Id either in the Single or Multiple user class ID format. The Single or Multiple User class option is provided to enable the switch to interpret the correct format in which the user class ID is sent by the client. The switch then retrieves the correct value of the user class ID sent by the DHCP client based on the selected format. This same user class ID format is used for the DDNS messages.

6. Enter IP Addresses in **Primary DNS Server**, **Secondary DNS Server** and **Default Gateway** and click the **Ok** button to return the Subnet configuration screen.
7. Click the **Apply** button on the Subnet configuration screen to save the changes and activate DDNS for that subnet.

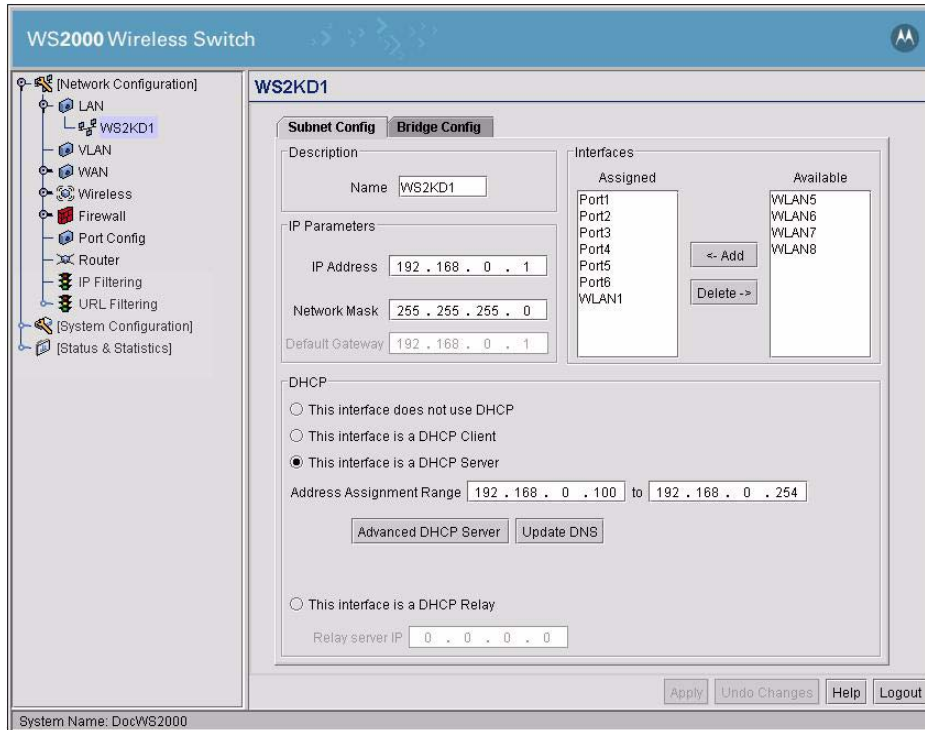
## 9.3 Updating DNS Entries using DDNS

Once DDNS has been configured and enabled for a subnet, it is possible to manually refresh the DNS entries for all active DHCP clients on a single subnet or on all active subnets.

### 9.3.1 Updating DNS Entries for a Single Subnets

The DNS entries for a single subnet can be updated using the following steps.

1. Select the subnet you wish to refresh from the menu tree on the left side of the screen.



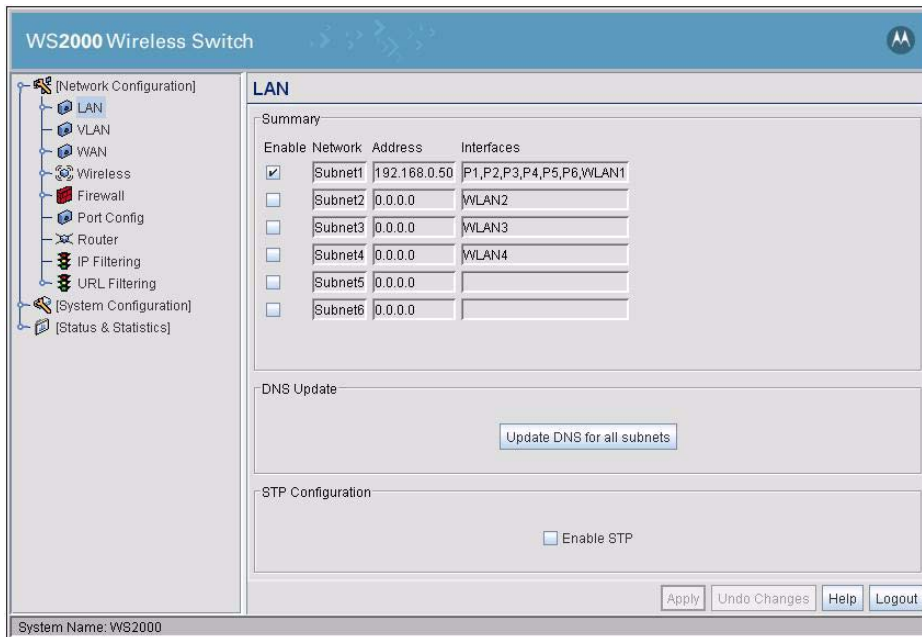
2. From the Subnet configuration screen click the **Update DNS** button located in the DHCP section of the screen.

After the Update DNS button has been clicked, an ADD DNS message for all the active leases on the DHCP server for that subnet is sent to the DNS server. A DELETE DNS message for all the inactive leases on the DHCP server for that subnet is sent to the DNS server.

### 9.3.2 Updating DNS Entries for All Active Subnets

The DNS entries for all active subnets can be updated using the following steps.

1. Select **LAN** from menu tree on the left side of the screen.



2. From the DNS Update section of the screen click the **Update DNS for All Subnets** button located in the DHCP section of the screen.

After the **Update DNS for All Subnets** button has been clicked, an ADD DNS message for all the active leases on the DHCP servers for all active subnets is sent to the DNS server. A DELETE DNS message for all the inactive leases on the DHCP server for all active subnets is sent to the DNS server.





# 10

## ***Trunking VLANs Through the WAN Port***

10.1 Overview .....	10-2
10.1.1 Assigning VLAN Tags to Packets .....	10-2
10.1.2 Installation Considerations and Default VLAN Settings .....	10-2
10.2 Configuring VLAN Trunking .....	10-3
10.2.1 Mapping VLANs to VLANs .....	10-4

## 10.1 Overview

Earlier versions of WS2000 had a limit of 31 VLAN IDs (IDs 1-31) due to LAN port switch hardware limitations. It was difficult to seamlessly integrate the WS2000 with existing network topology of VLANs with VLAN IDs greater than 31.

To enable easier integration into networks with existing VLAN infrastructure, you can now configure the existing WAN port as a Trunk-Port and the user can configure any VLAN-IDs in the range 1-4094. With this setup, the WAN port can be configured either as a TRUNK port or as a WAN Link.

### 10.1.1 Assigning VLAN Tags to Packets

VLAN tag assignment to packets is achieved as follows:

- Wired hosts are assigned VLANs based on the Port to which they are connected.
- Wireless hosts, upon successful authentication, are assigned VLANs based on the WLAN through which they authenticate.

The WS2000 then maintains a table to store the hosts to VLAN mapping information.

Packets coming in from the LAN ports are handled as follows:

- For unicast packets destined to hosts on the same VLAN, the LAN switch handles the packet if both the hosts are wired.
- For unicast packets destined to hosts on different VLANs, the WS2000 switches the packet.
- For broadcast packets, the same packet is duplicated and forwarded to all ports and WLANs on the same VLAN.

### 10.1.2 Installation Considerations and Default VLAN Settings

By default the WAN port is configured as a WAN LINK. This port has a default VLAN ID of 1.

After upgrading the WS2000 to version 2.1 or above, the WAN port can be configured as either a WAN Link or as a TRUNK port. The user can configure any VLAN IDs between 1 and 4094.

The Factory Setting for the WS2000 Version 2.1 would be as follows:

- Native VLAN by default is VLAN ID 1
- No Trunk Port is configured.
- The WAN port is configured as a WAN Link.
- No VLANs are enabled for Trunking.

## 10.2 Configuring VLAN Trunking

Use the following steps to configure VLAN trunking on the WAN port.

1. Select **Network Configuration --> VLAN** to open the VLAN Configuration screen.

1. Use the pull-down menu to select a **VLAN Type** for this switch. The two options are **User Based** and **Port Based**.

**Port-based VLANs** partitions traffic based on port on which the packet is received. The switch inspects each packet, extracts the port on which it was received (from control information provided by the driver) and processes the packet based on the port. The port is mapped to a subnet and each subnet is mapped to a single VLAN. The switch processes the packet based on this mapping.

**User-based VLAN** traffic classification is performed only for Wireless traffic. The VLAN for a particular MU is identified when the MU authenticates itself with the RADIUS server using a user ID and password. The RADIUS server provides the VLAN ID corresponding to this MU and User ID information combination. The switch processes the packet based on the VLAN ID provided by the RADIUS server.

For wired traffic, the classification as done in Port-based VLANs applies.

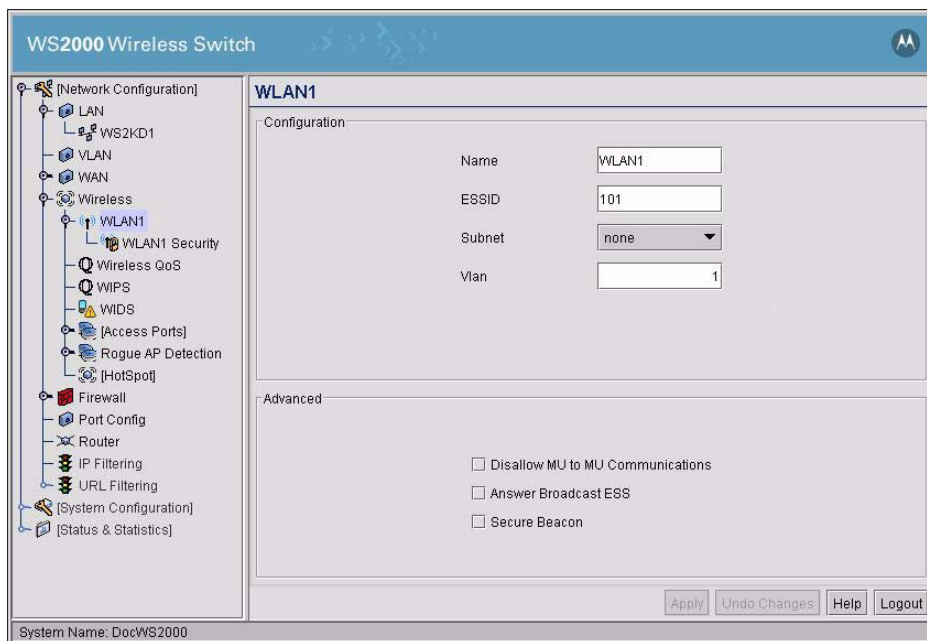
2. Use the pull-down menu to select a **Trunk Port** for the switch. Only the WAN port can be configured as the Trunk Port.
3. Enter the **Default VLAN ID** to be used for packets that do not have the VLAN tag inserted. The default VLAN ID must be one of the IDs assigned to the subnets if the **VLAN Type** is *Port Based*. If the **VLAN Type** is *User Based*, then the **Default VLAN ID** must be one from the **Allowed VLANs** list.
4. For each enabled Subnet, enter the **VLAN ID**.
5. Enter a list of allowed VLANs between 1 and 4094 in the **Allowed VLANs** box. The VLANs in this list will be allowed access through the WAN port. When entering multiple VLAN IDs, separate each ID with a comma. When entering a range of VLAN IDs, separate the starting and ending values with a "-".

6. To enable filtering using IP, check the **Enable IP Filtering** check box. This option is only available only when **Trunk Port** is set to *Wan*. To add an IP filter, click **IP Filtering** button. The *IP Filtering* dialog appears. Set the appropriate filter and click **Ok** to close the dialog.
7. Click **Ok** on the *VLAN Configuration* screen to save changes.

## 10.2.1 Mapping WLANs to VLANs

Use the following steps to map a VLAN, that is not already a part of any subnet, to a WLAN:

1. Select the desired WLAN from the menu.
2. From the Subnet pulldown menu select **none**. The WLAN is now not associated with any subnet and the VLAN field can now be edited.
3. Enter a VLAN ID in the **VLAN** field to map that VLAN ID to the current WLAN.



4. Click the **Apply** button to save the changes.

## ***Status & Statistics***

11.1 WAN Statistics .....	11-2
11.2 Subnet Statistics .....	11-3
11.2.1 Subnet Lease stats .....	11-3
11.2.2 Subnet Stats .....	11-5
11.2.3 STP Stats .....	11-6
11.3 Wireless LAN Statistics .....	11-8
11.3.1 Displaying WLAN Summary Information .....	11-8
11.3.2 Getting Statistics for a Particular WLAN .....	11-10
11.3.3 General WLAN Information .....	11-11
11.4 Access Port Statistics .....	11-12
11.4.1 Access Port Statistics Summary Screen .....	11-12
11.4.2 Detailed Information About a Particular Access Port .....	11-13
11.4.3 General Access Port Information .....	11-14
11.6 Mesh Statistics .....	11-17
11.6.1 Mesh Base Connections .....	11-17
11.6.2 Mesh Client Connections .....	11-17
11.7 Intrusion Prevention Statistics .....	11-19
11.8 View Statistics in Graphic Form .....	11-19

## 11.1 WAN Statistics

The WS2000 Network Management System provides a set of screens that allow the administrator to view real-time statistics for monitoring the switch's activity. One of those screens displays statistics for the Wide Area Network (WAN) port. Selecting **Status & Statistics** --> **WAN Stats** displays the following screen.

WAN Stats			
<b>Information</b>			
Status:	Enabled	IP Addresses:	157.235.208.59
HW Address:	00:A0:F8:71:1B:05		
Mask:	255.255.255.0		
Link:	Up		
Speed:	100 Mbps		
<b>Received</b>			
RX Packets:	73087	RX Errors:	1
RX Bytes:	21856595	RX Dropped:	0
		RX Overruns:	0
		RX Frame:	1
<b>Transmitted</b>			
TX Packets:	18928	TX Errors:	0
TX Bytes:	10073408	TX Dropped:	0
		TX Overruns:	0
		TX Carrier:	0

The **Information** portion of the WAN Stats screen displays general information about the WAN. Much of this information is generated from settings on the WAN screen in the Network Configuration area.

- The **Status** field displays “Enabled” if the WAN interface is currently enabled on the WAN screen (**Network Configuration** --> **WAN**). If the WAN interface is disabled on the WAN screen, the **WAN Stats** screen does not display connection information and statistics.
- The **HW address** is the Media Access Control (MAC) address of the switch's WAN port, which is set at the factory.
- The **Mask** field displays the subnet mask number for the switch's WAN connection. This number is set on the WAN screen.
- The **Link** field displays “Up” if the WAN connection is active, and “Down” if the WAN connection is interrupted or lost.
- The WAN connection speed is displayed in Megabits per second (Mbps), for example, 100 Mbps, in the **Speed** field.
- The **IP addresses** displayed here for the WAN connection are set on the WAN screen (**Network Configuration** --> **WAN**).

The Received and Transmitted portions of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the WAN interface, since the WAN was last enabled or the switch was last rebooted.

Received Field	Description
<b>RX Packets</b>	The total number of data packets received over the WAN connection
<b>RX Bytes</b>	The total number of bytes of information received over the WAN connection

Received Field	Description
<b>RX Errors</b>	The total number of errors including dropped data packets, buffer overruns, and frame errors on inbound traffic
<b>RX Dropped</b>	The number of data packets that failed to reach the WAN interface
<b>RX Overruns</b>	The total number of buffer overruns (when packets are received faster than the WAN interface can handle them)
<b>RX Frame</b>	The total number of TCP/IP data frame errors received

Transmitted Field	Description
<b>TX Packets</b>	The total number of data packets sent over the WAN connection
<b>TX Bytes</b>	The total number of bytes of information sent over the WAN connection
<b>TX Errors</b>	The total number of errors including dropped data packets, buffer overruns, and carrier errors that fail on outbound traffic
<b>TX Dropped</b>	The number of data packets that fail to get sent from the WAN interface
<b>TX Overruns</b>	The total number of buffer overruns (when packets are sent faster than the WAN interface can handle them)
<b>TX Carrier</b>	The total number of TCP/IP data carrier errors received

## 11.2 Subnet Statistics

The WS2000 Network Management System provides a set of screens that allow the administrator to view real-time statistics for monitoring the switch's activity. The screens provided are:

- Subnet Lease stats screen
- One screen for each of the defined subnets
- Spanning Tree Protocol (STP) stats for each of the defined subnets

### 11.2.1 Subnet Lease stats

The Subnet Lease stats screen provides information about each DHCP lease for clients on the enabled subnets. To display the *Subnet Lease stats* screen, select **Status & Statistics --> Subnet Stats** from the left menu.

**WS2000 Wireless Switch**

**Subnets Lease stats**

Leases

Idx	IP	MAC	Life Left	Lease Start	Lease End
1	192.168.0.135	00:15:70:15:2B:B9	86343	Thu Jan 1 06:11:20 1970	Fri Jan 2 06:11:20 1970
2	192.168.0.122	00:A0:F8:D3:11:77	86132	Thu Jan 1 06:07:49 1970	Fri Jan 2 06:07:49 1970
3	192.168.0.133	00:A0:F8:D1:06:E8	85942	Thu Jan 1 06:04:39 1970	Fri Jan 2 06:04:39 1970
4	192.168.0.118	00:A0:F8:EF:32:9C	85936	Thu Jan 1 06:04:33 1970	Fri Jan 2 06:04:33 1970
5	192.168.0.105	00:15:70:17:B2:42	85884	Thu Jan 1 06:03:41 1970	Fri Jan 2 06:03:41 1970
6	192.168.0.134	00:A0:F8:D1:07:0E	85844	Thu Jan 1 06:03:01 1970	Fri Jan 2 06:03:01 1970
7	192.168.0.110	00:15:70:15:73:5A	85818	Thu Jan 1 06:02:35 1970	Fri Jan 2 06:02:35 1970
8	192.168.0.115	00:A0:F8:EE:98:33	85784	Thu Jan 1 06:02:01 1970	Fri Jan 2 06:02:01 1970
9	192.168.0.132	00:A0:F8:E8:D2:D6	85757	Thu Jan 1 06:01:34 1970	Fri Jan 2 06:01:34 1970
10	192.168.0.113	00:15:70:4B:BC:62	83853	Thu Jan 1 05:29:50 1970	Fri Jan 2 05:29:50 1970
11	192.168.0.131	00:A0:F8:BB:08:9F	83530	Thu Jan 1 05:24:27 1970	Fri Jan 2 05:24:27 1970
12	192.168.0.130	00:15:70:34:80:89	83178	Thu Jan 1 05:18:35 1970	Fri Jan 2 05:18:35 1970
13	192.168.0.129	00:15:70:46:8E:A9	83168	Thu Jan 1 05:18:25 1970	Fri Jan 2 05:18:25 1970
14	192.168.0.125	00:15:70:50:63:A7	81962	Thu Jan 1 04:58:19 1970	Fri Jan 2 04:58:19 1970
15	192.168.0.128	00:15:70:44:5E:15	81884	Thu Jan 1 04:57:01 1970	Fri Jan 2 04:57:01 1970
16	192.168.0.127	00:15:70:4E:2C:4B	81859	Thu Jan 1 04:56:36 1970	Fri Jan 2 04:56:36 1970
17	192.168.0.126	00:15:70:44:5E:12	81853	Thu Jan 1 04:56:30 1970	Fri Jan 2 04:56:30 1970
18	192.168.0.106	00:A0:F8:BC:2B:EC	80760	Thu Jan 1 04:38:17 1970	Fri Jan 2 04:38:17 1970
19	192.168.0.124	00:15:70:49:17:CD	80475	Thu Jan 1 04:33:32 1970	Fri Jan 2 04:33:32 1970
20	192.168.0.101	00:A0:F8:D3:7C:79	79828	Thu Jan 1 04:22:45 1970	Fri Jan 2 04:22:45 1970

System Name: WS2000

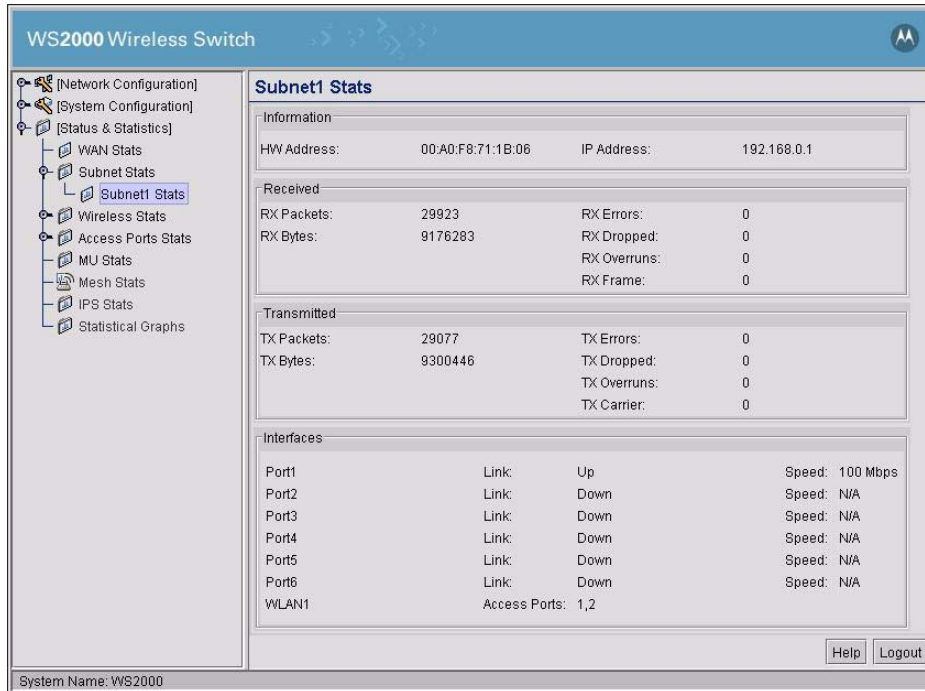
The following information is displayed:

- The **Idx** field displays a unique number for each of the DHCP client lease.
- The **IP** field displays the IP address assigned to the client by the DHCP server.
- The **MAC** field displays the MAC address of each of the DHCP clients. This address is for the network interface on the specified client.
- The **Life Left** field displays the remaining lease time in seconds for each DHCP lease.
- The **Lease Start** field displays the Day, Date, Time, and Year when each of the DHCP lease was started.
- The **Lease End** field displays the Day, Date, Time, and Year when each DHCP lease expires.



## 11.2.2 Subnet Stats

The Subnet Stats screens displays statistics for each of the subnets. Selecting **Status & Statistics --> Subnet Stats --> <Subnet Name> Stats** from the left menu displays the following screen.



The **Information** portion of the Subnet Stats screen displays general information about the subnet.

- The HW address is the Media Access Control (MAC) address of the switch’s WAN port, which is set at the factory.
- The IP addresses displayed here for the subnet connection are set on the subnet screen (**Network Configuration --> WLAN --> <subnet name>**).

The Received and Transmitted portions of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the WAN interface since the WAN was last enabled or the switch was last rebooted.

Received Field	Description
<b>RX Packets</b>	The total number of data packets received over the subnet
<b>RX Bytes</b>	The total number of bytes of information received over the subnet
<b>RX Errors</b>	The total number of errors including dropped data packets, buffer overruns, and frame errors on inbound traffic
<b>RX Dropped</b>	The number of data packets that failed to reach the subnet
<b>RX Overruns</b>	The total number of buffer overruns (when packets are received faster than the subnet can handle them)
<b>RX Frame</b>	The total number of TCP/IP data frame errors received

<b>Transmitted Field</b>	<b>Description</b>
<b>TX Packets</b>	The total number of data packets sent over the subnet
<b>TX Bytes</b>	The total number of bytes of information sent over the subnet
<b>TX Errors</b>	The total number of errors including dropped data packets, buffer overruns, and carrier errors that fail on outbound traffic
<b>TX Dropped</b>	The number of data packets that fail to get sent from the subnet
<b>TX Overruns</b>	The total number of buffer overruns (when packets are sent faster than the subnet can handle them)
<b>TX Carrier</b>	The total number of TCP/IP data carrier errors received

### 11.2.2.1 Interfaces

The interfaces section of the screen displays information about the ports and Access Ports associated with the subnet (set in **Network Configuration** --> **Subnet** --> <Subnet Name>).

The area shows the status of the port-subnet link and the speed of the connection. The **Link** field displays "Up" if the adjacent port is active, and "Down" if the adjacent port is inactive. When a port's link status is "Up" the speed of the link (in Mbps) will be listed in the **Speed** field.

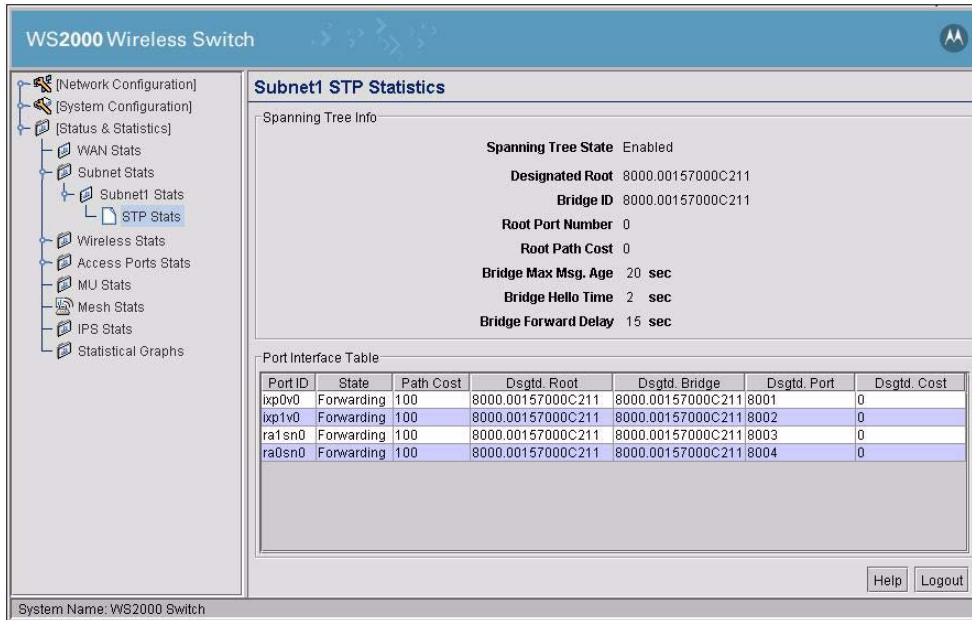
The area also shows the status of the port-WLAN associations. In this case, the adopted **Access Ports** for each of the associated WLANs are listed.

### 11.2.3 STP Stats

Spanning Tree Protocol (STP) is a OSI Layer-2 protocol for Bridged LANs. Spanning Tree Protocol (STP) is a OSI Layer-2 protocol for a bridged LAN. It creates a spanning tree within a Mesh network of connected bridges and disables links that are not a part of the tree leaving a single active path between any two network nodes.

The protocol allows a network design to include redundant links to provide an automatic backup path(s) in case the primary path fails avoiding loops between bridges or any manual intervention.

Selecting the [Status & Statistics]-->Subnet Stats--><Subnet Name> Stats-->STP Stats displays the following screen.



The Spanning Tree Info portion of the screen displays the following information:

Field	Description
<b>Spanning Tree State</b>	Displays whether the spanning tree state is currently enabled or disabled. The spanning tree state must be enabled for a unique spanning-tree calculation to occur when the bridge is powered up or when a topology change is detected.
<b>Designated Root</b>	Displays the access point MAC address of the bridge defined as the root bridge in the Bridge STP Configuration screen.
<b>Bridge ID</b>	The Bridge ID identifies the priority and ID of the bridge sending the message
<b>Root Port Number</b>	Identifies the root bridge by listing its 2-byte priority followed by its 6-byte ID.
<b>Root Path Cost</b>	Bridge message traffic contains information identifying the root bridge and the sending bridge. The root path cost represents the distance (cost) from the sending bridge to the root bridge.
<b>Bridge Max Msg. Age</b>	The Max Msg Age measures the age of received protocol information recorded for a port, and to ensure the information is discarded when it exceeds the value set for the Maximum Message age timer.
<b>Bridge Hello Time</b>	The Bridge Hello Time is the time between each bridge protocol data unit sent. This time is equal to 2 seconds (sec) by default, but can be tuned between 1 and 10 sec. The 802.1d specification recommends the Hello Time be set to a value less than half of the Max Message age value.
<b>Bridge Forward Delay</b>	The Bridge Forward Delay value is the time spent in a listening and learning state. This time is equal to 15 sec by default, but can be set between 4 and 30 sec.

The screen also provide comprehensive information on the port interfaces used. This information is displayed in the form of a table in the Port Interface Table portion of the screen.

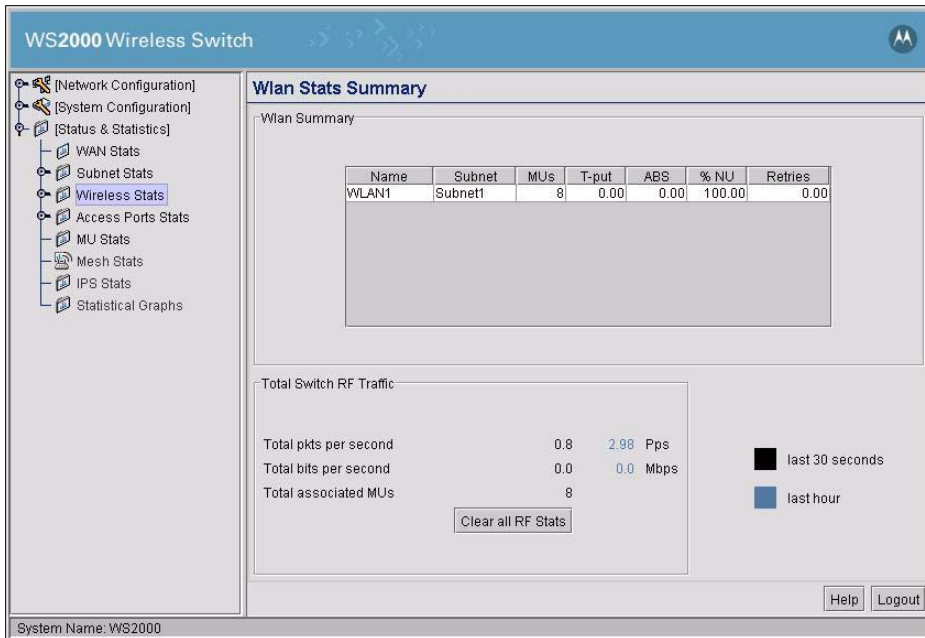
<b>Field</b>	<b>Description</b>
<b>Port ID</b>	Identifies the port from which the configuration message was sent.
<b>State</b>	Displays whether a bridge is forwarding traffic to other members of the mesh network (over this port) or blocking traffic. Each viable member of the mesh network must forward traffic to extent the coverage area of the mesh network.
<b>Path Cost</b>	The root path cost is the distance (cost) from the sending bridge to the root bridge.
<b>Dsgtd. Root</b>	Displays the MAC address of the access point defined with the lowest priority within the Mesh STP Configuration screen.
<b>Dsgtd. Bridge</b>	There is only one root bridge within each mesh network. All other bridges are designated bridges that look to the root bridge for several mesh network timeout values.
<b>Dsgtd. Port</b>	Each designated bridge must use a unique port. The value listed represents the port used by each bridge listed within the table to route traffic to other members of the mesh network.
<b>Dsgtd. Cost</b>	Displays the unique distance between each access point MAC address listed in the Designated Bridge column and the access point MAC address listed in the Designated Root column.

## 11.3 Wireless LAN Statistics

The WS2000 Network Management System provides screens that display information about all of the switch's wireless operations as well as information for each enabled wireless LAN (WLAN). Both screens are described in this section.

### 11.3.1 Displaying WLAN Summary Information

To see a summary information about wireless operations, select **Status & Statistics** --> **Wireless Stats** from the left menu.



The WLAN Summary section of the screen shows basic statistics about the currently enabled WLANs.

<b>Name</b>	The WLAN name.
<b>Subnet</b>	Displays the name of the subnet that is associated with the WLANs.
<b>MUs</b>	Displays the number of mobile units associated with this WLAN.
<b>T-put</b>	Displays the total throughput in Megabits per second (Mbps) for each of the active WLANs.
<b>ABS</b>	Displays the Average Bit Speed (ABS) in Megabits per second (Mbps) for each of the active WLANs.
<b>%NU</b>	Displays the percentage of the total packets for each active WLAN that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
<b>Retries</b>	Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.

In the lower section of the screen, the **Total Switch RF Traffic** table gives summary information about RF traffic.

<b>Total pkts per second</b>	Displays the average number of RF packets sent per second across all active WLANs on the wireless 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.
<b>Total bits per second</b>	Displays the average bits sent per second across all active WLANs on the wireless switch. The number in black displays this statistic for the last 30 seconds and the number in blue displays this statistic for the last hour.
<b>Total associated MUs</b>	Displays current total number of Mobile Units associated with all the active WLANs on the wireless switch.

To clear the RF statistics, click the **Clear all RF Stats** button.

### 11.3.2 Getting Statistics for a Particular WLAN

To see a summary information about wireless operations, select **Status & Statistics --> Wireless Stats - -> <WLAN name> Stats** from the navigation menu. A screen like the one shown for EngWLAN (below) will appear.

The screenshot displays the WS2000 Wireless Switch interface. The navigation menu on the left includes: [Network Configuration], [System Configuration], [Status & Statistics], WAN Stats, Subnet Stats, Wireless Stats (selected), WLAN1 Stats (selected), Access Ports Stats, MU Stats, Mesh Stats, IPS Stats, and Statistical Graphs. The main content area is titled "WLAN1 Stats" and contains the following data:

Information			
ESSID:	101	Authentication Type:	No Authentication
Subnet:	Subnet	Encryption Type:	No Encryption
Num. Associated MUs:	7	Adopted APs:	1,2

Traffic (does not include "retry overhead")					
	Total		Rx		Tx
Pkts per second	1	3 Pps	0	1 Pps	1
Throughput	0.0010	0.0010 Mbps	0.0	0.0 Mbps	0.0010
Avg. Bit Speed	0.0	10.02 Mbps			
% Non-unicast pkts	96.3%	47.21%			

RF Status			Errors		
Avg MU Signal	0.0	-103.7 dBm	Avg Num of Retries	16.0	0.6
Avg MU Noise	0.0	-169.1 dBm	% Gave Up Pkts	100.0%	3.23%
Avg MU SNR	0.0	65.4 dB	% of Undecryptable Pkts	0.0%	0.0%

At the bottom of the main content area, there are two radio buttons: "last 30 seconds" (selected) and "last hour". At the bottom right, there are "Help" and "Logout" buttons. The system name "WS2000" is displayed at the bottom left.

There are four areas on the screen. The Information area shows general information about the Access Port. The Received and Transmitted areas of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the Access Port. The Associated Mobile Units section lists the MUs and provides information on specific MUs that are currently transmitting through the Access Port.

### 11.3.3 General WLAN Information

#### 11.3.3.1 Information Section

<b>ESSID</b>	Displays the Extended Service Set Identification name that users will see when accessing the WLAN.
<b>Subnet</b>	Displays the name of the subnet to which this WLAN is associated.
<b>Num. Associated MUs</b>	Lists the number of mobile units (MUs) currently associated with the Access Port.
<b>Authentication Type</b>	Displays the type of authentication used with this WLAN.
<b>Encryption Type</b>	Displays type of encryption used with this WLAN.
<b>Adopted APs</b>	Lists the Access Ports that have been adopted by this WLAN.

#### 11.3.3.2 Traffic Area

<b>Packets per second</b>	The Total column 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.
<b>Throughput</b>	The Total column displays the average throughput in Mbps for a given time period 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 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.
<b>Avg. Bit Speed</b>	The Total column displays the average bit speed in Mbps for a given time period on the selected WLAN. 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.
<b>% Non-unicast pkts</b>	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.

#### 11.3.3.3 RF Status

<b>Avg MU Signal</b>	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.
<b>Avg MU Noise</b>	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.

<b>Avg MU SNR</b>	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 networks.
-------------------	---

### 11.3.3.4 Errors

<b>Avg Num of Retries</b>	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.
<b>% Gave Up Pkts</b>	Displays the percentage of packets which 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.
<b>% of Undecryptable Pkts</b>	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.

## 11.4 Access Port Statistics

The WS2000 Network Management System provides two screens, one that displays summary information for all associated access ports, and one that displays real-time statistics about the activity for each Access Port and its associated units.

### 11.4.1 Access Port Statistics Summary Screen

To see Access Port Summary information for the entire switch, select **Status & Statistics --> Access Port Stats** from the left menu.

The screenshot shows the WS2000 Wireless Switch interface. The left navigation pane is expanded to 'Access Ports Stats', showing a tree view of AP1 through AP6. The main content area is titled 'AP Stats Summary' and contains a table with the following data:

Name	Type	MUs	T-put	ABS	RF Util	% NU	Retries
AP1	B	0	0.00	0.00	0.00	100.00	0.00
AP2	A	0	0.00	0.00	0.00	100.00	0.00
AP3	B	31	0.00	6.49	0.07	32.22	2.28
AP4	A	0	0.00	0.00	0.00	100.00	0.00
AP5	BG	0	0.00	0.00	0.00	100.00	0.00
AP6	A	0	0.00	0.00	0.00	100.00	0.00

At the bottom of the interface, there are 'Help' and 'Logout' buttons, and the system name 'System Name: WS2000 Switch' is displayed.



Each Access Port associated with the switch is listed in the AP Summary area. For each AP, the following information is provided.

Field	Description
<b>IP</b>	Displays the IP address of the Access Port.
<b>WLAN</b>	Displays the WLAN with which the Access Port is associated.
<b>AP</b>	Displays the name of the Access Port with which the Access Port is associated.
<b>T-Put</b>	Displays the total throughput in Megabits per second (Mbps) for the Access Port.
<b>ABS</b>	Displays the Average Bit Speed (ABS) in Megabits per second (Mbps) for the Access Port.
<b>%NU</b>	Displays the percentage of the total packets for the Access Port that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
<b>Retries</b>	Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.

## 11.4.2 Detailed Information About a Particular Access Port

To see statistics about a particular Access Port, select **Status & Statistics --> Access Port Stats --> <Access Port Name>** from the left menu.

The screenshot displays the WS2000 Wireless Switch interface. The left navigation pane shows the following structure:

- [Network Configuration]
- [System Configuration]
- [Status & Statistics]
  - WAN Stats
  - Subnet Stats
  - Wireless Stats
  - Access Ports Stats
    - AP1 Stats [B]
    - AP2 Stats [A]
  - MU Stats
  - Mesh Stats
  - IPS Stats
  - Statistical Graphs

The main content area is titled **AP2 Stats** and contains the following sections:

**Information**

HW Address:	00:A0:F8:B5:36:0D	Radio Type:	802.11a
Placement:	Indoors	Power:	20 dB
Current Channel:	36	Num. Associated MUs:	0
Adopted by:	WLAN1	Active SIP Session count	0
Location:		Roamed SIP Session count	0
IP Address	N.A.		

**Traffic (does not include "retry overhead")**

	Total		Rx		Tx	
Pkts per second	1	1 Pps	0	0 Pps	1	1 Pps
Throughput	0.0010	0.0010 Mbps	0.0	0.0 Mbps	0.0010	0.0010 Mbps
Avg. Bit Speed	0.0	0.0 Mbps				
Approximate RF Utilization	0.0%	0.0%				
% Non-unicast pkts	100.0%	100.0%				

**RF Status**

Avg MU Signal	0.0	0.0 dBm
Avg MU Noise	0.0	0.0 dBm
Avg MU SNR	0.0	0.0 dB

**Errors**

Avg Num of Retries	0.0	0.0
% Gave Up Pkts	0.0%	0.0%
% of Undecryptable Pkts	0.0%	0.0%

Legend:  last 30 seconds  last hour

Buttons: Help, Logout

System Name: WS2000

There are four areas on the screen. The Information area shows general information about the Access Port. The Received and Transmitted areas of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the Access Port. The Associated Mobile Units section lists the MUs and provides information on specific MUs that are currently transmitting through the Access Port.

### 11.4.3 General Access Port Information

#### 11.4.3.1 Information Section

<b>HW Address</b>	The Media Access Control (MAC) address of the Access Port. This value is typically set at the factory and can be found on the bottom of the Access Port.
<b>Placement</b>	Lists whether the Access Port is placed indoors or outdoors. This is determined by the placement setting in the Access Port configuration screen in the Network Configuration section.
<b>Current Channel</b>	This field indicates the channel for communications between the Access Port and mobile units. To specify the value, go to the corresponding Access Port screen.
<b>Adopted by</b>	The WLANs that currently adopt this Access Port (see Network Configuration --> Wireless for the Access Port Adoption List).
<b>Location</b>	The site location of the Access Port (an optional field that the administrator fills in on the <b>Wireless --&gt; Access Ports --&gt; &lt;Access Port Name&gt;</b> screen).
<b>IP Address</b>	Displays the IP address of the AP if it is adopted over OSI Layer-3.
<b>Radio Type</b>	Displays the radio type of the selected Access Port. Radio types can be 802.11a, 802.11b, or 802.11b/g.
<b>Power</b>	The power level in milliwatts (mW) for RF signal strength is specified on the corresponding Access Port screen.
<b>Num. Associated MUs</b>	Lists the number of mobile units (MUs) currently associated with the Access Port.
<b>Active SIP Session Count</b>	Lists the number of currently active SIP Sessions on the selected Access Port. SIP is the Session Initiation Protocol which controls sessions for multimedia and voice conferences.
<b>Roamed SIP Sessions count</b>	Lists the number of SIP Sessions on the selected Access Port that have roamed to other Access Ports. SIP is the Session Initiation Protocol which controls sessions for multimedia and voice conferences.

#### 11.4.3.2 Traffic Area

<b>Packets per second</b>	The Total column displays the average total packets per second that cross the selected Access Port. The Rx column displays the average total packets per second received on the selected Access Port. The Tx column displays the average total packets per second sent on the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
<b>Throughput</b>	The Total column displays the average throughput in Mbps for a given time period on the selected Access Port. The Rx column displays the average throughput in Mbps for packets received on the selected Access Port. The Tx column displays the average throughput for packets sent on the Access Port 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.

<b>Avg. Bit Speed</b>	The Total column displays the average bit speed in Mbps for a given time period on the selected Access Port. 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.
<b>Approx RF Utilization</b>	The approximate utilization of the Access Port's RF port. This is calculated as Throughput divided by Average bit speed. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
<b>% Non-unicast pkts</b>	Displays the percentage of the total packets for the selected Access Port 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.

### 11.4.3.3 RF Status

<b>Avg MU Signal</b>	Displays the average RF signal strength in dBm for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
<b>Avg MU Noise</b>	Displays the average RF noise for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
<b>Avg MU SNR</b>	Displays the average Signal to Noise Ratio (SNR) for all MUs associated with the selected Access Port. The Signal to Noise Ratio is an indication of overall RF performance on your wireless networks.

### 11.4.3.4 Errors

<b>Avg Num of Retries</b>	Displays the average number of retries for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
<b>% Gave Up Pkts</b>	Displays the percentage of packets which the switch gave up on for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
<b>% of Undecryptable Pkts</b>	Displays the percentage of undecryptable packets for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

## 11.5 Mobile Unit (MU) Statistics

Each Access Port can have up to 32 associated mobile units. These units are listed in the Mobile Unit Access Control List of the WLAN Security screen (**Network Configuration** --> **Wireless** --> <WLAN Name> --> <WLAN Name> **Security**).

To see a summary of the associated mobile units and general information about each unit, select **Status & Statistics** --> **MU Stats**. The MU Stats Summary screen appears.

IP	Wlan	Ap	Vlan	T-put	ABS	% NU	Retries	Detail
192.168.0.136	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail
0.0.0.0	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail
0.0.0.0	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail
0.0.0.0	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail
0.0.0.0	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail
0.0.0.0	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail
0.0.0.0	WLAN1	AP1	1	0.00	10.47	0.00	0.50	MU Detail
192.168.0.117	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail
0.0.0.0	WLAN1	AP1	1	0.00	0.00	0.00	0.00	MU Detail

Field	Description
<b>IP</b>	Displays the IP address of the mobile unit.
<b>WLAN</b>	Displays the WLAN with which the mobile unit is associated.
<b>AP</b>	Displays the name of the Access Port with which the mobile unit is associated.
<b>Vlan</b>	Displays the VLAN that each of the mobile units is associated with.
<b>T-Put</b>	Displays the total throughput in Megabits per second (Mbps) for the mobile unit.
<b>ABS</b>	Displays the Average Bit Speed (ABS) in Megabits per second (Mbps) for the mobile unit.
<b>%NU</b>	Displays the percentage of the total packets for the mobile unit that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
<b>Retries</b>	Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.
<b>Detail</b>	<p>Clicking <b>MU Detail</b> will launch a new window with detailed statistics about the selected mobile unit.</p> <p>The MU Details screen is separated into four sections, MU Properties, MU Traffic, MU Signal, and MU Errors. The MU Properties section displays basic information such as hardware address, IP address, and associated WLAN and AP. The MU Traffic section displays statistics on RF traffic and throughput. The RF Status section displays information on RF signal averages from the MU. The Error section displays RF traffic errors based on retries, dropped packets and undecryptable packets.</p>

## 11.6 Mesh Statistics

A mesh network is a type of local area network where each node participating in the network is connected directly to its peers. This kind of network provides a robustness that cannot be matched by the standard network. In a mesh network, devices participating in the network, assist each other in transmitting packets through the network and provides a highly scalable network with multiple redundant communication paths.

Wireless mesh network provide additional benefits of being highly adaptable. As required, nodes to a wireless network can be added or removed.

The Mesh Stats screen provides information about the state of the Mesh network on this device. This screen consist of the **Mesh Base Connections** and **Mesh Client Connection** tabs.

### 11.6.1 Mesh Base Connections

The Mesh Base Connections screen displays information about the connections to the base

The following information is displayed.

<b>MAC</b>	The unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier. This value is hard coded at the factory by the manufacturer and cannot be changed.
<b>Wlan</b>	Displays the WLAN name each wireless bridge is inter-operating with.
<b>Ap</b>	The AP on which connection is made to the base bridge.
<b>Vlan</b>	The VLAN of the mesh connection
<b>T-put</b>	The total throughput in Megabits per second (Mbps) for each associated bridge.
<b>ABS</b>	The Average Bit Speed (ABS) in Megabits per second (Mbps) for each associated bridge.
<b>%NU</b>	Displays the percentage of the total packets for the base bridge that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
<b>Retries</b>	Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.
<b>Detail</b>	Clicking <b>Detail</b> will launch a new window with detailed statistics about the selected base bridge.  The Base Bridge Details screen is separated into four sections, Base Bridge Properties, Base Bridge Traffic, Base Bridge Signal, and Base Bridge Errors. The MU Properties section displays basic information such as hardware address, IP address, and associated WLAN and AP. The MU Traffic section displays statistics on RF traffic and throughput. The RF Status section displays information on RF signal averages from the MU. The Error section displays RF traffic errors based on retries, dropped packets and undecryptable packets.

### 11.6.2 Mesh Client Connections

The Mesh Client Connections screen displays information about the client connections to this device.

The following information is displayed.

<b>MAC</b>	The unique 48-bit, hard-coded Media Access Control address, known as the devices station identifier. This value is hard coded at the factory by the manufacturer and cannot be changed.
<b>Wlan</b>	Displays the WLAN name each wireless bridge is inter-operating with.
<b>Ap</b>	The AP on which connection is made to the Client bridge.
<b>Vlan</b>	The VLAN of the mesh connection
<b>T-put</b>	The total throughput in Megabits per second (Mbps) for each associated bridge.
<b>ABS</b>	The Average Bit Speed (ABS) in Megabits per second (Mbps) for each associated bridge.
<b>%NU</b>	Displays the percentage of the total packets for the Client bridge that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
<b>Retries</b>	Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.
<b>Detail</b>	<p>Clicking <b>Detail</b> will launch a new window with detailed statistics about the selected Client bridge.</p> <p>The Client Bridge Details screen is separated into four sections, Client Bridge Properties, Client Bridge Traffic, Client Bridge Signal, and Client Bridge Errors. The MU Properties section displays basic information such as hardware address, IP address, and associated WLAN and AP. The MU Traffic section displays statistics on RF traffic and throughput. The RF Status section displays information on RF signal averages from the MU. The Error section displays RF traffic errors based on retries, dropped packets and undecryptable packets.</p>

## 11.7 Intrusion Prevention Statistics

The Intrusion Prevention Statistics (IPS) screen displays the IPS statistics. To view IPS statistics, click **Status & Statistics --> IPS Stats** menu item from the left menu. The following screen appears.

The screenshot shows the WS2000 Wireless Switch interface. The left sidebar contains a tree view with the following items: [Network Configuration], [System Configuration], [Status & Statistics] (expanded), WAN Stats, Subnet Stats, Wireless Stats, Access Ports Stats, MU Stats, Mesh Stats, **IPS Stats** (selected), and Statistical Graphs. The main content area is titled 'IPS Stats' and contains two sections:

**IPS GLOBAL STATISTICS**

Status:	Enabled
Number of packets received	17057
Number of packets processed	17057
Number of packets dropped	0
Number of connections disconnected	0

**Individual Category Stats**

TELNET ▼

Number of Rules	41
Number of Alerts	1
Number of Logs	0
Number of packets dropped	0
Number of disconnections	0

Buttons: Help, Logout

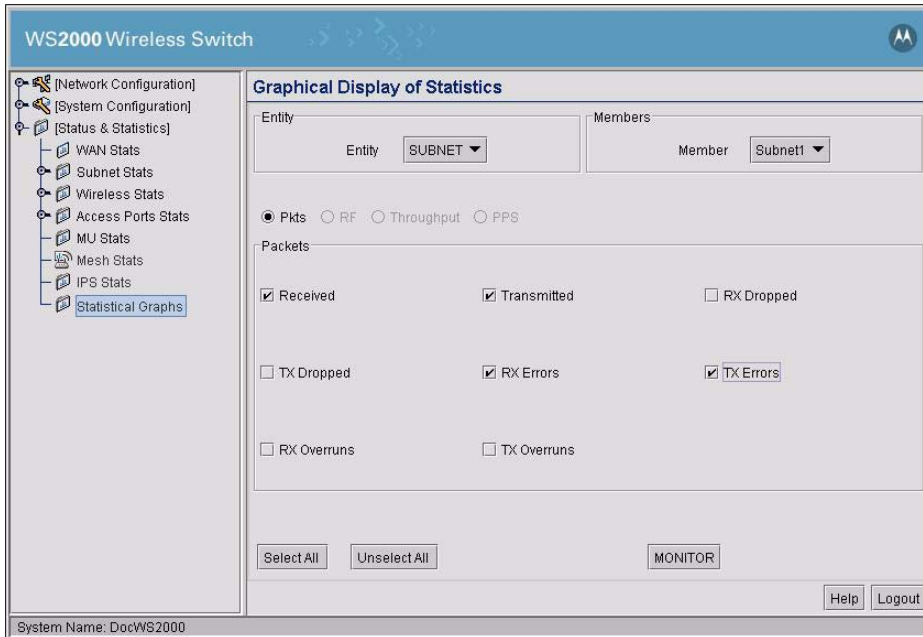
System Name: WS2000

This screen is divided into two sections. The top one, **IPS Global Statistics**, displays the global IPS information. The bottom section, **Individual Category Statistics** displays IPS information for a selected category. To view the statistics for a category, select the category from the drop down list in the **Individual Category Statistics** section.

## 11.8 View Statistics in Graphic Form

In the screens described by the previous sections of this chapter, the statistics for the WAN, LAN, WLAN, Access Ports, and mobile units are presented in a tabular format. However, administrators often want to see the trends of the activity on the LAN. To aid with that project, the WS2000 Wireless Switch enables the administrator to view the statistics in a graphical format that is constantly updated.

Select **[Status & Statistics]** --> **Statistical Graphs** from the navigation menu on the left. The Graphical Display of Statistics screen appears.



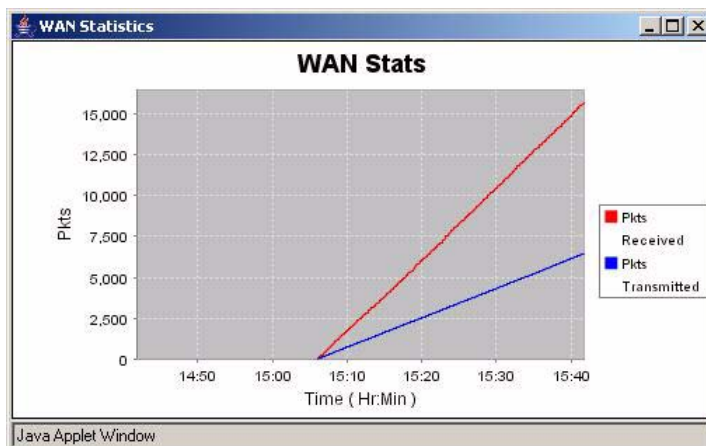
To create a graph that will remain on your screen until you close it, follow these steps:

1. Select the type of **Entity** (**WAN**, **SUBNET**, **WLAN**, **AP**, or **MU**) that you want to display from the menu.
2. Select the particular member that you want to watch from the **Member** menu.
3. Select the data to monitor. Depending on the selected entity type, one or more of four radio buttons will become available to choose from. The radio button selection indicates what is being monitored (graphed on the X axis). Selections can be one of:

<b>Pkts</b>	If selected, the switch will monitor and graph packet traffic statistics. Select one or more of the eight values to monitor, including: packets received and transmitted, received and transmitted packets that were dropped, reception and transmission errors, and transmission and reception overruns.
<b>RF</b>	If selected, the switch will monitor radio frequency statistics. Select one or more of the different RF values to monitor, including: signal, noise, and signal-to-noise ratio (SNR).
<b>Throughput</b>	If selected, the switch will monitor the switches throughput. Select one or more of the different throughput values to monitor: total throughput, transmission received, transmitted throughput or the average bit speed.
<b>PPS</b>	If selected, information about packets per second will be graphed for the selected member. Select one or more of the three values to monitor: total packets per second, received packets, and transmitted packets.

4. Click the **MONITOR** button to open the graphics window. A window like the following will appear.





5. Repeat Steps 1 through 4 to display as many statistics windows as required.

A graphical statistics display window will stay available until you manually close it or Logout of the application.



# 12

## ***WS2000 Use Cases***

12.1 Retail Use Case . . . . .	12-3
12.1.1 A Retail Example . . . . .	12-3
12.2 The Plan . . . . .	12-3
12.3 Contacting the Wireless Switch . . . . .	12-4
12.3.1 Entering the Basic System Settings . . . . .	12-5
12.3.2 Setting Access Control . . . . .	12-6
12.3.3 The IP Address Plan . . . . .	12-7
12.4 Configuring POS Subnet . . . . .	12-8
12.5 Configuring the Printer Subnet . . . . .	12-9
12.6 Configuring the Cafe Subnet . . . . .	12-11
12.7 Configuring the WAN Interface . . . . .	12-12
12.8 Configuring Network Address Translation (NAT) . . . . .	12-13
12.9 Inspecting the Firewall . . . . .	12-14
12.10 Configuring the Access Ports . . . . .	12-15
12.10.1 Setting Access Port Defaults . . . . .	12-15
12.10.2 Naming the POS Access Port . . . . .	12-17
12.10.3 Configuring the Printer Access Port . . . . .	12-17
12.10.4 Configuring the Cafe Access Port . . . . .	12-18
12.10.5 Associating the Access Ports to the WLANs . . . . .	12-19
12.11 Configuring the Cafe WLAN . . . . .	12-19
12.12 Configuring the Printer WLAN . . . . .	12-21
12.13 Configuring the POS WLAN . . . . .	12-24
12.14 Configuring Subnet Access . . . . .	12-27
12.15 Configuring the Clients . . . . .	12-29
12.15.1 Testing Connections . . . . .	12-29
12.16 Field Office Use Case . . . . .	12-30
12.16.1 A Field Office Example . . . . .	12-30
12.17 The Plan . . . . .	12-30
12.18 Configuring the System Settings . . . . .	12-31
12.18.1 Contacting the Wireless Switch . . . . .	12-31
12.18.2 Entering the Basic System Settings . . . . .	12-33
12.18.3 Setting Access Control . . . . .	12-34
12.19 Configuring the LAN . . . . .	12-35
12.19.1 Configuring the Engineering LAN . . . . .	12-36
12.19.2 Configuring the Sales Subnet . . . . .	12-38

12.20 Configuring the WAN Interface .....	12-40
12.21 Configuring the WAN Interface .....	12-41
12.21.1 Setting Up Network Address Translation.....	12-41
12.22 Confirm Firewall Configuration.....	12-42
12.23 Adopting Access Ports .....	12-43
12.24 Configuring the WLANs .....	12-45
12.24.1 Security .....	12-46
12.25 Configuring the Access Ports .....	12-49
12.26 Configuring Subnet Access.....	12-54
12.27 Configuring the VPN .....	12-57
12.28 Installing the Access Ports and Testing .....	12-60

## 12.1 Retail Use Case

### 12.1.1 A Retail Example

#### 12.1.1.1 Background

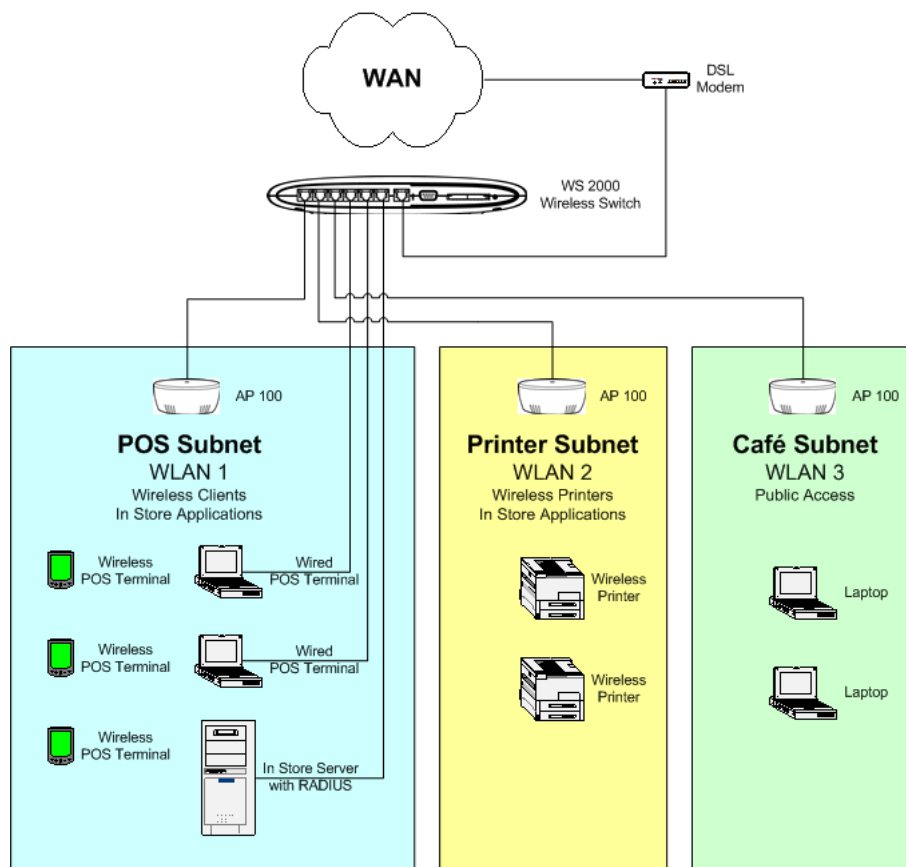
CCC Clothing Stores have, in the past, used POS terminals with a 10BaseT Ethernet connection to an in-house server. Management has decided to install wireless networking in the stores. Wireless point of sale (POS) terminals and printers will allow them to be more flexible with store layout. Wireless handheld terminals for inventory and price lookup will make inventory faster and more accurate. In some stores, management is adding a cafe with free wireless Internet access. The hope is that customers will visit more often and stay longer if their partners can use the Internet while they shop.

The following links show the tasks that the system administrator will carry out to complete the wireless upgrade.

## 12.2 The Plan

Clarissa is the employee assigned to implement the new network in San Jose. She needs three very different security policies. Wireless security policies are part of a WLAN configuration, so she will need three different WLANs.

- **WLAN #1:** Confidential information, such as credit card numbers and customer purchases, will travel over the links to wireless POS terminals. For these, she wants the strongest security measures possible. The two components of a wireless security policy are user authentication and data encryption. The corporation has a RADIUS server for user authentication and it is a logical choice for this application. If the corporation did not have a RADIUS server, an alternative would have been to install Kerberos on the in-store server and use Kerberos user authentication. As for data encryption, WEP is not secure enough for this traffic. A survey of the wireless POS terminals reveals that they all support WPA-TKIP, so Clarissa will use WPA-TKIP for data encryption.
- **WLAN #2:** The wireless printers are difficult to misuse - no keyboards - and the data stream to them does not include any information that needs strong encryption. On this WLAN, Clarissa can limit user access by limiting connections to just those devices which have their MAC addresses entered in the switch. The data will be WEP encrypted.
- **WLAN #3:** In the cafe, Clarissa wants an open network - no authentication or encryption. She believes that otherwise the support problems will be too difficult. But management wants to be absolutely certain that users of the cafe net cannot get access to the store computers or POS terminals. The WS2000 allows the administrator to restrict access from one subnet to another, so Clarissa will create a subnet that is just for WLAN #3, and then restrict access from that subnet to the other subnets.



This plan covers all the wireless devices—the POS terminals, the printers, and the customer laptops—except the wireless handheld terminals. Clarissa decides to put them on the WLAN with the POS terminals.

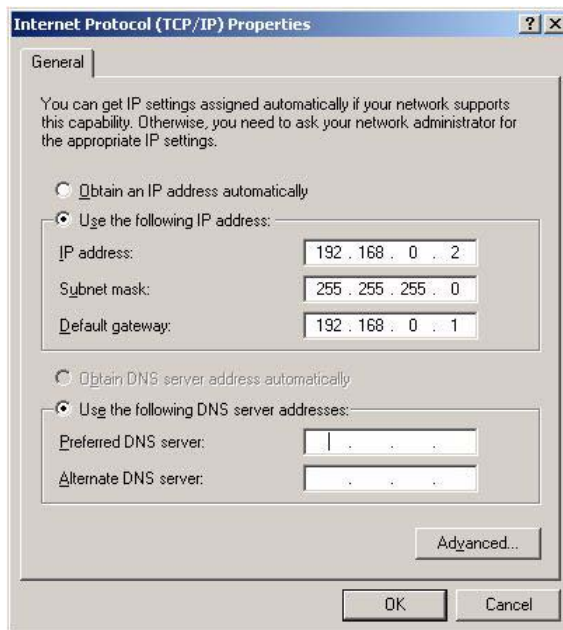
There are also some conventional, 100baseT wired devices to consider. There is the store server and two wired POS terminals. Clarissa will put all of these on the 100baseT ports on the WS2000.

To keep things simple, Clarissa decides to define one subnet for each WLAN and assign one Access Port to each WLAN. The wired devices will be part of the POS subnet.

The WS2000 will connect to the Internet through a DSL line.

## 12.3 Contacting the Wireless Switch

Clarissa sets up a direct network link between her laptop and the switch, plugging the cable into one of the local, non-WAN, ports. The switch defaults to having all the LAN ports on the first subnet and that subnet having an IP address of 192.168.0.1. So, as far as this connection is concerned, the switch comes up with an initial IP address of 192.168.0.1. She sets her laptop to have an IP address of 192.168.0.2 and a netmask of 255.255.255.0. She also sets the gateway IP address to be 192.168.0.1, the WS2000's IP address.



Clarissa starts her web browser and enters “<http://192.168.0.1/>” as the URL. The WS2000 sends a login page to her browser.

She logs in using “**admin**” for the username and “**symbol**” as the password. The system immediately asks her to change the password to something else. Clarissa does so.

### 12.3.1 Entering the Basic System Settings

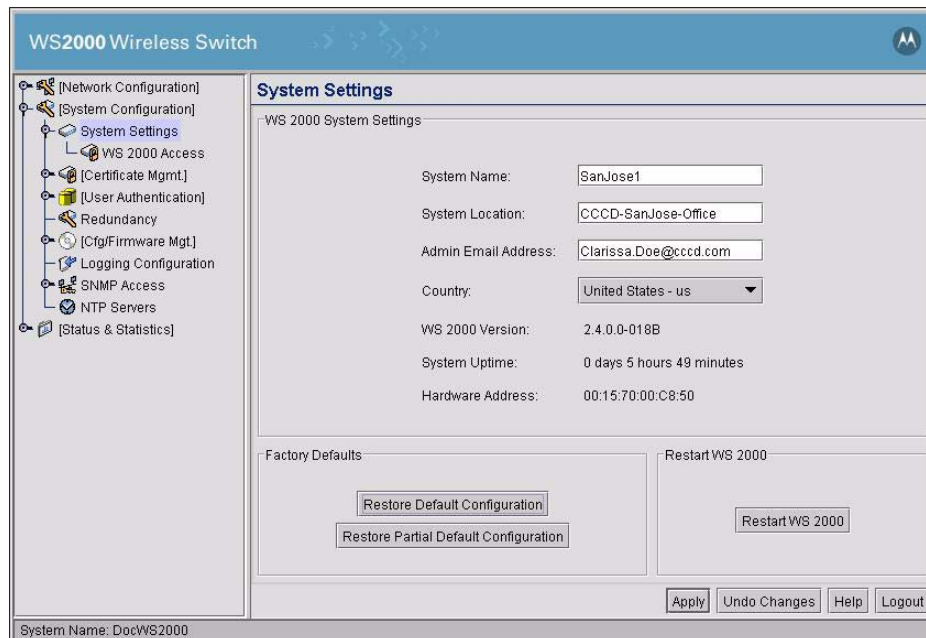
Clarissa selects **System Settings** from the left menu, located under the System Configuration heading.

Upon selecting this screen for the first time, the WS2000 switch immediately asks her to choose a country. Different countries have different regulations for the use of these radio frequencies. Setting the location configures the switch to use only the channels, frequencies, and power levels that are legal for that country. She sets the country to United States - US.

The system name is used to distinguish between WS2000 switches for remote configuration. She gives the switch a descriptive name, “**SanJose-1**”. This name will appear in the footer for subsequent configuration windows for the switch. She does not need the name now, while she is in San Jose. But later, when she returns to corporate headquarters and wants to log into several switches remotely, it will help her to know which switch she is working on. She also enters a slightly longer description on the **System Location** field.

She enters her E-mail address into the **Admin Email Address** box. CCC uses an SNMP manager that has the capability of monitoring network devices and sending email to the manager of a device that is in an unusual state. This is the email address that will be supplied to that SNMP manager for this switch.

Clarissa clicks the **Apply** button to save her changes.

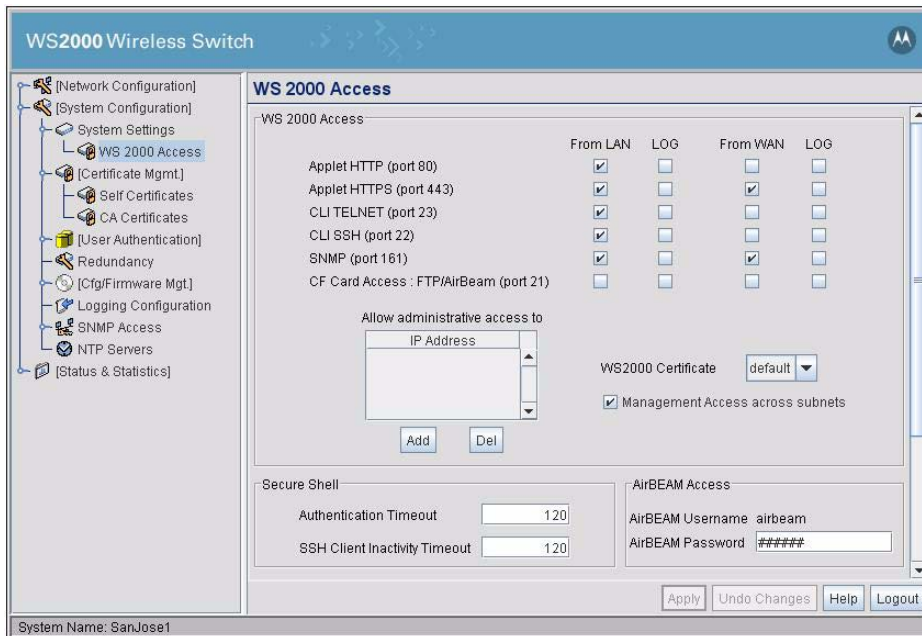


### 12.3.2 Setting Access Control

In the WS2000 Access screen, Clarissa controls which network interfaces can be used to reconfigure the WS2000 switch. She is currently using HTTP access on port 80 over the LAN, so she leaves that on. She may also want to make changes using the Command Line Interface (CLI), so she leaves on local CLI access. She wants to be able to manage the switch from corporate headquarters, but she does not want to leave the standard HTTP port, port 80, open over the WAN. She elects to leave port 443 open over the WAN instead. She knows she will want to monitor the switch from her SNMP system at corporate, so she leaves **SNMP WAN access** on.

AirBEAM is a Motorola Technology software system designed to simplify maintenance of wireless devices. CCC Clothing Stores recently purchased an AirBEAM license as part of a major commitment to Motorola Technology wireless bar code scanners for inventory. Clarissa would like to integrate the WS2000 into the AirBEAM management system and she leaves AirBEAM access on.





Clarissa clicks the **Apply** button to save her changes.

Clarissa leaves the rest of the System Configuration screens for now, moves to the left menu, and clicks on **Network Configuration** so that she can begin to define the subnets.

### 12.3.3 The IP Address Plan

Subnets can be renamed, assigned an IP address, and have ports associated with them. Clarissa needs to plan how she is going to assign IP addresses to the subnets and the devices on them.

Clarissa only has one IP address from corporate for this store. She will use network address translation (NAT) for all of the devices, making request from those devices look to the outside world as if they came from the single static IP address that she has. For the devices, she plans to use IP numbers from the range 192.168.\*.\*, because IP addresses in that range are designated for internal use only.

She will assign them as follows:

Subnet	IP Address Range
192.168.0.***	POS subnet
192.168.1.***	Printer subnet
192.168.2.***	Cafe subnet

And for each subnet:

192.168.**.1	The WS2000 address on that subnet
192.168.**.2 to 192.168.**.10	Devices with static IP addresses
192.168.**.11 to 192.168.**.254	Devices with DHCP-supplied IP addresses

With this plan, she can begin to configure the individual subnets.

## 12.4 Configuring POS Subnet

Clarissa selects the first subnet from the LAN menu items in the left menu.

Clarissa renames this subnet "**POSSn**", then gives the switch an IP address of 192.168.0.1 on that subnet and assigns a subnet mask of 255.255.255.0. The devices on this subnet are:

- Everything on the POS WLAN: wireless POS terminals and wireless handheld terminals
- One wired POS terminal on port 4 and one on port 5
- One in-store server on port 6

Using the Interfaces section of the screen on the right, she associates the first WLAN with this subnet, as well as Ports 1 (the one the POS WLAN is plugged into), 4 and 5 (the wired POS terminals), and 6 (the server). She activates the DHCP server and gives it an IP address range of 192.168.0.11 to 192.168.0.254.

The screenshot displays the configuration interface for a WS2000 Wireless Switch. On the left, a navigation tree shows the 'LAN' menu expanded to 'Subnet1'. The main area is titled 'Subnet1' and has two tabs: 'Subnet Config' (selected) and 'Bridge Config'. Under 'Subnet Config', the 'Name' field is 'POSSn'. The 'IP Parameters' section includes 'IP Address' (192.168.0.1), 'Network Mask' (255.255.255.0), and 'Default Gateway' (192.168.0.1). The 'DHCP' section has three radio buttons: 'This interface does not use DHCP', 'This interface is a DHCP Client', and 'This interface is a DHCP Server' (selected). Below this, the 'Address Assignment Range' is set to '192.168.0.11' to '192.168.0.254'. There are buttons for 'Advanced DHCP Server' and 'Update DNS'. The 'Interfaces' section shows two columns: 'Assigned' (Port1, Port4, Port5, Port6, WLAN1) and 'Available' (WLAN5, WLAN6, WLAN7, WLAN8, Port2, Port3). Between these columns are buttons for '<- Add' and 'Delete ->'. At the bottom right are 'Apply', 'Undo Changes', 'Help', and 'Logout' buttons. The bottom left shows 'System Name: SanJose1'.

After the Address Assignment Range is entered, Clarissa clicks **Advanced DHCP Server**.

Advanced DHCP Server

Enable Dynamic DNS

Single User Class Option

Multiple User Class Option

Primary DNS Server 206 . 148 . 10 . 1

Secondary DNS Server 206 . 148 . 10 . 2

Default Gateway 192 . 168 . 0 . 1

WINS Server 192 . 168 . 0 . 254

DHCP Lease Time (sec) 86400

Domain Name

DNS Forward Zone

TFTP Server Address 0 . 0 . 0 . 0

Bootfile

Option 189

Option 43

Static DHCP Mappings:

Client MAC	IP Address

Add Del

Ok Cancel Help

Java Applet Window

The **Default Gateway** is already set to the subnet address. This is the IP address to which the DHCP clients on this subnet will forward their outbound traffic. Clarissa fills in the **DNS Server addresses**, which corporate has specified. This will also be supplied to the DHCP clients. The **DHCP Lease Time** is the time an IP address will remain assigned to a client after there is no more activity. She leave it at the default and clicks **Ok** to save her changes.

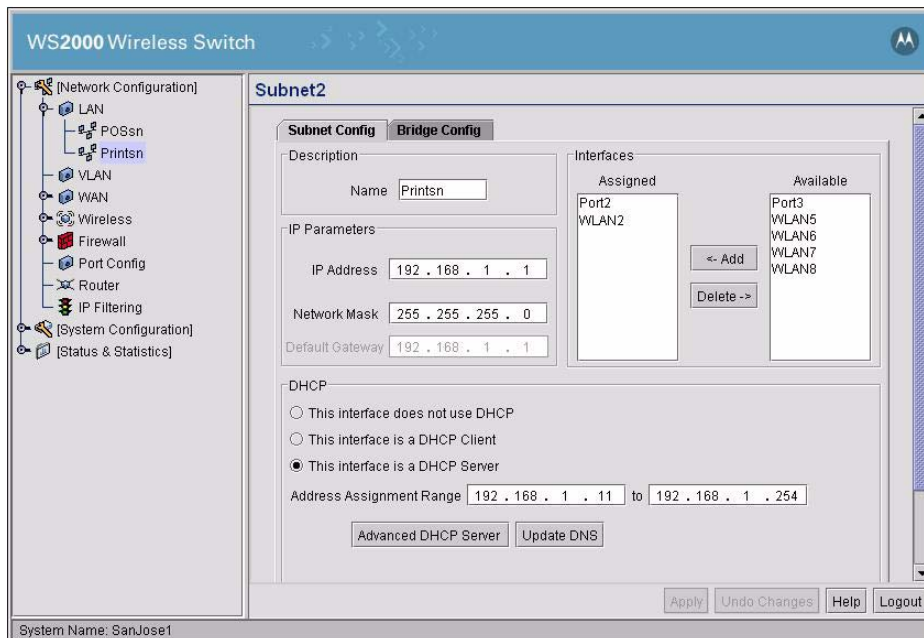
Then, in the subnet screen, she clicks **Apply** to save her overall changes.

Now she will configure the printer subnet.

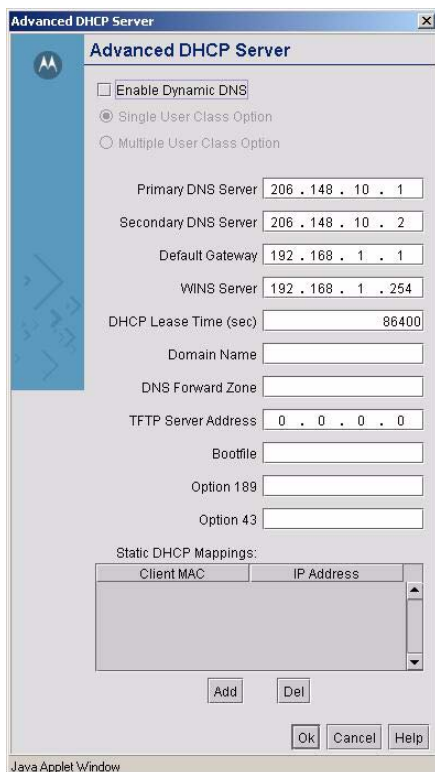
## 12.5 Configuring the Printer Subnet

Clarissa selects the second subnet from the list of LAN menu items in the left menu.

She renames this subnet "**Printsn**", then gives it an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0. The only devices on this subnet are the wireless printers. Using the Interfaces section of the screen, she associates the second WLAN with this subnet. She activates the DHCP server with an IP address range of 192.168.1.11 to 192.168.1.254.



After the Address Assignment Range is entered, Clarissa clicks **Advanced DHCP Server**.



Clarissa enters the **DNS server IP addresses** and leaves the **Default Gateway** and **DHCP Lease Time** at their defaults. She clicks **Ok** in the Advanced DHCP Server window and then **Apply** in the Subnet window to save her changes.

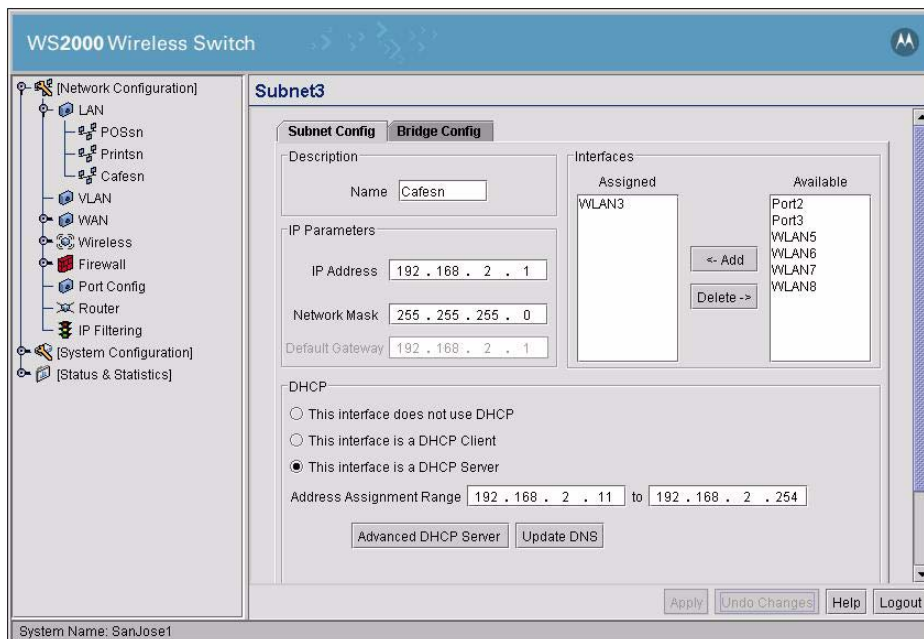
Now Clarissa will configure the Cafe subnet.

## 12.6 Configuring the Cafe Subnet

Clarissa selects the third subnet in the LAN menu list under Network Configuration in the left menu.

She then renames this subnet “**Cafesn**” and gives it the IP address 192.168.2.1 and a subnet mask of 255.255.255.0. The only devices on this subnet are the customer’s laptops in the cafe.

Using the Interfaces section of the screen, she associates the third WLAN with this subnet, and activates the DHCP server with an IP address range of 192.168.2.11 to 192.168.2.254.



Clarissa clicks **Advanced DHCP Server** and enters the **DNS server IP addresses**. The **Default Gateway** is fine. However, Clarissa expects the cafe patrons to come and go frequently, so she reduces the **IP address lease time** to 1800 seconds. This means that a DHCP client mobile unit will give up its IP address if it is inactive on the network for more than half an hour. This seems about right for the usage patterns that she expects for the cafe. If she gets complaints, she will increase it to an hour.

Advanced DHCP Server

Enable Dynamic DNS

Single User Class Option

Multiple User Class Option

Primary DNS Server 206 . 148 . 10 . 1

Secondary DNS Server 206 . 148 . 10 . 2

Default Gateway 192 . 168 . 2 . 1

WINS Server 192 . 168 . 2 . 254

DHCP Lease Time (sec) 1800

Domain Name

DNS Forward Zone

TFTP Server Address 0 . 0 . 0 . 0

Bootfile

Option 189

Option 43

Static DHCP Mappings:

Client MAC	IP Address

Add Del

Ok Cancel Help

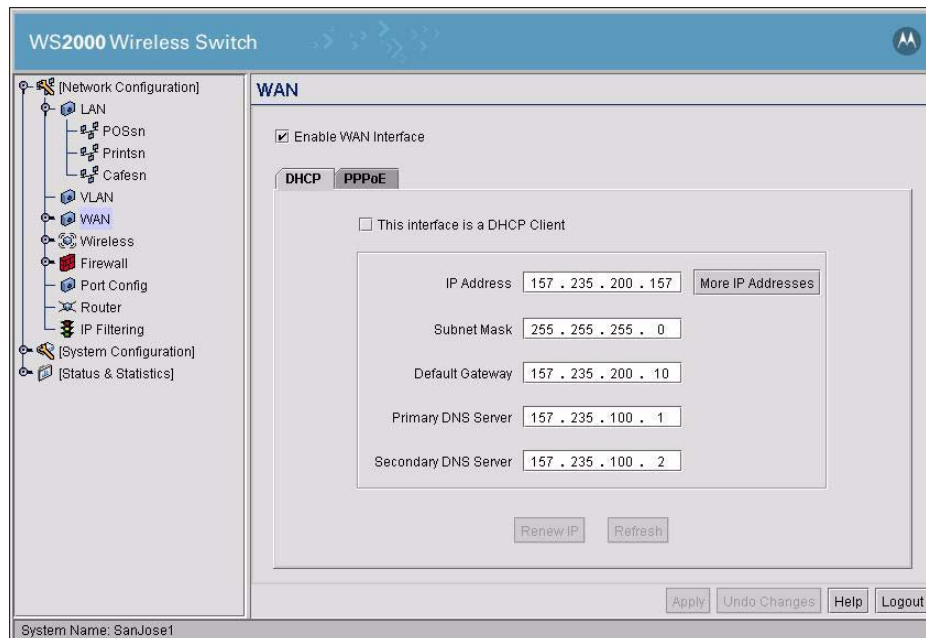
Java Applet Window

Clarissa clicks the **Ok** button in the Advanced DHCP Server window, then on the **Apply** button in the subnet screen to save her choices. The subnets are now configured.

Next Clarissa configures the WAN interface.

## 12.7 Configuring the WAN Interface

Now Clarissa selects the WAN node in the left menu. Here she enters the static IP address assigned to this store by CCC corporate. She also enters the other information supplied to her by corporate: the gateway IP address, the subnet mask, and the DNS server IP addresses. She is connecting by a DSL modem, but because she has a static IP address, her Internet service provider (ISP) does not require PPP-over-Ethernet connection information. If her ISP required PPPoE account information, she would have to enter that information in the PPP-over-Ethernet section of the screen.



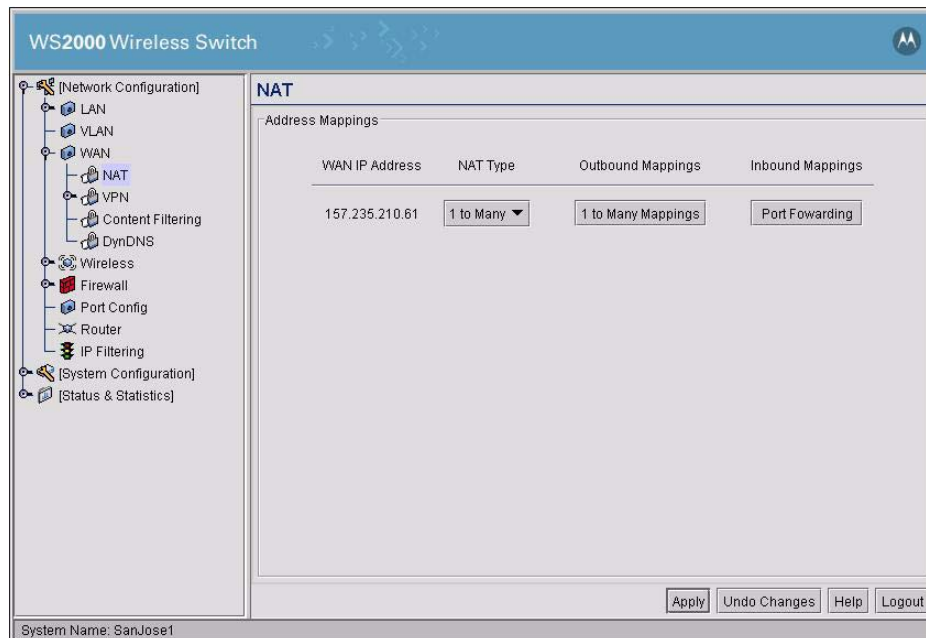
If corporate had not paid their ISP for a static IP address for each store, she would have selected the **This interface is a DHCP Client** option and the WAN configuration settings would have been assigned by the ISP each time they connected to the Internet.

Clarissa clicks the **Apply** button to save her changes.

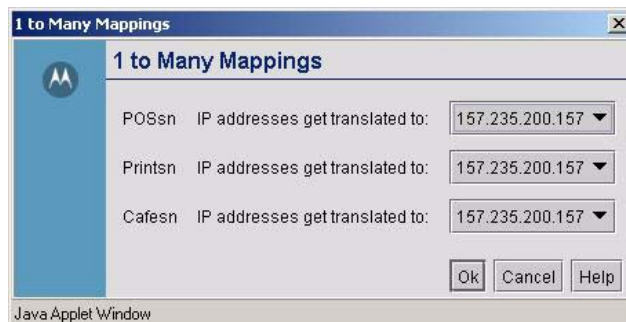
## 12.8 Configuring Network Address Translation (NAT)

Clarissa has only one public IP address for the whole store. She will use network address translation to make all requests from internal IP addresses to appear as if they came from the single public IP address.

She selects the **NAT** node under the WAN item in the left menu. The screen shows all IP addresses assigned to the switch in the WAN interface configuration step. In this case, there is one IP address shown. She selects **"1 to Many"** from the NAT Type menu to the right of the IP address.



After she makes this selection a new button appears, labelled **“1 to Many Mappings”**. She selects the **“1 to Many Mappings”** button.



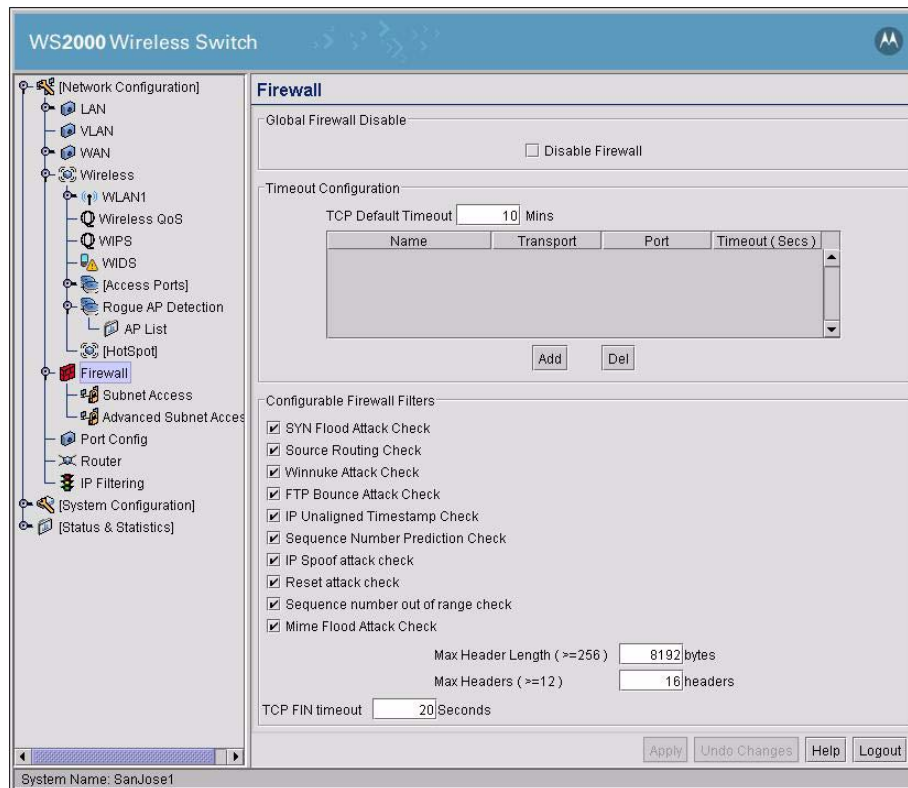
If Clarissa had more than one static IP address, she would have been able to assign several to the WAN interface. This screen would be used to choose how the internal IP addresses on each subnet translated into the selection of external IP addresses. However, she has only one external IP address. All requests from any IP address on the store network will be translated into a request using the single public IP address for the store.

Clarissa clicks the **Ok** button to confirm the mappings and then clicks the **Apply** button in the main screen to confirm the NAT choices and save her choices on the switch.

## 12.9 Inspecting the Firewall

Clarissa selects the **Firewall** item in the left menu. Each of the check box items represents a type of attack which the WS2000 can filter out. She checks to see that all of the options are enabled.





Clarissa clicks the **Apply** button to confirm that all attacks listed will be filtered.

## 12.10 Configuring the Access Ports

So far, Clarissa has been operating with the WS2000 connected only to her laptop. To configure the Access Ports, she will need to connect them to the switch. She plans to use switch ports as follows:

Switch Port	Connected to
Port 1	Access port for the POS WLAN
Port 2	Access port for the Printer WLAN
Port 3	Access port for the Cafe WLAN
Port 4	Wired POS terminal #1
Port 5	Wired POS terminal #1
Port 6	In-store server

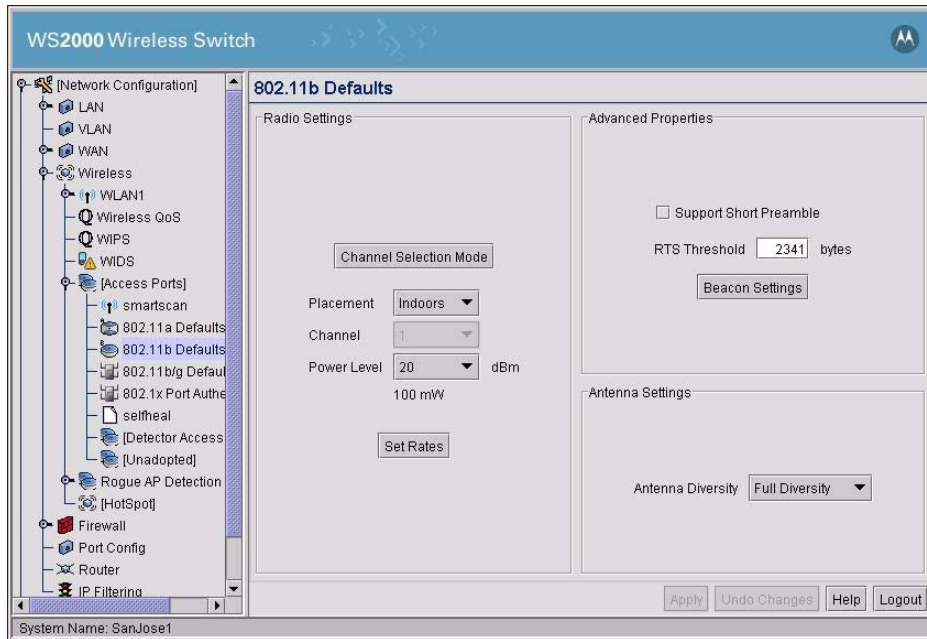
### 12.10.1 Setting Access Port Defaults

The WS2000 allows the user to specify the default settings for Access Ports. Clarissa expands the **Access Ports** node in the left menu and selects the **802.11b Defaults** node. Clarissa has only 802.11b Access Ports.

All of the Access Ports will be indoors, so she specifies **Placement** as Indoors. She sets the **Channel** to one, though she will reset each Access Port to a different 802.11b channel later. She sets the **Power Level** to 20dB, the maximum level allowed in the US.

She does not change the supported rates—using the **Set Rates** button—but leaves them as they are. The switch will operate at the maximum rate allowed by radio conditions, scaling back as needed.

She also does not change the **Antenna Diversity** setting, **Short Preamble** setting, **RTS Threshold**, or the **Beacon Settings**. These parameters control some of the broadcast mechanics of an 802.11 conversation between mobile units and Access Ports. In most cases, there is no reason to change them.

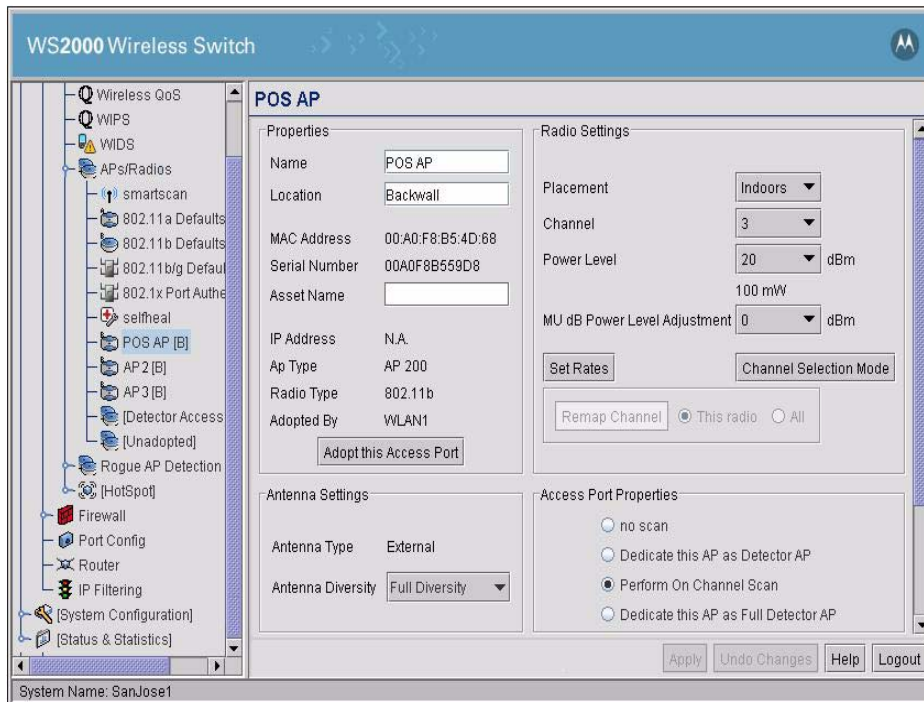


Clarissa clicks **Apply** to save her changes.

After setting the default settings for 802.11a and 802.11b Access Ports, Clarissa removes the Access Ports from their packaging and labels the each with the name of the WLAN which it will support. She connects the Access Ports to the switch, using the ports selected in her plan.

### 12.10.2 Naming the POS Access Port

Having specified the general Access Port defaults, Clarissa goes on to name and configure the Access Port for the POS WLAN. She selects the first Access Port in the left menu.



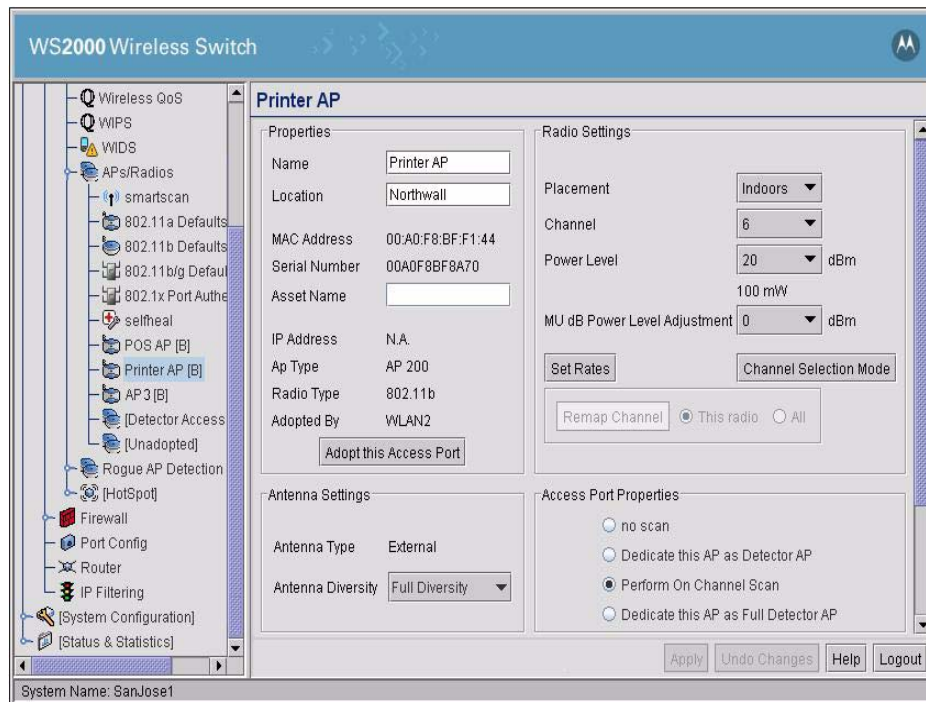
In the Properties section, Clarissa enters a new name for the Access Port and a brief description of its permanent location.

In the Radio Settings section, Clarissa sets the **Channel** to 3. She knows that the store uses cordless phones that transmit on channel 1. She also wants to maintain some separation between the channel used by this Access Port and the other Access Ports at this location.

She doesn't change any of the other settings. She clicks the **Apply** button to save her changes.

### 12.10.3 Configuring the Printer Access Port

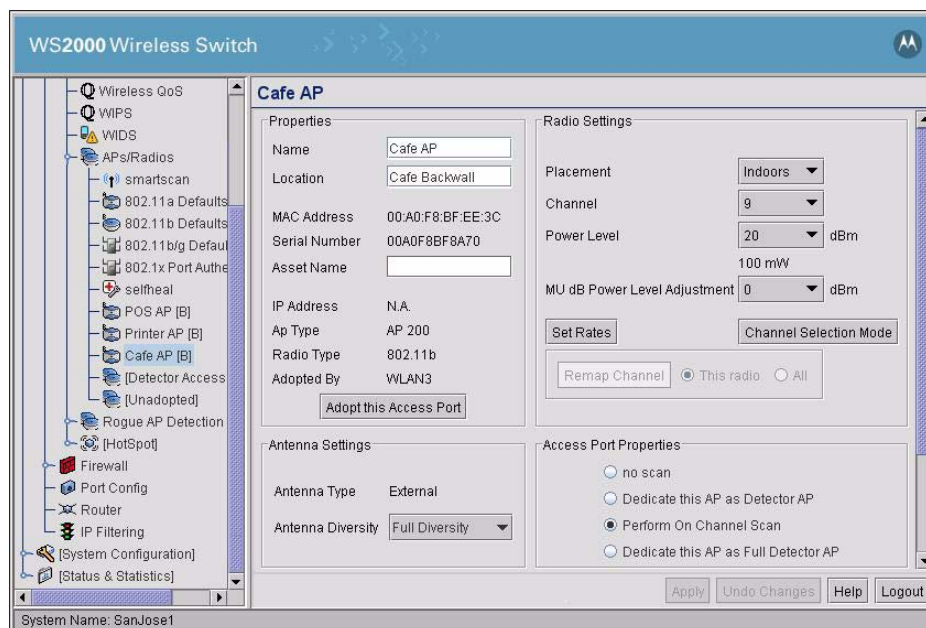
Clarissa configures the Printer Access Port in a similar way. She give it the name "**Printer AP**" and a location description. She assigns channel 6 to this Access Port, avoiding contention with the POS AP and the Cafe AP.



She clicks the **Apply** button to save her changes.

### 12.10.4 Configuring the Cafe Access Port

Finally, she names the third Access Port “**Cafe AP**” and gives it a channel of 9. In this case she makes sure **Support Short Preamble** is not selected. There are two preambles in use in the wireless world, an older, longer one and a newer, shorter one. Most wireless devices support both and use the shorter one by default. However, in the cafe, there will be older wireless devices coming in and rather than confuse them, she will stick with the longer preamble on this WLAN.



Again, she clicks the **Apply** button to save her changes.

## 12.10.5 Associating the Access Ports to the WLANs

Now Clarissa selects the **APs/Radio** item in the left menu. This screen indicates which Access Ports are associated with which WLANs.

First Clarissa looks in the **[Network Configuration] --> Wireless** screen to determine that all three WLANs are enabled.

In the **Radio Adoption Table** screen, the screen begins with a single line with "ANY" as the Start MAC address, "ANY" as the End MAC address, and checks under all three of the WLANs. Clarissa removes the checks from the WLAN check boxes.

Any discovered radio is displayed in the **Radio Adoption Table**. Clarissa looks in the table to determine that the required radios are discovered. By default, all the radios are checked for all WLANs. This indicates that all radios can be adopted by all WLANs. Clarissa removes the checks for all the radios for all WLANs.

Clarissa then checks the appropriate radio for each WLAN.

The screenshot shows the WS2000 Wireless Switch configuration interface. On the left is a tree view under [Network Configuration] with items like LAN, WLAN, WAN, Wireless, WLAN1-4, Wireless QoS, WIPS, WIDS, and APs/Radios. The APs/Radios section is expanded, showing various radio types and APs. The main area is titled "Radio Adoption Table" and contains a table with columns for SL, Radio MAC, Radio Type, and WLAN1 through WLAN8. The table has four rows of data, with checkboxes in the WLAN columns. The bottom of the interface has buttons for Apply, Undo Changes, Help, and Logout, and a System Name field showing "SanJose1".

SL	Radio MAC	Radio Type	WLAN1	WLAN2	WLAN3	WLAN4	WLAN5	WLAN6	WLAN7	WLAN8
	ANY	ANY	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	00:A0:F8:BF:F1:44	802.11b	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	00:A0:F8:BF:EE:3C	802.11b	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	00:A0:F8:B5:4D:68	802.11b	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	00:A0:F8:B5:36:0D	802.11a	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Clarissa clicks the **Apply** button to save her choices.

## 12.11 Configuring the Cafe WLAN

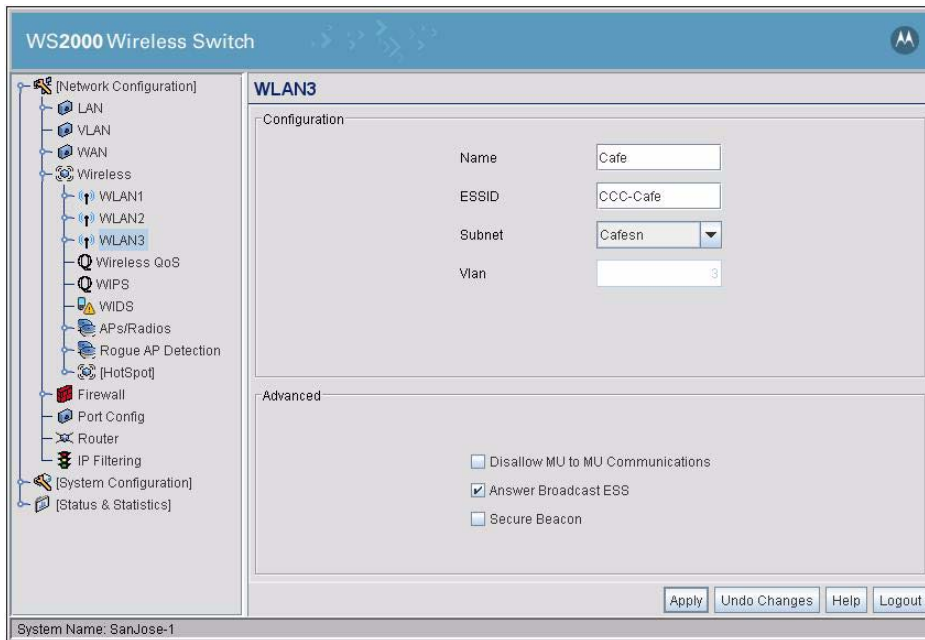
Clarissa clicks the button to the left of the Wireless menu item in the left menu. It opens up to show the individual WLANs. She selects the third WLAN. This is the WLAN which she plans to use for the cafe WLAN.

The WLAN name is used with in the WS2000 configuration screens to make the interface easier to navigate. She names this WLAN from "WLAN3" to "**Cafe**". She also gives it an ESSID of "**CCC-Cafe**". The ESSID is broadcast to the users and will be what the cafe users see when they select a wireless network on their laptops. Finally, she uses the Subnet pull-down menu to make this WLAN part of the third subnet, the "Cafesn" subnet.

She leaves the **Disallow MU to MU communications** option unchecked. She is certain that some cafe users will want to communicate between themselves, so she does not choose the Disallow.

She turns on **Answer Broadcast ESS** for this WLAN. Some mobile units come with a default ESSID of "101". This option allows the WLAN to respond to these mobile units even if the WLAN is set up with a

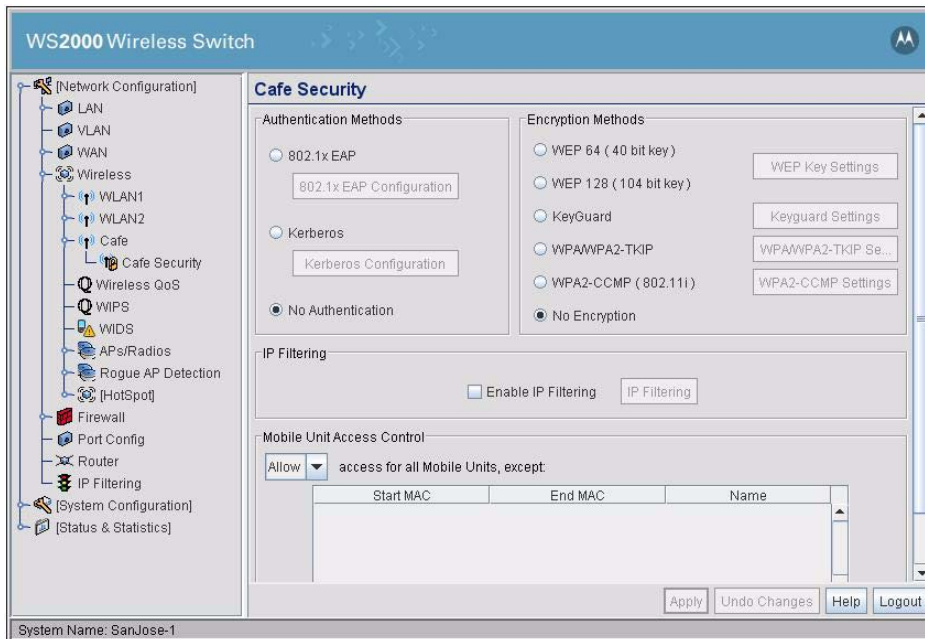
different ESSID. Since the cafe is a public access WLAN, leaving this option on will make it easier for the cafe customer to associate with the WLAN. For the private WLANs on this switch, she will turn this option off.



She clicks the **Apply** button to save her choices.

Clarissa goes to the left menu and clicks the button to the left of the Cafe WLAN node. A menu item labeled **“Cafe Security”** is displayed and Clarissa selects it.

She confirms that the Cafe Security screen shows that no authentication and no encryption methods.



Clarissa clicks the **Apply** button to save her choices.

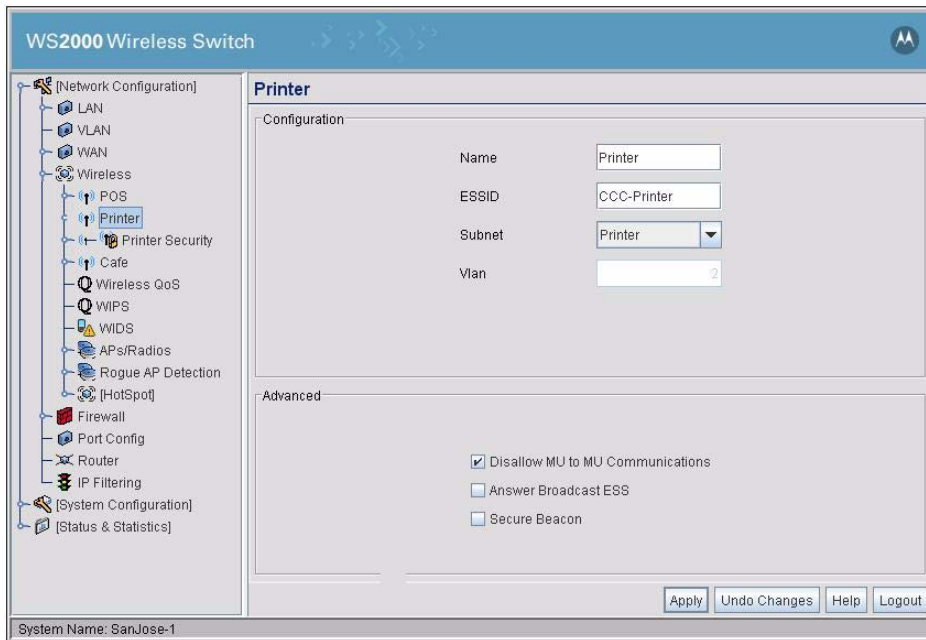
## 12.12 Configuring the Printer WLAN

For the printer WLAN, Clarissa makes the following selections:

Name	Printer
ESSID	CCC-Printer
Subnet	Printsn
Disallow MU to MU Communication	Yes
Secure Beacon	No
Answer Broadcast ESS	No

The wireless printers will never need to communicate with each other directly. MU-to-MU communications can be safely disallowed. Allowing **“Answer Broadcast ESS”** is a way to allow mobile units that are not configured with the network ESSID to associate with the WLAN. She knows that she will configure all of the mobile units on this WLAN with the correct ESSID, so she disallows this option, potentially keeping a cafe customer out of the printer WLAN.

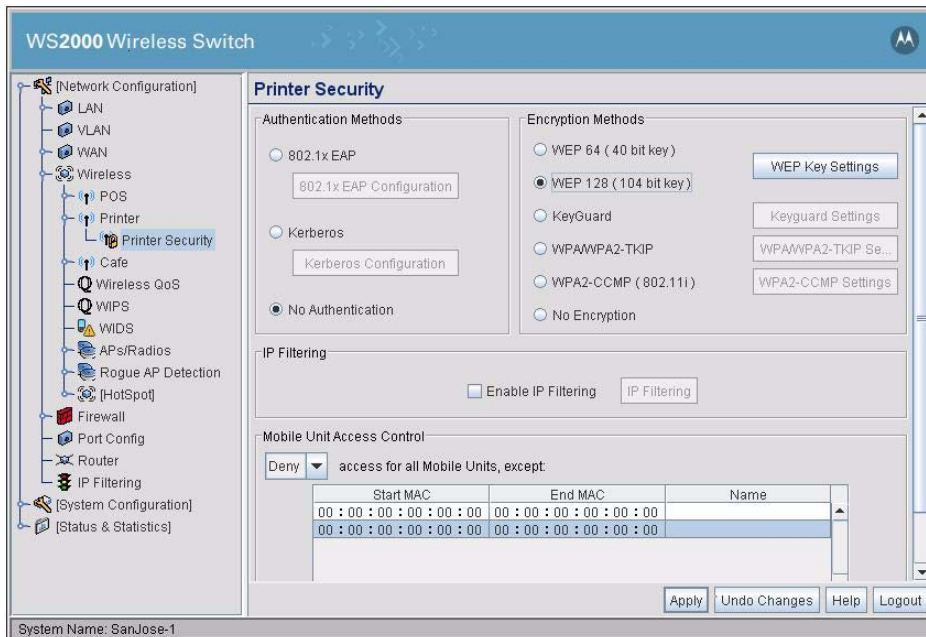




Clarissa clicks the **Apply** button to confirm her choices.



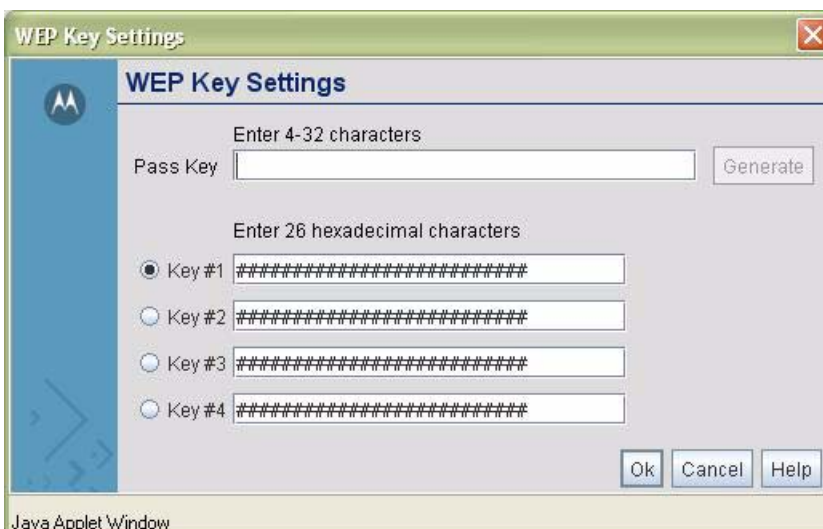
Clarissa clicks the + to the left of the Printer WLAN menu item and selects the **Printer Security** item. In the screen that displays, Clarissa selects no authentication. She enters the MAC numbers of the wireless printers in the Mobile Access Control section. The MAC numbers are unique numbers assigned to every network-cable hardware device and are usually listed on the same label that shows the device's model number and serial number. She enters each by clicking on the **Add** button and entering the MAC address in the Start MAC column of the new row.



She uses the Mobile Unit Access Control pull-down menu to select **Deny**. This specifies that the switch will deny access to any mobile unit that has a MAC address that is not listed.

In the Encryption Methods section, she selects **WEP 128 (104-bit key)**. WEP encryption is weak compared with WPA-TKIP, but still requires a day or so of solid traffic samples and a fair amount of effort to break. There is no data transversing this link that a data thief couldn't find in the trash. In any case, the store's wireless printers only support WEP.

She clicks the **WEP Key Settings** button and enters the keys she will use:



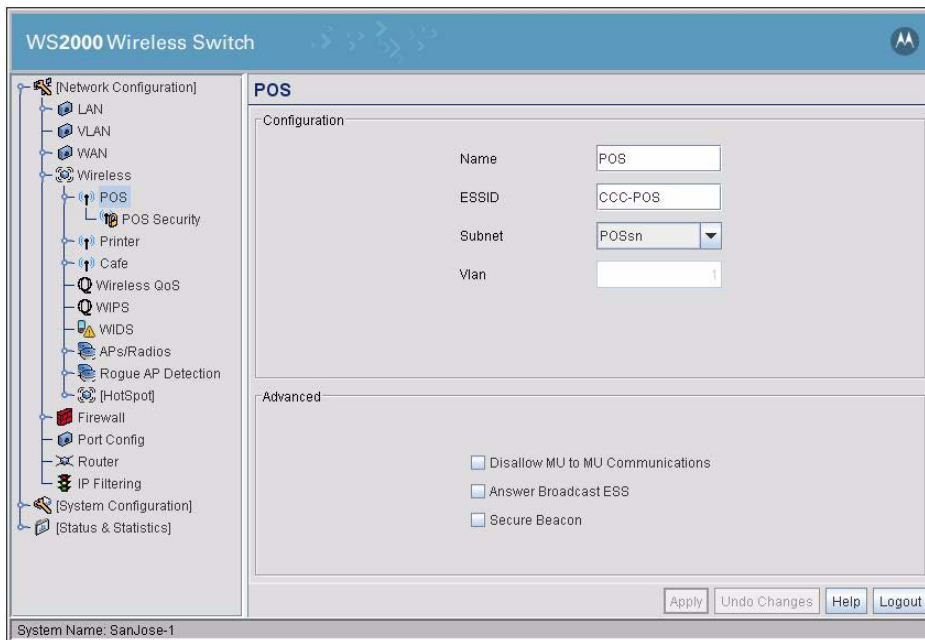
She clicks the **Ok** button to confirm the WEP key selections, then the **Apply** button to confirm the screen selections.

## 12.13 Configuring the POS WLAN

For the POS WLAN, she makes the following choices:

Name	POS
ESSID	CCC-POS
Subnet	POSsn
Disallow MU to MU Communication	No
Secure Beacons	No
Answer Broadcast ESS	No

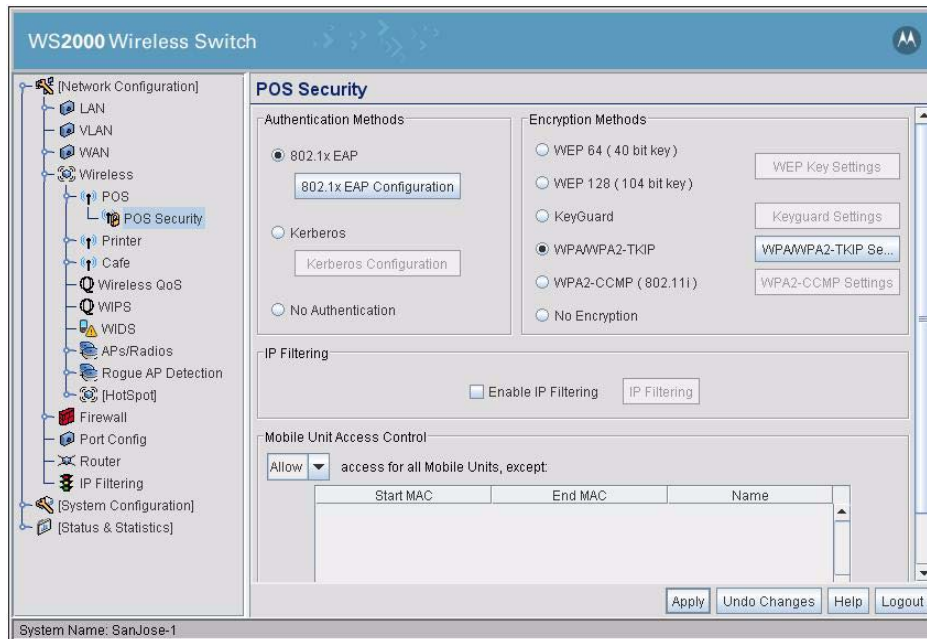
Allowing “**Answer Broadcast ESS**” is a way to allow mobile units which are not configured with the network ESSID to associate with the WLAN. She knows that she will configure all of the mobile units on this WLAN with the correct ESSID, so she disallows this option, potentially keeping a cafe customer out of the POS WLAN.



Clarissa clicks the **Apply** button to save her choices.

Clarissa then clicks the “+” to the left of the POS WLAN in the left menu and selects **POS Security**.

In that screen, she selects **802.1x EAP** for authentication. This will allow her to use the corporate RADIUS server for user authentication. Under Encryption Methods, she selects **WPA/WPA2-TKIP encryption**.



Then she selects the “**802.1x EAP Configuration**” key. In the next screen, she enters the corporate RADIUS server’s IP address, its port number, and the secret string needed to access it. In this case, her corporation is using a port number other than the standard one of 1812. She wants to allow the software to reauthenticate the users, but she is uncomfortable with the 3600 second (one hour) interval, and changes it to 10 minutes (600 seconds). She sees no reason to change the other 802.1x parameters.

**802.1x EAP Configuration**

**Server Settings**

	Primary	Secondary
Radius Server Address	69 . 32 . 12 . 14	69 . 33 . 12 . 14
Radius Port	5117	5117
Radius Shared Secret	YsJ7GikRon8	sT6Yv9Q3z

**Reauthentication**

Enable Reauthentication

Period  (30-9999) secs

Max. Retries  (1-99) retries

**Advanced Settings**

MU Quiet Period	<input type="text" value="10"/> (1-65535) secs	MU Timeout	<input type="text" value="10"/> (1-255) secs
MU Tx Period	<input type="text" value="5"/> (1-65535) secs	MU Max Retries	<input type="text" value="2"/> (1-10) retries
Server Timeout	<input type="text" value="5"/> (1-255) secs	Server Max Retries	<input type="text" value="2"/> (1-255) retries

**Radius Client Accounting**

Enable Accounting ( Save to CF Card )  Enable Syslog

MU Timeout  (1-255) sec Syslog Server IP

Retries  (1-10) retries

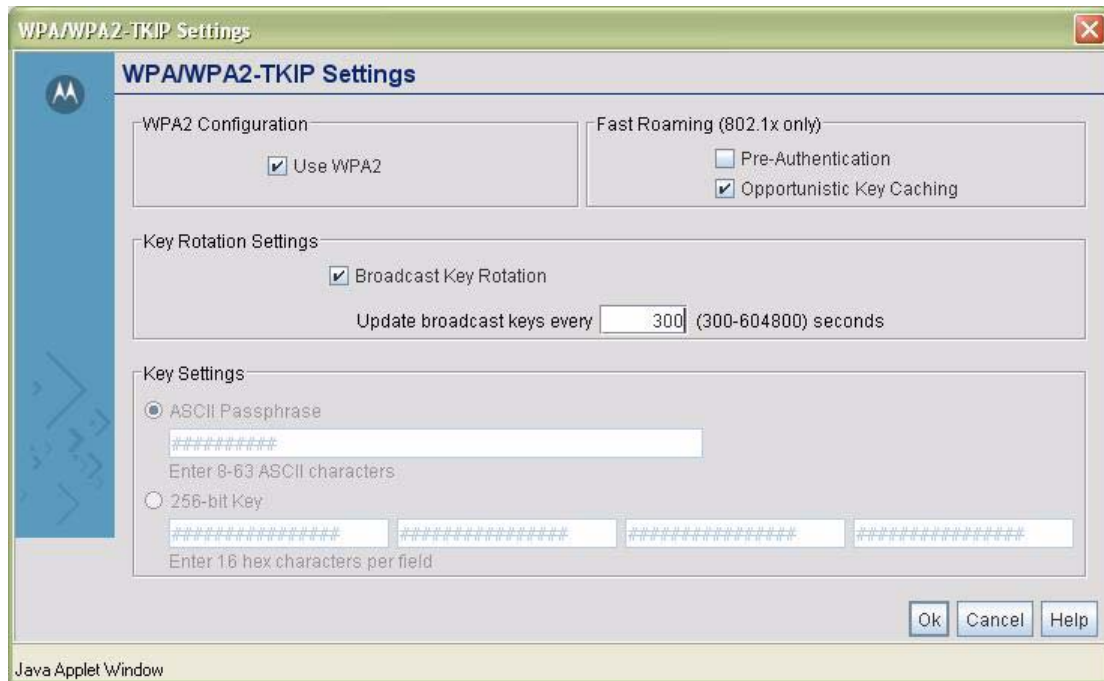
Java Applet Window

She clicks the **Ok** button in the 802.1x-EAP configuration window. She then clicks the **WPA-TKIP Settings** button in the security screen.

Clarissa selects the **Use WPA** choice to enable WPA. WPA is disabled by default.

TKIP encryption protocol calls for keys between two specific nodes to change with every packet. However, there is no standard with respect to how often one should change keys for broadcast packets. A very busy network with lots of broadcast packets could generate enough packets for successful decrypting in about an hour. Clarissa sets the system to rotate the broadcast keys every five minutes.

TKIP requires an initial shared key to start, so that all messages can be encrypted, including the first one. This initial key setting would be entered in the lower half of this screen, if it were needed. However, if 802.1x EAP user authentication is enabled, the authentication server will provide the initial key to the client and the key settings will be grayed out. In this case, Clarissa is using 802.1x EAP user authentication, so she does not have to enter an initial shared key.

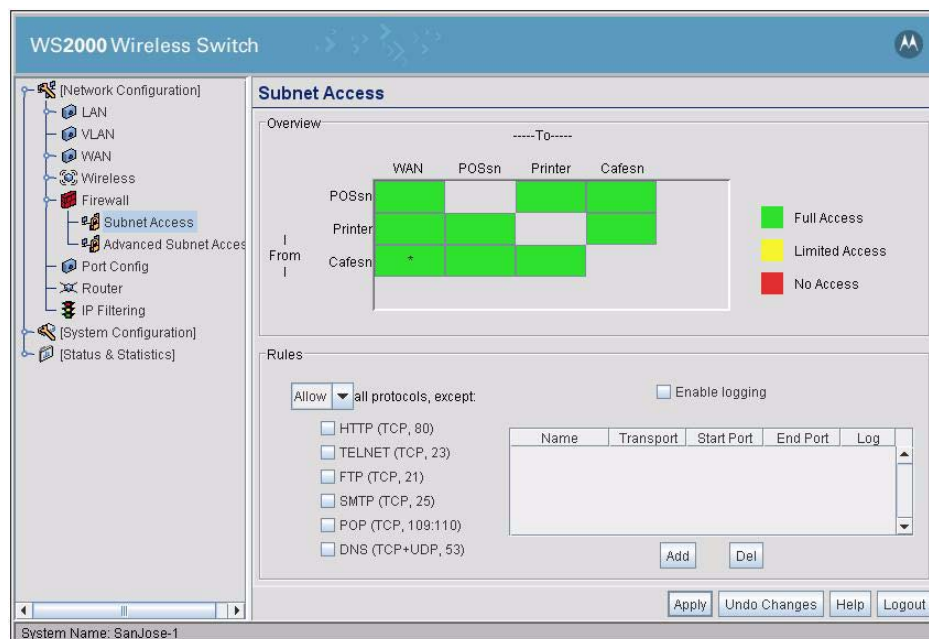


With this, Clarissa has finished configuring the basic WLAN configuration and the WLAN security. She clicks the **Ok** button in the WPA-TKIP window and then the **Apply** button in the WLAN security screen.

## 12.14 Configuring Subnet Access

Clarissa wants the two internal subnets to have complete access to one another, but she wants the Cafe subnet to have access only to the WAN.

In the left menu, she opens the **Firewall** item under Network Configuration and selects the **Subnet Access** node.



To set the subnet access for a pair of subnets, she clicks the square for traffic from one subnet to another and then uses the detail section, which appears below, to determine the rules for traffic between those two subnets.

She allows the Cafe subnet to have full access to the WAN. For the Cafe subnet to or from any other internal subnet, she selects the appropriate square, then uses the detail box below to “Deny” all protocols.

The screenshot shows the 'Subnet Access' configuration page. The Overview section displays a grid of access permissions between subnets. The Rules section shows 'Allow all protocols, except' with a list of protocols to be denied.

From \ To	WAN	POSsn	Printer	Cafesn
POSsn	Full Access	Full Access	Full Access	No Access
Printer	Full Access	Full Access	Full Access	No Access
Cafesn	Full Access	No Access	No Access	No Access

Rules section: Allow  all protocols, except.  Enable logging

- HTTP (TCP, 80)
- TELNET (TCP, 23)
- FTP (TCP, 21)
- SMTP (TCP, 25)
- POP (TCP, 109:110)
- DNS (TCP+UDP, 53)

For the POS subnet and the Printer subnet, she selects “Allow” all protocols when going to the WAN, the POS subnet, and the Printer subnet.

The screenshot shows the 'Subnet Access' configuration page, identical to the previous one. The Overview section displays a grid of access permissions between subnets. The Rules section shows 'Allow all protocols, except' with a list of protocols to be denied.

From \ To	WAN	POSsn	Printer	Cafesn
POSsn	Full Access	Full Access	Full Access	No Access
Printer	Full Access	Full Access	Full Access	No Access
Cafesn	Full Access	No Access	No Access	No Access

Rules section: Allow  all protocols, except.  Enable logging

- HTTP (TCP, 80)
- TELNET (TCP, 23)
- FTP (TCP, 21)
- SMTP (TCP, 25)
- POP (TCP, 109:110)
- DNS (TCP+UDP, 53)

After specifying all of the subnet access rules, she clicks the **Apply** button to save her changes.

## 12.15 Configuring the Clients

Clarissa has now finished configuring the switch. Next she configures the wired clients.

Going to each device, she gives it the IP address and other networking information that it will need to communicate with the switch:

Client	IP Address	Subnet Mask	Gateway	WS2000 Port
Wired POS terminal #1	192.168.0.4	255.255.255.0	192.168.0.1	4
Wired POS terminal #2	192.168.0.5	255.255.255.0	192.168.0.1	5
Server	192.168.0.6	255.255.255.0	192.168.0.1	6

Then she does the same thing with the wireless clients:

Client type	WLAN ESSID	Wireless channel	Authentication	Encryption
Wireless POS terminals	CCC-POS	3	802.1x EAP	WPA-TKIP
Handheld terminals	CCC-POS	3	802.1x EAP	WPA-TKIP
Wireless printers	CCC-Printers	7	None	WEP

The remaining tasks are to test the network and to put the Access Ports in their permanent locations.

### 12.15.1 Testing Connections

Clarissa powers up several sample devices and tests them, to be sure that they work as configured. She tests whether the devices can connect to the wireless switch and whether they can connect to devices on other subnets.

After she is confident that everything is working, she moves the Access Ports to their permanent locations. She connects the WS2000 to the DSL modem. Finally, she tests the connection from each subnet to the WAN.

The store network is now complete.

## 12.16 Field Office Use Case

### 12.16.1 A Field Office Example

#### 12.16.1.1 Background

Leo is the network administrator, system administrator, and IT professional for a field office with 60 employees. The users include sales people, sales engineers, office administration and customer support people. All of the sales personnel have laptops and many of them have personal digital assistants (PDAs).

The office is connected to the Internet and to corporate through a frame relay link. Between the office network and the frame relay, there is a router and a virtual private network (VPN) appliance. All traffic to corporate is encrypted by the VPN appliance. Traffic to other addresses passes straight through.

Leo installed a wireless access point about six months ago and quickly found that many employees preferred to use it. However, the throughput of the lone unit was not enough to service 40 or so users and coverage was weak in many areas of the building. In addition, Leo was doing user authentication by maintaining a list of permissible user MAC addresses on the access point. This required modifications to the list once or twice a week. Recently, when a laptop was stolen, Leo could not determine which MAC address to remove from the list for several hours. He concluded that a better method of user authentication was needed. Also, the data encryption on the old access point was WEP and WEP encryption can be broken with several hours of data encrypted with the same key. Leo changes the key every week, but some users complain when last week's key does not work anymore.

Leo has decided to upgrade to a WS2000 wireless switch. He will have four Access Ports, one in the administration office area, one in the sales office area, one in the sales engineering area, and one in the engineers' demonstration room. Throughput and coverage will increase significantly. Leo will convert to 802.1x/EAP-TTLS user authentication through the corporate RADIUS server and convert to WPA2 encryption, improving security considerably and reducing maintenance significantly.

Leo's company is also growing. Corporate has rented an expansion office for engineering in another part of the same building. Leo needs to establish secure communication from the engineering subnet to this expansion office. The other office will also have a WS2000, so Leo will establish a direct VPN link to that WS2000 and use the VPN as the secure communication link.

The following links show the tasks that Leo will carry out to complete the wireless upgrade.

## 12.17 The Plan

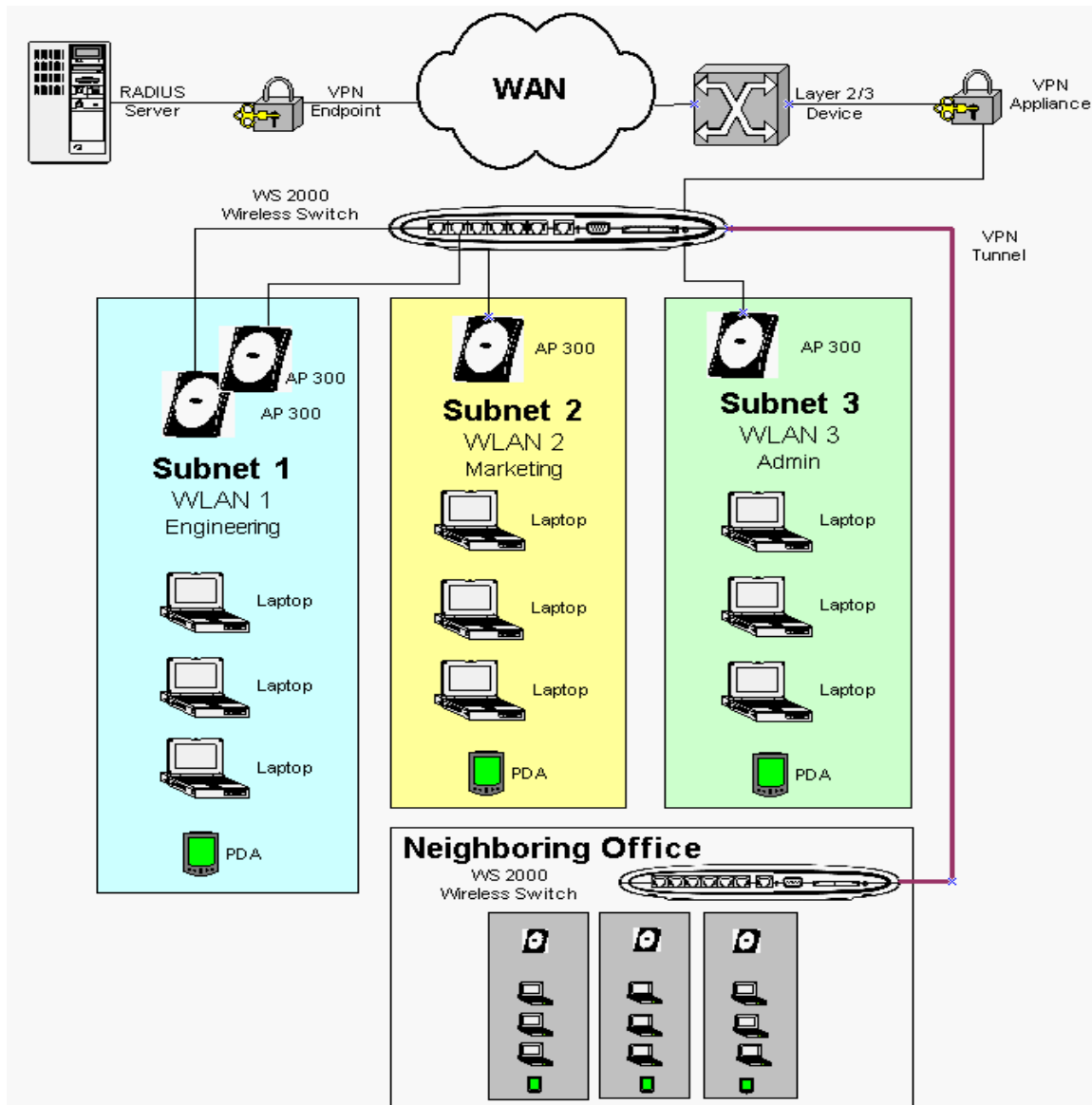
Each WS2000 WLAN has exactly one security policy, where a security policy is defined as a user authentication method and a data encryption method. Because each WLAN can have one and only one security policy, WLAN configuration is usually defined by the security needs of the installation. If two groups of users require different security policies, then they must associate to the WS2000 through different WLANs. See the retail case study for an example of an installation where different security needs drive the need for separate WLANs.

In this situation, all of Leo's users will use the same security system: 802.1x/EAP-TTLS user authentication and WPA data encryption. Leo can set up the WLANs in any way that is convenient.

Corporate has given Leo three static IP addresses for the wireless network. He will configure the WS2000 as a DHCP server giving out internal-use-only IP addresses and use network address translation (NAT) in the switch to convert the outward-bound traffic to one of the static IP addresses.



To keep things simple, he will define one subnet for the administration users, one subnet for the sales and marketing users, and one subnet for the engineers. Each subnet will have one WLAN associated with it and one Access Point. The only exception is the engineering subnet, which will have one WLAN and two Access Ports. The marketing subnet will not have any access to the engineering or administration subnets. All of the subnets will be restricted to just HTTP, SMTP, and POP access to the WAN.

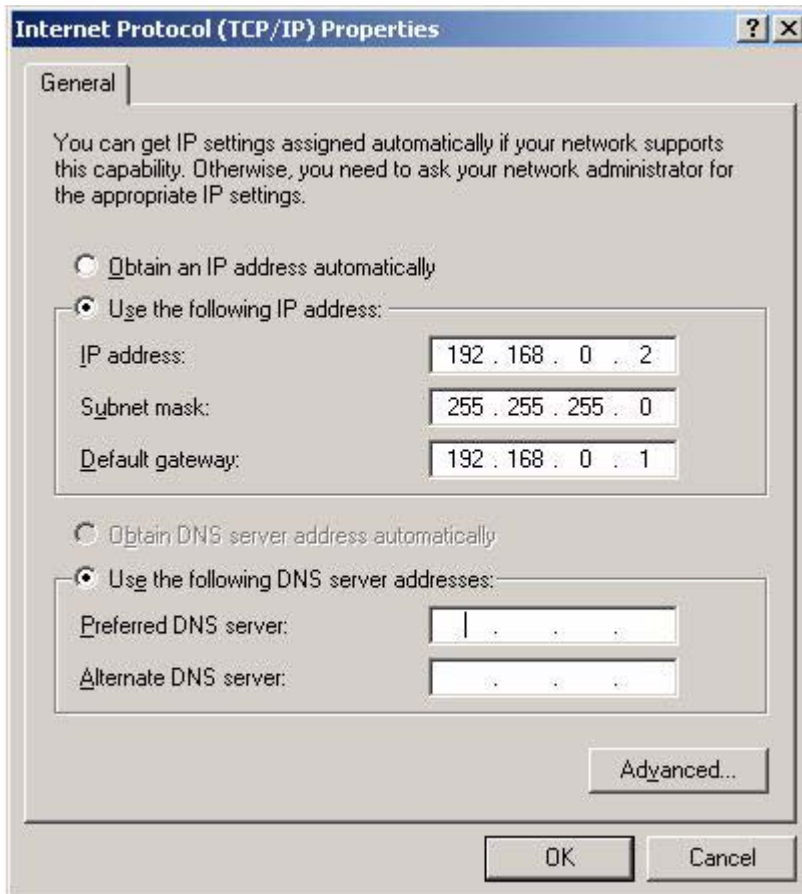


## 12.18 Configuring the System Settings

### 12.18.1 Contacting the Wireless Switch

To begin configuration of the switch, Leo sets up a communication link to the switch. Leo starts with a direct network link between his laptop and the switch, plugging the cable into one of the local, non-WAN, ports. The switch defaults to having all the LAN ports on the first subnet and that subnet having an IP address of **192.168.0.1**. So, as far as this connection is concerned, the switch comes up with an initial IP address of

**192.168.0.1**. He sets his laptop to have an IP address of **192.168.0.2** and a netmask of **255.255.255.0**. He also sets the gateway IP address to be **192.168.0.1**, the WS2000's IP address.



Leo launches his web browser and enters "<http://192.168.0.1/>" as the URL. He logs in using admin for the username and symbol as the password.



As soon as he logs in, the WS2000 asks him to set the password. He sets the administration password to something relatively secure.

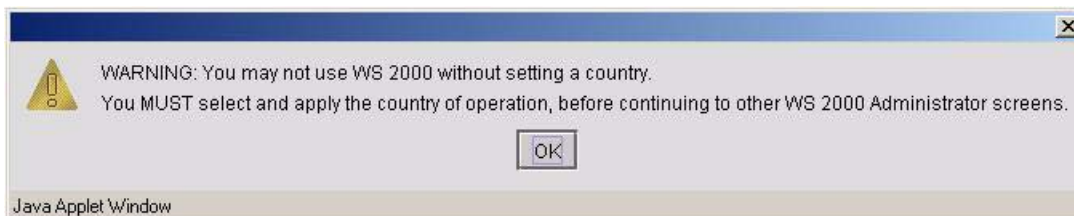


He presses **Update Password Now** to record his changed password.

### 12.18.2 Entering the Basic System Settings

The interface opens by displaying the **System Setting** screen. This screen is also accessible by clicking the toggle to the left of System Configuration in the left menu, then selecting **System Settings** in the left menu.

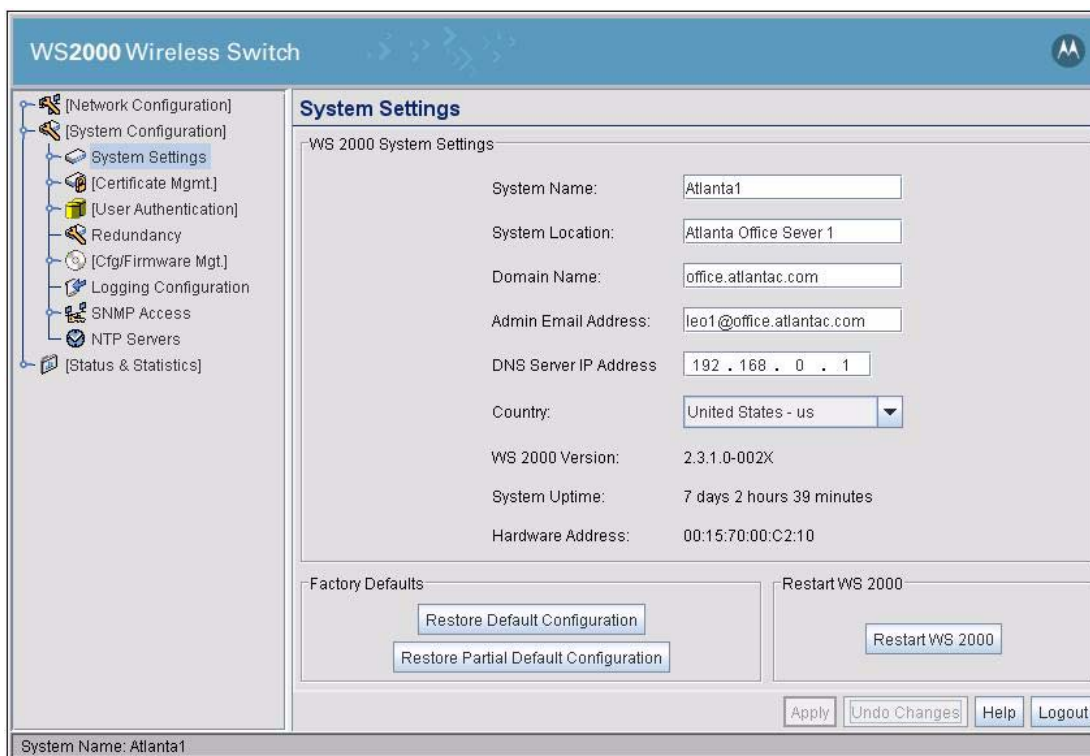
The first time System Settings are displayed, a dialog box is displayed, warning the administrator to select a country of operation.



Different countries have different regulations for the use of radio frequencies. Setting the location configures the switch to use only the channels, frequencies, and power levels that are legal for that country. Leo sets the location to United States - us.

The system name is used to distinguish between WS2000 switches for remote configuration. Leo gives the switch a descriptive name, **Atlanta1**. This name will appear in the footer for subsequent configuration windows for the switch. He does not need the descriptive name, but he wants to put in something appropriate in case he needs it later. If the office eventually has more than one wireless switch, the name will help him to know which switch he is working on.

He also enters his email address into the **Admin Email Address** box. Leo's corporation uses an SNMP manager which has the capability of monitoring network devices and sending email to the manager of a device that is in an unusual state. This is the email address that will be supplied to that SNMP manager for this switch.



### 12.18.3 Setting Access Control

Leo then clicks the **WS 2000 Access** node in the left menu. This controls which subnet can be used to reconfigure the WS2000 switch and how that reconfiguration can be accomplished. Leo will be inside the LAN, so he leaves on all means of reconfiguring from within the LAN. Corporate may want to have read access from outside the LAN, so Leo leaves on SNMP access from the WAN.

AirBEAM<sup>®</sup> is a Symbol Technology product for the management of software on wireless devices. Leo does not have a copy of AirBEAM yet, but he hopes to get one when the company purchases some Voice over IP (VoIP) phones. He also doesn't expect to access the switch from the Compact Flash card slot. So, he turns **AirBEAM Access** off.

The screenshot shows the WS2000 Wireless Switch configuration interface. The left sidebar contains a tree view with the following items: [Network Configuration], [System Configuration], System Settings (expanded), WS 2000 Access (selected), [Certificate Mgmt], [User Authentication], Redundancy, [Cfg/Firmware Mgt], Logging Configuration, SNMP Access, NTP Servers, and [Status & Statistics].

The main content area is titled "WS 2000 Access" and contains the following sections:

- WS 2000 Access Table:**

	From LAN	LOG	From WAN	LOG
Applet HTTP (port 80)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applet HTTPS (port 443)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CLI TELNET (port 23)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CLI SSH (port 22)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP (port 161)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CF Card Access : FTP/AirBeam (port 21)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Allow administrative access to:**
  - IP Address: [Empty text box]
  - Buttons: Add, Del
- WS2000 Certificate:** default (dropdown menu)
- Management Access across subnets

Below the main configuration area are several sub-sections:

- Secure Shell:**
  - Authentication Timeout: 120
  - SSH Client Inactivity Timeout: 120
- Admin Authentication:**
  - Local (selected), Radius
  - Authenticate AirBEAM user using Local DB
- Radius Server for Admin Authentication:**

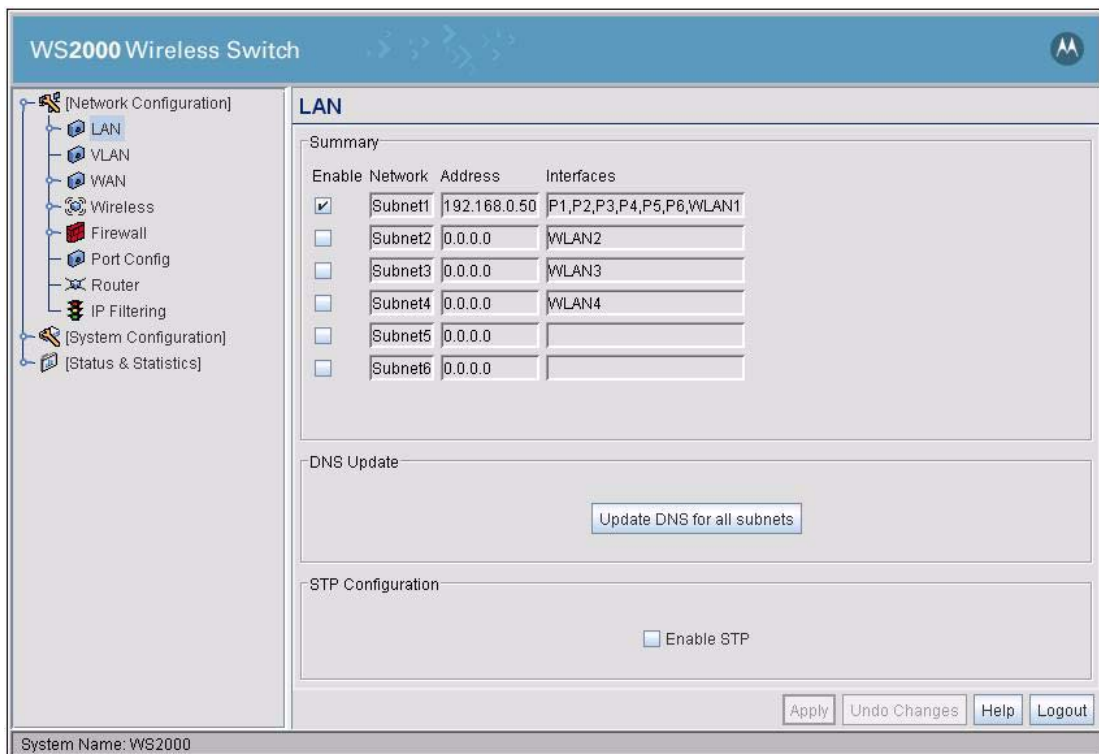
Radius Server IP	Port	Shared Secret
192.168.0.4	1812	#####
- AirBEAM Access:**
  - AirBEAM Username: airbeam
  - AirBEAM Password: #####
- Applet Timeout:**
  - HTTP/S Timeout: 0 Mins
- Administrator Access:**
  - Change Admin/Manager/Guest Admin Password

At the bottom of the interface are buttons for Apply, Undo Changes, Help, and Logout. The System Name is Atlanta1.

Leo clicks on the **Apply** button in the WS2000 Access screen to save his changes.

## 12.19 Configuring the LAN

Leo clicks the toggle to the left of Network Configuration in the left menu. The tree expands and he selects the **LAN** item.

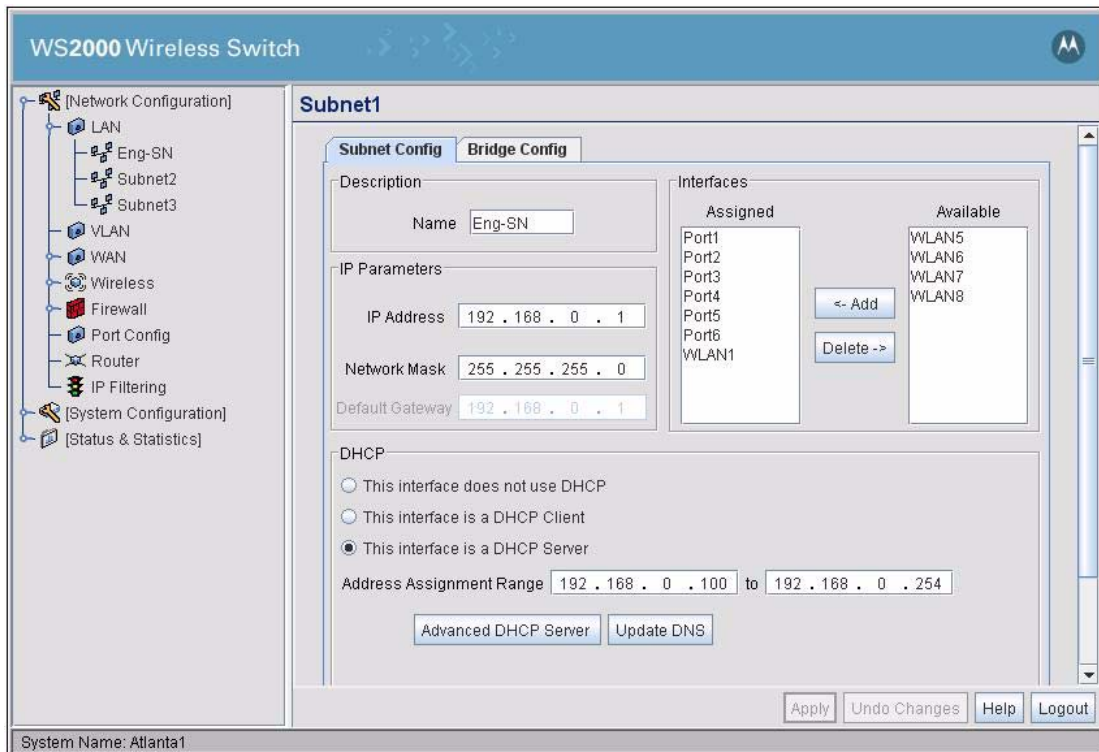


This screen shows the subnets, their IP addresses, and the network interfaces (the 10/100BaseT ports and the WLANs) that are currently associated with each subnet. Only the first subnet is initially enabled, so Leo clicks on the check boxes to the left of **Subnet2** and **Subnet3** to enable them. He clicks the **Apply** button to record his changes.

Next Leo needs to configure each of the subnets. He clicks the toggle symbol to the left of LAN in the left menu to expand it.

### 12.19.1 Configuring the Engineering LAN

Leo selects **Subnet1** from the choices under the LAN heading. He enters a new name for the subnet, **Eng-SN**, to make it easier to recognize this subnet throughout the WS2000 interface.



He also selects the option **This interface is a DHCP Server**. Choosing this DHCP option means that the switch will pick IP addresses from the Address Assignment Range and assign them to network clients on this subnet, as needed.

This screen also sets the IP address for the switch's interface to the subnet. Any address that starts with "192.168" is an internal-use-only IP address. That is, network administrators are free to use these IP addresses anyway they want, as long as the IP addresses are never visible to the outside world. The switch defaults to an address of 192.168.0.1 for the first subnet interface. Leo elects to use the range of IP addresses from **192.168.0.11** to **192.168.0.254** for the DHCP clients in this subnet.

Leo then selects the **Advanced DHCP Server** button. The DNS server IP addresses and the Gateway IP address entered here will be passed down the DHCP clients for this subnet for their own use while associated with this subnet. Leo enters the IP addresses that the corporation's IT department has specified for the corporate primary and secondary DNS servers. For the gateway, Leo enters the IP address for the subnet, the same IP address that he entered for the IP Address in the IP Parameters section of the Subnet screen.

The DHCP Lease Time (sec) specifies how long in seconds a client may keep an IP address when that client is not active on the net. The lease time is currently set for 86,400 seconds, or 24 hours. Leo expects that people using these WLANs will connect for a work day or not. While in the office, he expects that their machines will initiate contact with the network every 10 or 15 minutes for email. When they unplug to go home, this lease time will hold their IP address for another full day and not return it to the usable pool until the end of the next day. Leo would prefer that the lease time expire sometime during the night. He figures a lease time of somewhere between 10,000 seconds and 30,000 seconds is appropriate for this application. Leo sets it to 10000 seconds and figures he will change it if anyone complains.

The **WINS Server** field is designed to supply the Windows Network Server IP address to any DHCP clients that request it. Leo supplies the IP number for the local WINS server.



The **Domain Name** field will be supplied to any DHCP clients that request it. Leo enters his company's domain name.

**Advanced DHCP Server**

Enable Dynamic DNS

Single User Class Option

Multiple User Class Option

Primary DNS Server: 206 . 148 . 10 . 1

Secondary DNS Server: 206 . 148 . 10 . 2

Default Gateway: 192 . 168 . 0 . 1

WINS Server: 192 . 168 . 0 . 254

DHCP Lease Time (sec): 86400

Domain Name: \_\_\_\_\_

DNS Forward Zone: \_\_\_\_\_

TFTP Server Address: 0 . 0 . 0 . 0

Bootfile: \_\_\_\_\_

Option 189: \_\_\_\_\_

Option 43: \_\_\_\_\_

Static DHCP Mappings:

Client MAC	IP Address

Add Del

Ok Cancel Help

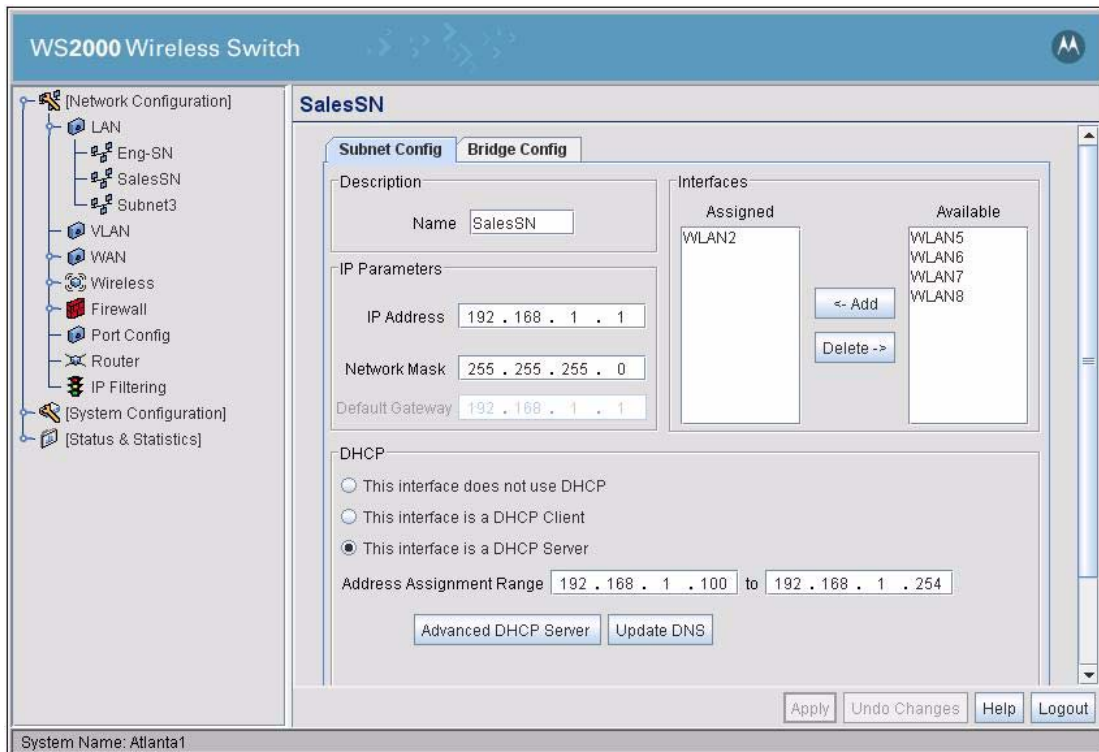
Java Applet Window

There is no reason to set up static DHCP mappings now. These would permanently lease an IP address to a client with a specific MAC address. Leo clicks the **Ok** button on the Advanced DHCP Server window, then the **Apply** button on the subnet window.

### 12.19.2 Configuring the Sales Subnet

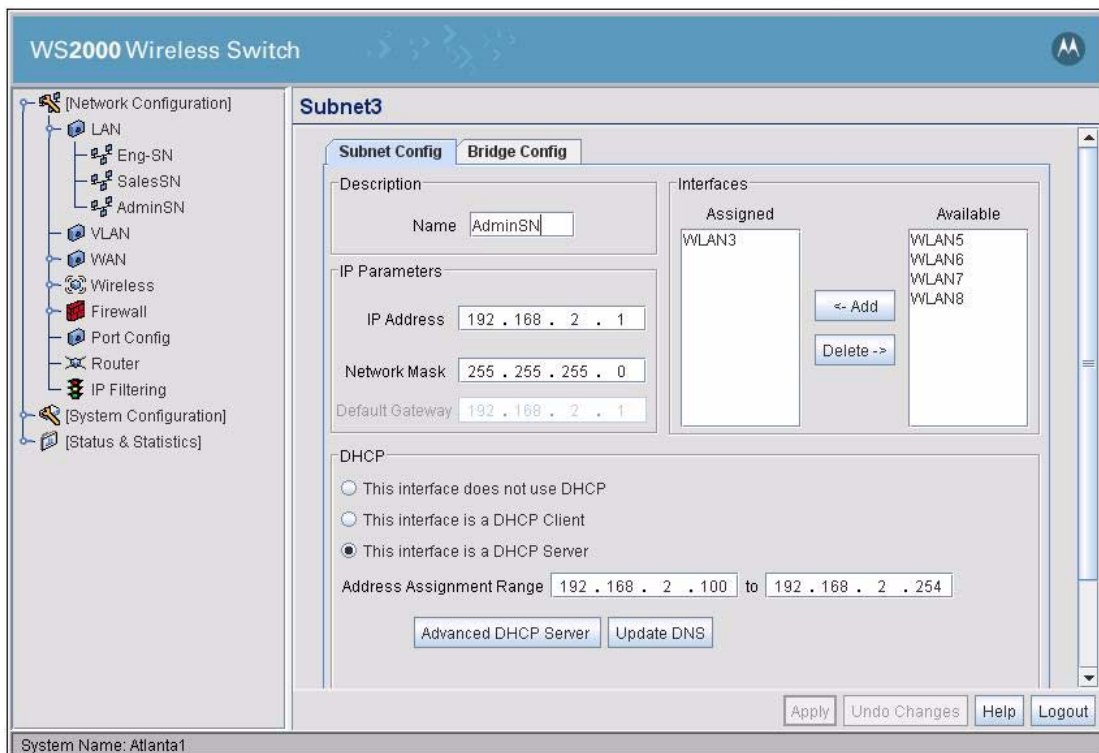
The sales and marketing subnet is configured exactly the same way as the engineering subnet, though with a different name and a different IP address range.





Leo selects the Advanced DHCP Server button and follows the same procedures as he did for the engineering subnet. Leo clicks the **Ok** button on the Advanced DHCP Server window, then the **Apply** button on the subnet window.

The administration subnet is configured in the same way:



Again, Leo fills out the advanced DHCP screen as he did for the two previous subnets. Leo clicks the **Ok** button on the Advanced DHCP Server window, then the **Apply** button on the subnet window.

The next step is to configure the WAN interface.

## 12.20 Configuring the WAN Interface

Next Leo configures the WS2000 WAN interface. This interface connects the WS2000 switch to the VPN appliance and, through that appliance, to the Internet.

Leo enables the WAN interface, but leaves the DHCP Client option disabled. Instead of using DHCP to get address information for the switch, he enters the permanent information which he previously obtained from the corporate network administrator. He enters the IP address for the switch, the gateway address (in this case, the VPN appliance), and the IP addresses of the corporate primary and secondary DNS servers.

The corporation has a frame relay link between this office, the corporate network and the Internet. If the connection to the WAN had been through a DSL link, the account information would be entered in the PPP over Ethernet section on the bottom of this screen. Since it will not be needed, Leo makes sure that the **Enable** check box in the PPP Over Ethernet section is not checked.

WS2000 Wireless Switch

WAN

Enable WAN Interface

**DHCP** **PPPoE**

This interface is a DHCP Client

IP Address: 157 . 235 . 208 . 215 [More IP Addresses](#)

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 157 . 235 . 208 . 246

Primary DNS Server: 157 . 235 . 187 . 3

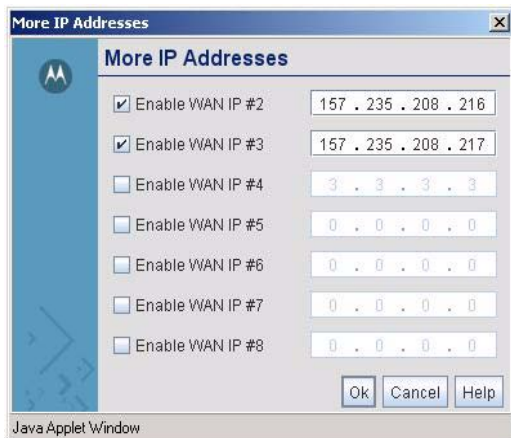
Secondary DNS Server: 157 . 235 . 187 . 131

Renew IP Refresh

Apply Undo Changes Help Logout

System Name: Atlanta1

Leo has three addresses for this switch. He plans to use one address for the traffic from each of the subnets. He clicks the **More IP Addresses** button and enters the other two IP addresses:

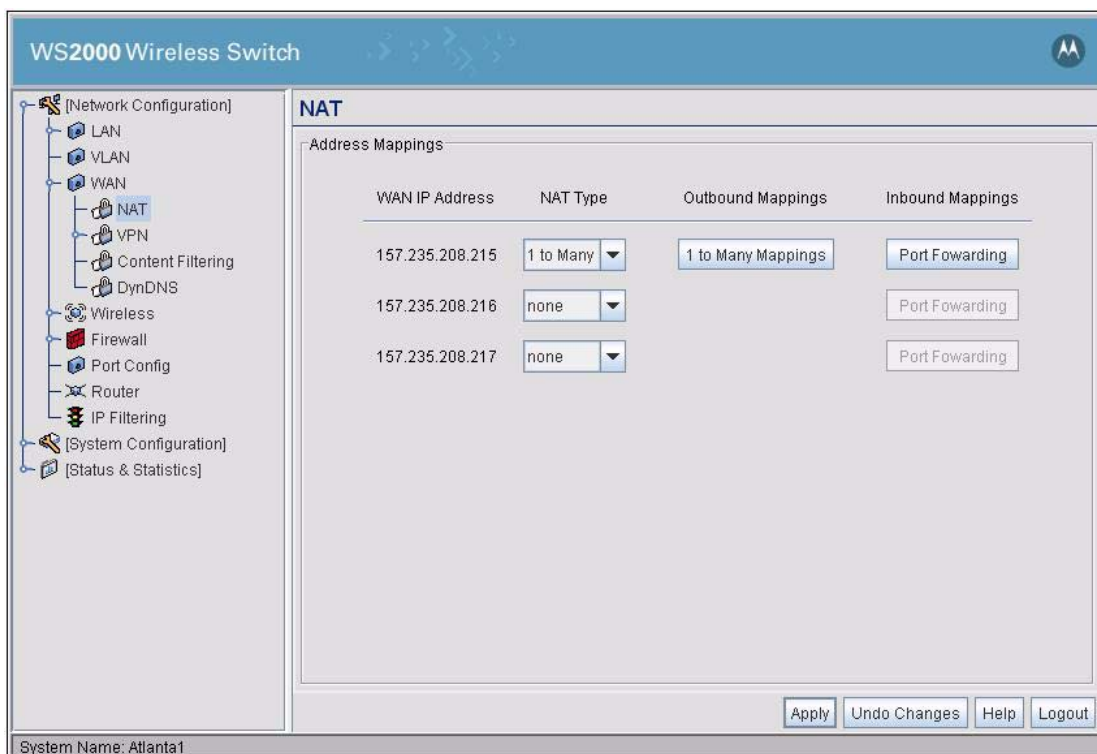


He clicks **Ok** button in the address window, then the **Apply** button on the WAN window to save his changes. The next step is to set up the network address translations (NAT).

## 12.21 Configuring the WAN Interface

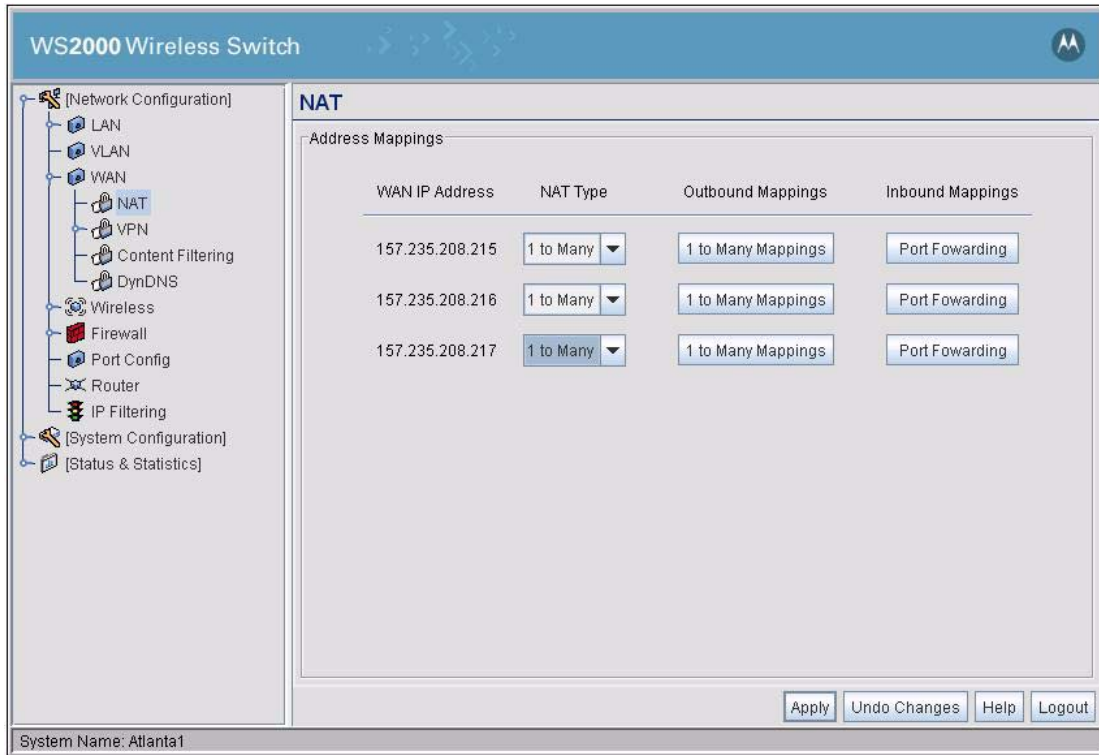
### 12.21.1 Setting Up Network Address Translation

After entering the IP addresses for the WAN interface, Leo clicks the toggle to the left of the WAN item in the left menu to expand it. He then selects the **NAT** item. The WS2000 displays the three IP addresses he entered when configuring the WAN.

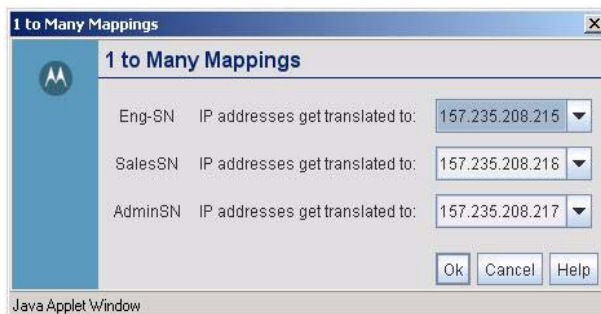


Each of these IP addresses will serve as the alias for all of the traffic from its corresponding subnet. That is, each IP address will serve as the only alias for many internal-only IP addresses. Leo chooses **1 to Many** in

the pull-down menus to the right of each IP number. As he does so, a **1 to Many Mappings** button appears to the right of the pull-down menus, in the **Outbound Mappings** column.



Leo clicks any of the **NAT Ranges** button to the right of the IP addresses. The 1 to Many Outbound Mappings window displays. Leo uses the pull-down menu to set the outbound IP address for each subnet. These are the same as the inbound IP addresses that he specified in the WAN configuration screen.

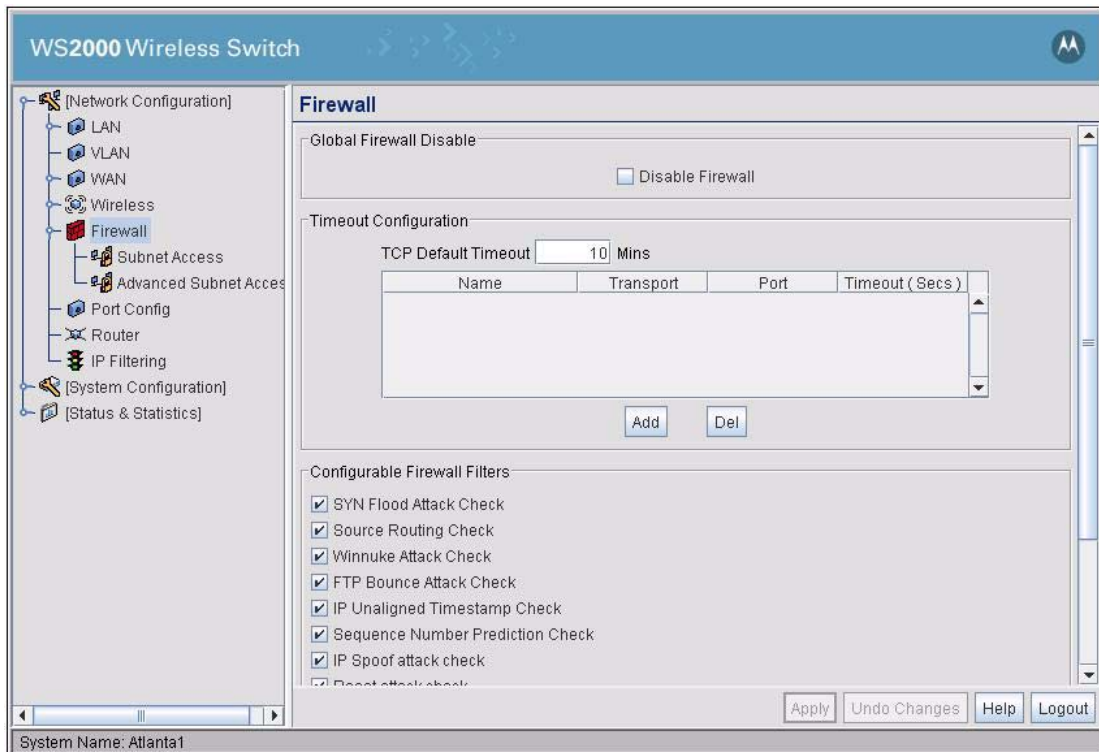


He clicks the **Ok** button to save his entries, then clicks the **Apply** button in the NAT screen.

The next step is to configure the firewall.

## 12.22 Confirm Firewall Configuration

After setting the NAT ranges, Leo selects **Firewall** under WAN in the left menu. The WS2000 displays a series of Configurable Firewall Filters, all of which are currently enabled.



Leo examines the list and sees no reason to turn off any of the filters. He clicks the **Apply** button.

The next step is to determine which Access Ports each WLAN will use.

## 12.23 Adopting Access Ports

Now that the LAN and WAN interfaces are configured, Leo needs to specify which Access Ports will go with which wireless LANs (WLANs). To do this, Leo needs the MAC address for each Access Port. He removes them from their packaging and connects them to the switch. The WS2000 discovers the connected APs automatically. Leo finds that they have consecutive MAC addresses: 00:A0:F8:BB:FC:94 through 00:A0:F8:BB:FC:97. He decides that he will deploy them as follows:

MAC Address	Location	WLAN	Adoption List Label
00:A0:F8:BB:FC:94	Engineering offices	Engineering	WLAN1
00:A0:F8:BB:FC:95	Demonstration room, engineering area	Engineering	WLAN1
00:A0:F8:BB:FC:96	Sales and marketing area	Marketing	WLAN2
00:A0:F8:BB:FC:97	Administration area	Admin	WLAN3

He marks each Access Port with its intended location and WLAN, so he will not get confused later.

Leo selects the **Wireless** item in the left menu. He sees that only the first wireless LAN is enabled. None of the WLANs have the names he would like them to have. He clicks on the check boxes to the left of **WLAN2** and **WLAN3**, then on the **Apply** button to enable these two WLANs.

**WS2000 Wireless Switch**

**Wireless**

**WLAN Summary** | **AP Adoption Configuration**

Enable	HotSpot	Name	ESSID	Subnet	Access Ports Adopted
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WLAN1	101	Eng-SN	1,2,3,4,5,6
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WLAN2	102	SalesSN	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	WLAN3	103	AdminSN	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN4	104	Subnet4	
<input type="checkbox"/>	<input type="checkbox"/>	WLAN5	105		
<input type="checkbox"/>	<input type="checkbox"/>	WLAN6	106		
<input type="checkbox"/>	<input type="checkbox"/>	WLAN7	107		
<input type="checkbox"/>	<input type="checkbox"/>	WLAN8	108		

**Miscellaneous**

WEP Shared Mode

SIP CAC Mode

Legacy mode (AP300)

HotSpot Credential Caching Mode

MU Inactivity Timeout:  Mins

Apply | Undo Changes | Help | Logout

System Name: Atlanta1

Now that the WLANs are enabled, Leo needs to specify which Access Ports go with which WLANs. He selects **APs/Radio** from the menu tree on the left. All discovered APs are listed in this screen.

**WS2000 Wireless Switch**

**Radio Adoption Table**

SL	Radio MAC	Radio Type	WLAN1	WLAN2	WLAN3	WLAN4	WLAN5	WLAN6	WLAN7	WLAN8
	ANY	ANY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	00:A0:F8:60:C8:58	802.11b	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	00:A0:F8:60:BE:2B	802.11a	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	00:A0:F8:B5:4D:68	802.11b	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	00:A0:F8:B5:36:0D	802.11a	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	00:A0:F8:BF:F1:44	802.11bg	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	00:A0:F8:BF:EE:3C	802.11a	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply | Undo Changes | Help | Logout

System Name: Atlanta1

He deselects the check boxes to the right of the row in which the MAC address range is specified as ANY.



For the engineering WLAN, Leo selects the AP with MAC of 00:A0:F8:BB:FC:94 and makes sure that all WLAN check boxes are not checked. He then selects the WLAN1 check box for this AP. He performs the same actions for the AP with MAC of 00:A0:F8:BB:FC:95.

For the Marketing WLAN, Leo selects the AP with MAC of 00:A0:F8:BB:FC:96. He makes sure that only the check box under the WLAN2 column is selected for this AP.

For the Marketing WLAN, Leo selects the AP with MAC of 00:A0:F8:BB:FC:97. He makes sure that only the check box under the WLAN3 column is selected for this AP.

The screenshot shows the WS2000 Wireless Switch configuration interface. The left sidebar contains a tree view of network configuration options, with 'APs/Radios' selected. The main area displays the 'Radio Adoption Table' with the following data:

SL	Radio MAC	Radio Type	WLAN1	WLAN2	WLAN3	WLAN4	WLAN5	WLAN6	WLAN7	WLAN8
	ANY	ANY	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	00:A0:F8:BB:FC:94	802.11b	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	00:A0:F8:BB:FC:95	802.11a	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	00:A0:F8:BB:FC:96	802.11b	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	00:A0:F8:BB:FC:97	802.11a	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	00:A0:F8:BF:F1:44	802.11bg	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	00:A0:F8:BF:EE:3C	802.11a	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the interface, there are buttons for 'Apply', 'Undo Changes', 'Help', and 'Logout'. The system name is 'Atlanta1'.

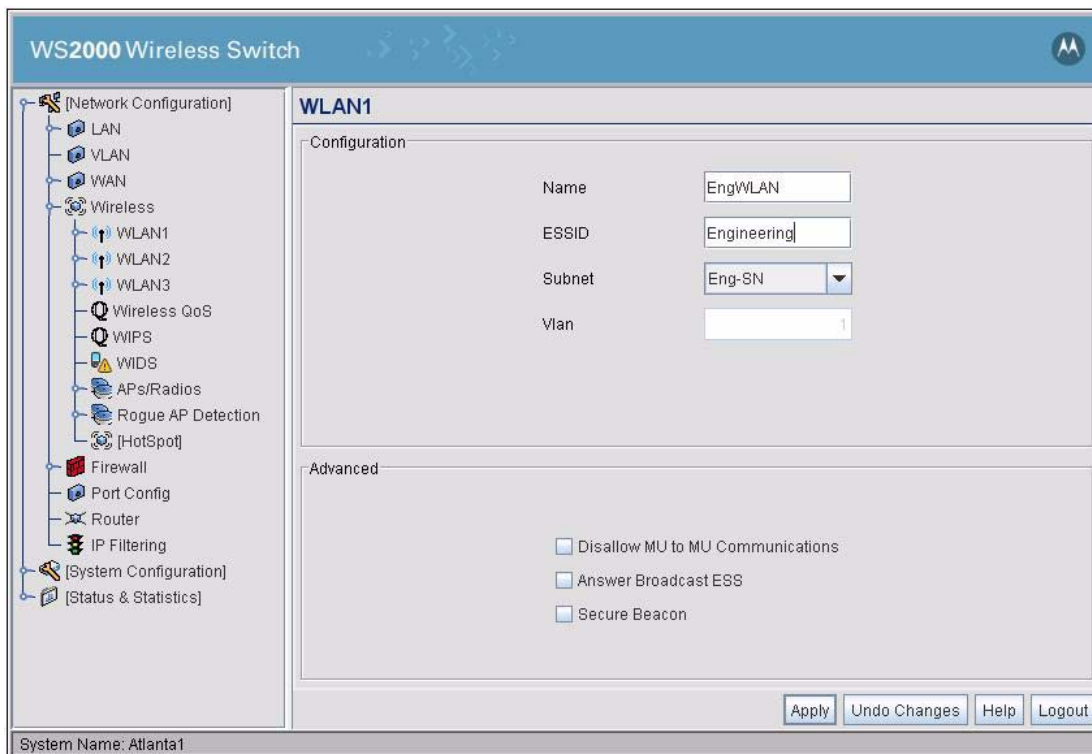
Leo clicks the **Apply** button to save his changes.

The next step is configure the WLANs.

## 12.24 Configuring the WLANs

Leo has specified which Access Ports go with which wireless LANs (WLANs). Now, he needs to name and configure each WLAN. He expands the **Wireless** node in the left menu, and selects the first WLAN listed.

Leo gives the WLAN the name **EngWLAN** so that subsequent screens in the WS2000 interface will be a little easier to read. The ESSID is the identification string that his users will see, so he uses a name that will be easy for them to recognize, the string **Engineering**. The interface shows that this WLAN is already part of the Engineering subnet, so there is no reason to change it.



In the Advanced section of the screen, the **Disallow MU to MU Communications** setting would keep mobile units from communicating directly with each other. Leo believes that people sometimes share files directly, laptop to laptop, instead of using the file server. Leo does not want to prevent this type of communication, so he leaves this option disabled.

**Answer Broadcast ESS** instructs the Access Ports on this WLAN to respond to communications from mobile units that do not know what the ESSID for the wireless network is and which are using a default ESSID of 101. Leo knows that there are no such units in the office; if there were they would not have worked with the previous access point. Leo leaves this check box unchecked.

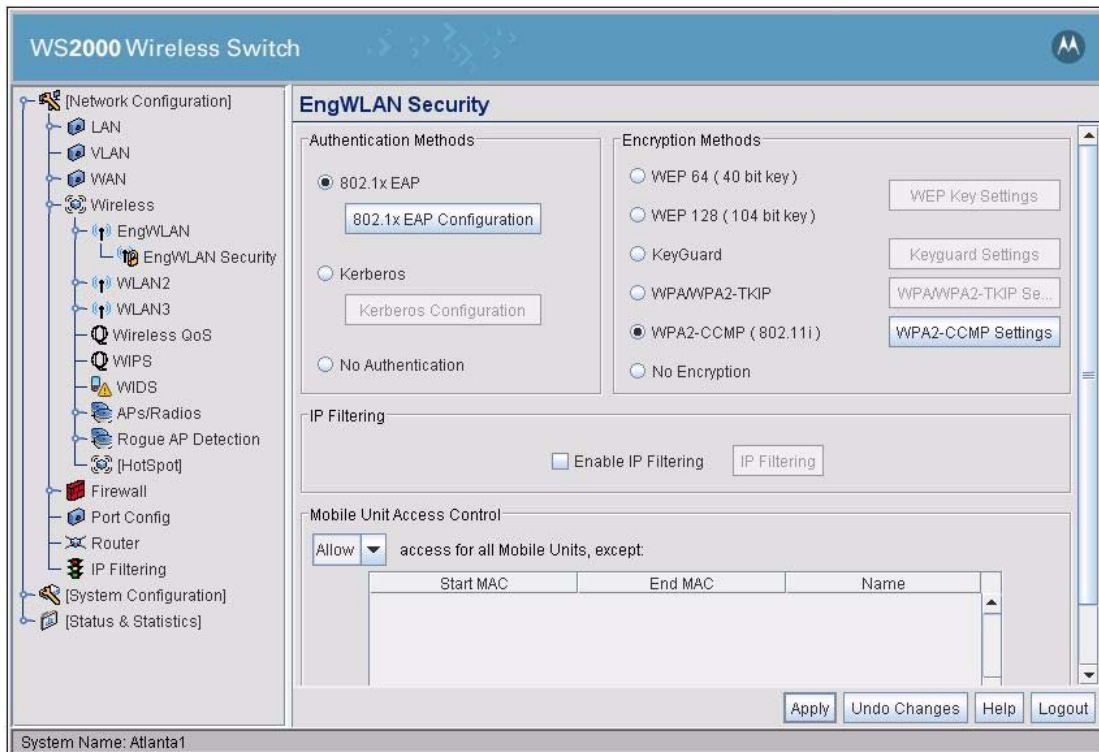
The **Secure Beacon** option prevents the APs from broadcasting the ESSID in its beacons. Leo turns on this option to further secure his corporate network.

Leo clicks the **Apply** button to save his changes.

### 12.24.1 Security

The next step to set security for the engineering WLAN. He selects the toggle to the left of EngWLAN in the left menu to display the **EngWLAN Security** item. Leo selects that item and the security screen is displayed. Leo selects **802.1x EAP** as the authentication method and **WPA2-CCMP** as the encryption method.





Leo also needs to configure the 802.1x EAP system and the WPA2 encryption. Leo clicks **802.1x EAP Configuration**. In the window that appears, he enters the RADIUS server information that he obtained from corporate system administration: the IP addresses of the RADIUS servers, the ports used for RADIUS communication, and the secret string used to start communication. He leaves the rest of the parameters at their default settings.

**802.1x EAP Configuration**

**Server Settings**

	Primary	Secondary
Radius Server Address	208 . 200 . 100 . 99	208 . 200 . 100 . 100
Radius Port	1812	1812
Radius Shared Secret	motorola	motorola

**Reauthentication**

Enable Reauthentication

Period:  (30-9999) secs

Max. Retries:  (1-99) retries

**Advanced Settings**

MU Quiet Period	<input type="text" value="10"/> (1-65535) secs	MU Timeout	<input type="text" value="10"/> (1-255) secs
MU Tx Period	<input type="text" value="5"/> (1-65535) secs	MU Max Retries	<input type="text" value="2"/> (1-10) retries
Server Timeout	<input type="text" value="5"/> (1-255) secs	Server Max Retries	<input type="text" value="2"/> (1-255) retries

**Radius Client Accounting**

Enable Accounting (Save to CF Card)  Enable Syslog

MU Timeout:  (1-255) sec

Retries:  (1-10) retries

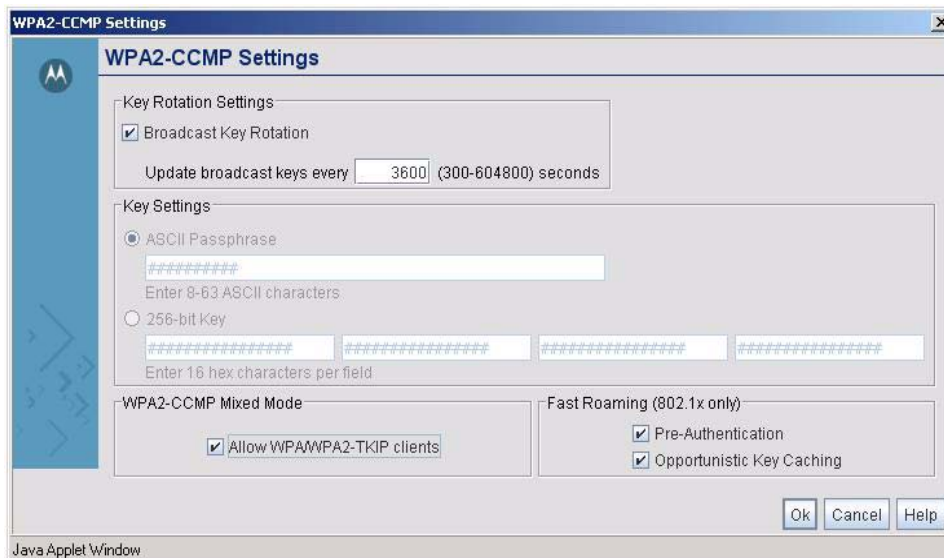
Syslog Server IP:

Java Applet Window

Leo clicks the **Ok** button to save the 802.1x EAP settings.

Leo then clicks the **WPA2-CCMP Settings** button. WPA2 constantly changes keys, but requires an initial key, known to both ends of the communication. If Leo was not using 802.1X EAP user authentication, that initial key would need to be entered here, in the Key Settings section. However, with 802.1x EAP, the RADIUS server supplies the initial key, so that Key Settings section is grayed out for Leo.

Leo does need to set the frequency with which the key for broadcast communication is changed. By default, the WS2000 changes the broadcast every 84,600 seconds, i.e., every twenty-four hours. Breaking WEP encryption requires several hours of solid traffic, so Leo decides to change the broadcast key rotation to 3600 seconds, or once an hour.



Leo also selects **Allow WPA/WPA2-TKIP clients** in the section labelled WPA2-CCMP Mixed Mode. WPA-TKIP is an earlier version of the WPA encryption method. WPA2 is more secure, but not all wireless clients in Leo's office are WPA2-capable. Selecting this option allows the older clients to use WPA-TKIP when they are not WPA2-CCMP-capable.

Leo also selects **Pre-Authentication** and **Opportunistic Key Caching** in the Fast Roaming section. These are options that are designed to make it easier for 802.1x wireless clients to roam within a WLAN. Under **Pre-Authentication**, a wireless client connected to one Access Port can communicate with other Access Ports and begin the authentication procedure before beginning to actual use that Access Port for network traffic. Under **Opportunistic Key Caching**, a wireless client which has agreed upon a given Pairwise Master Key (PMK) with one Access Port on a given WS2000 is allowed to use that same PMK with other Access Ports connected to the same WS2000. Both options increase the speed of roaming under 802.1x security and Leo enables both of them.

Leo clicks the **Ok** button to save his WPA2-CCMP settings, then the **Apply** button to confirm the WLAN configuration.

This completes configuration of the engineering WLAN. The sales and marketing WLAN and the administration WLAN are configured exactly the same way, with the sole exception that they take different names and ESSIDs.

WLAN	WS2000 Name	ESSID
Sales and Marketing	MrkWLAN	Marketing
Administration	AdmWLAN	Administration

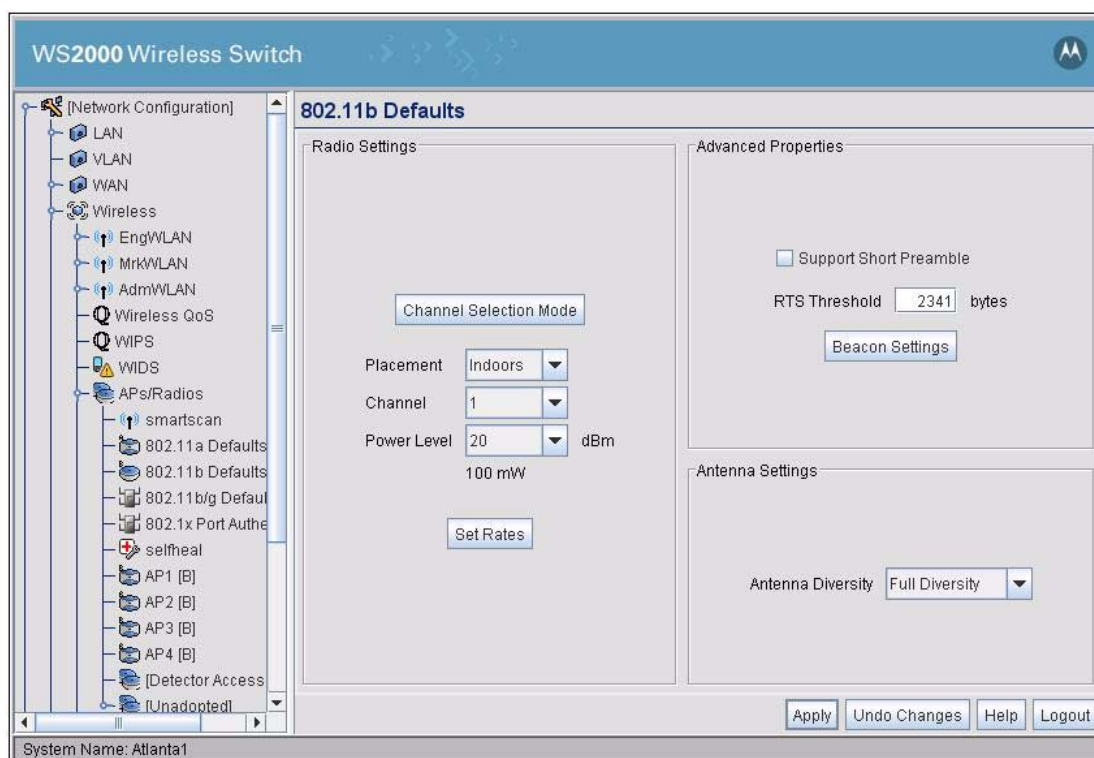
After these WLANs are configured, the next step is to configure the Access Ports.

## 12.25 Configuring the Access Ports

The WS2000 allows the user to specify default settings for Access Ports. Leo expands the **APs/Radios** node in the left menu and selects the **802.11b Defaults** node. Leo has four AP200 ports and he will be able to set the defaults for these in this section.

All the Access Ports will be indoors, so he specifies **Placement** as Indoors. He sets the default **Channel** as 1, even though all of his Access Ports will be using different 802.11b channels. He sets the **Power Level** to 20dBm. This will broadcast at 100 mW, the maximum level allowed in the US.

He does not change the settings for **Antenna Diversity**, **Support Short Preamble**, **RTS Threshold**, or **Beacon Settings**. These parameters control some of the broadcast mechanics of an 802.11 communication between mobile units and Access Ports. In most cases, there is no reason to change them. He clicks **Apply** to save his choices.

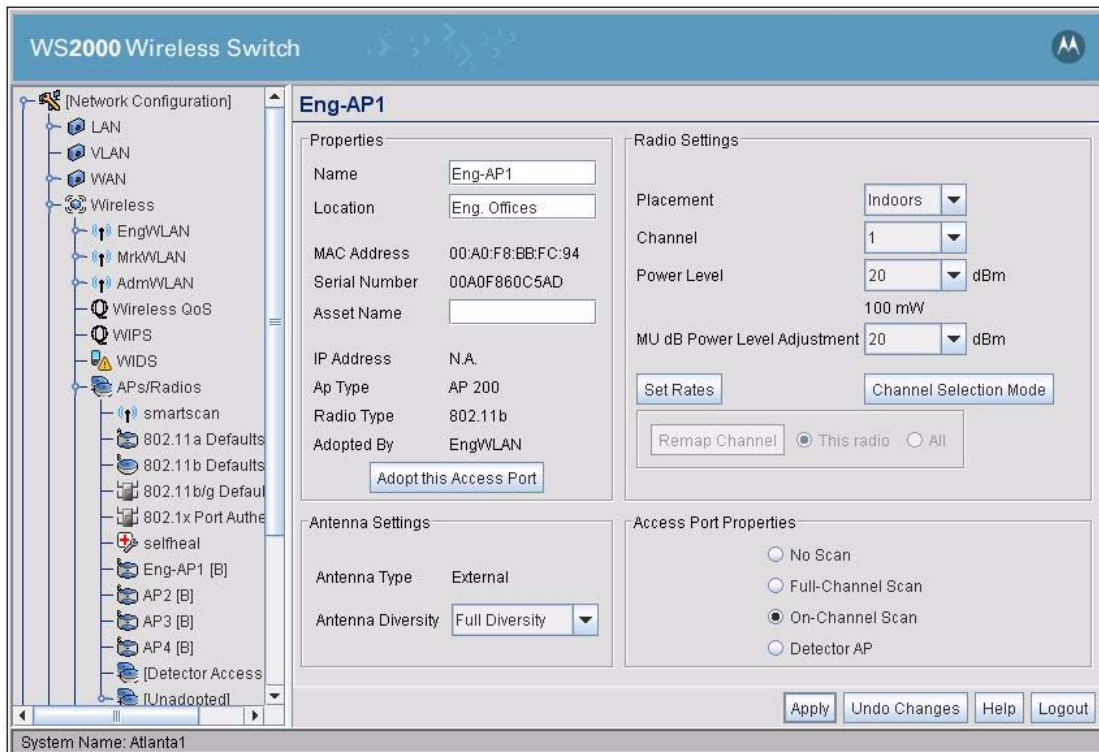


After configuring the default Access Port settings, Leo gets four short 100baseT cables and connects the four Access Ports to the switch. Just to make it easier to remember which port is which, he connects the one with the lowest MAC address to the first port number, the next lowest MAC address to the next port, and so on.

As he configures each Access Port, he will need to assign each Access Port to a channel. He can minimize radio interference if he has the radio channels for the different Access Ports separated as much as possible. He decides to use the following allocation:

Access Port	Channel
Engineering Offices	1
Demo Room	4
Sales and Marketing	7
Administration	10

He clicks the toggle to the left of Access Ports in the left menu and selects the menu item labeled **AP1**. The WS2000 has found and queried the Access Port for its MAC address. Leo enters a new name for the Access Port, **Eng-AP1**, and its location, **Eng. Offices**.



He sets the channel at 1, and notes the number. Access Ports channels should be separated as much as practical to minimize interference between them. The other engineering Access Port will use channel 4 and the marketing Access Port will use channel 7. He then sets the **Power Level** at the maximum setting of 100mW.

Before he can change the channels, Leo checks the **Channel Selection Mode**. The default Channel Selection mode is set under the respective radio's default screen. The default channel selection mode for 'b' radio is *User Selection*. Leo clicks the **Channel Selection Mode** button to display the *Channel Selection Mode* dialog.

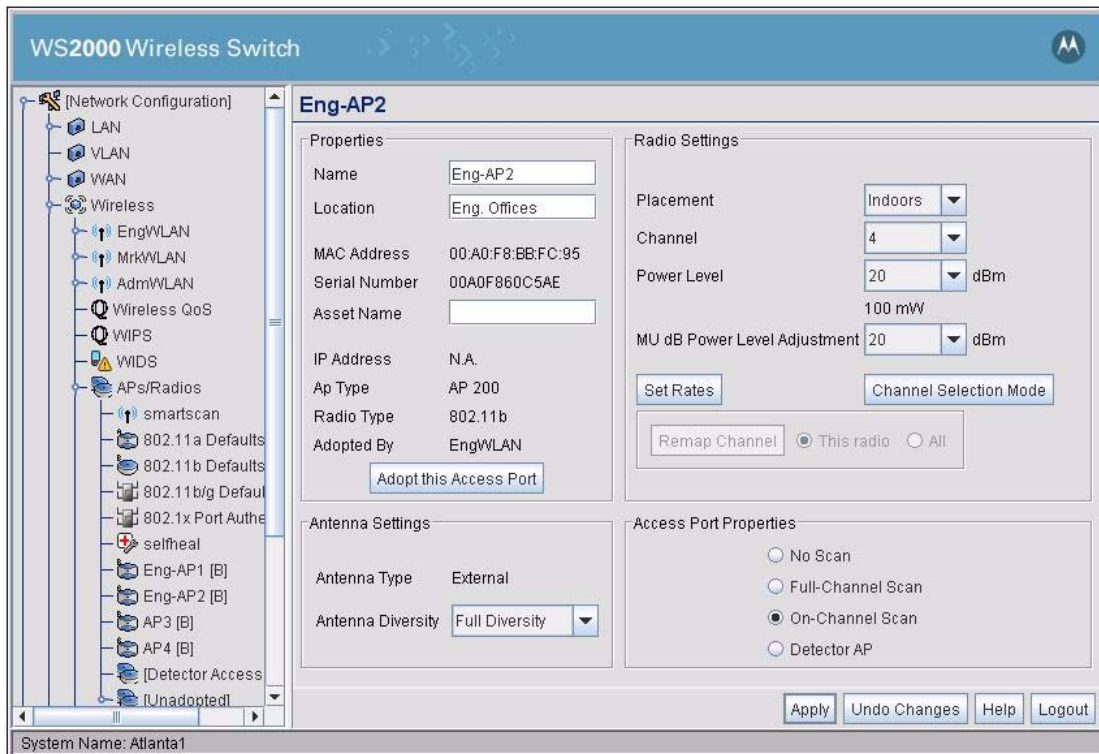


In the dialog, he selects **User Selection** option and clicks the **Ok** button to close and return back to the AP screen.

He also sees no reason to change the settings for **Antenna Diversity**, **Support Short Preamble**, **RTS Threshold**, or **Beacon Settings**. These parameters control some of the broadcast mechanics of an 802.11 conversation between mobile units and Access Ports. In most cases, there is no reason to change them.

He clicks the **Apply** button to save his changes.

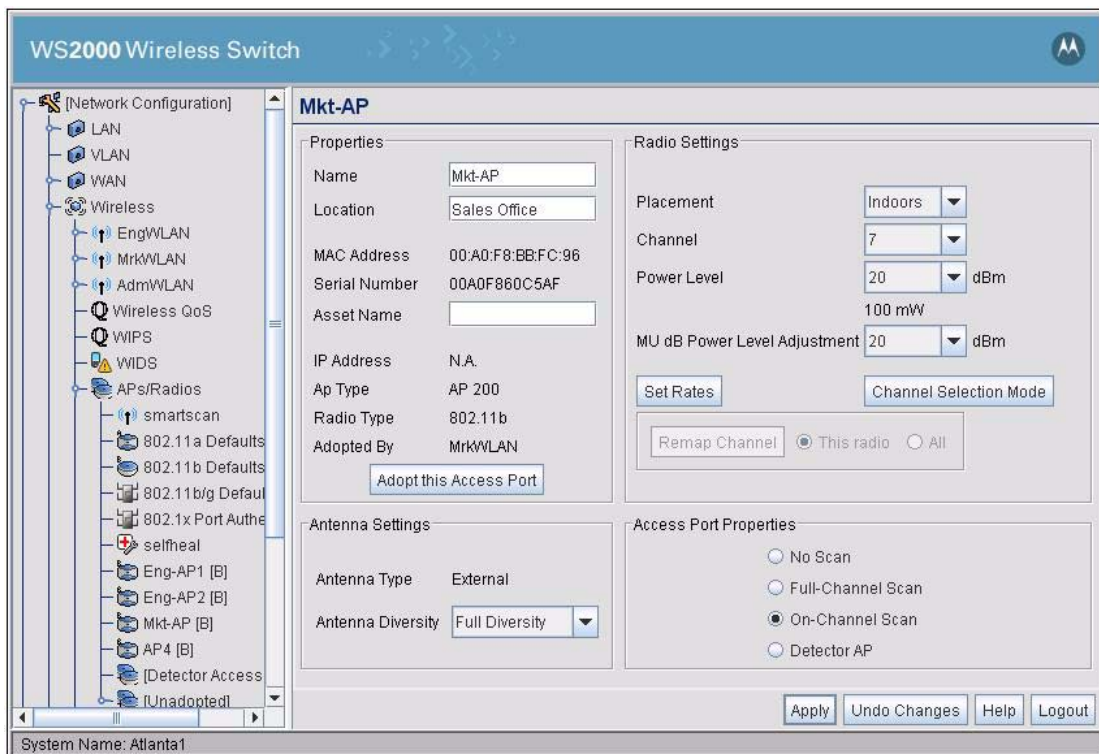
Leo then selects **AP2**, the second engineering Access Port. He gives it a new name, a location, and assigns it channel 4.



Leo clicks the **Apply** button to save the configuration for this Access Port.

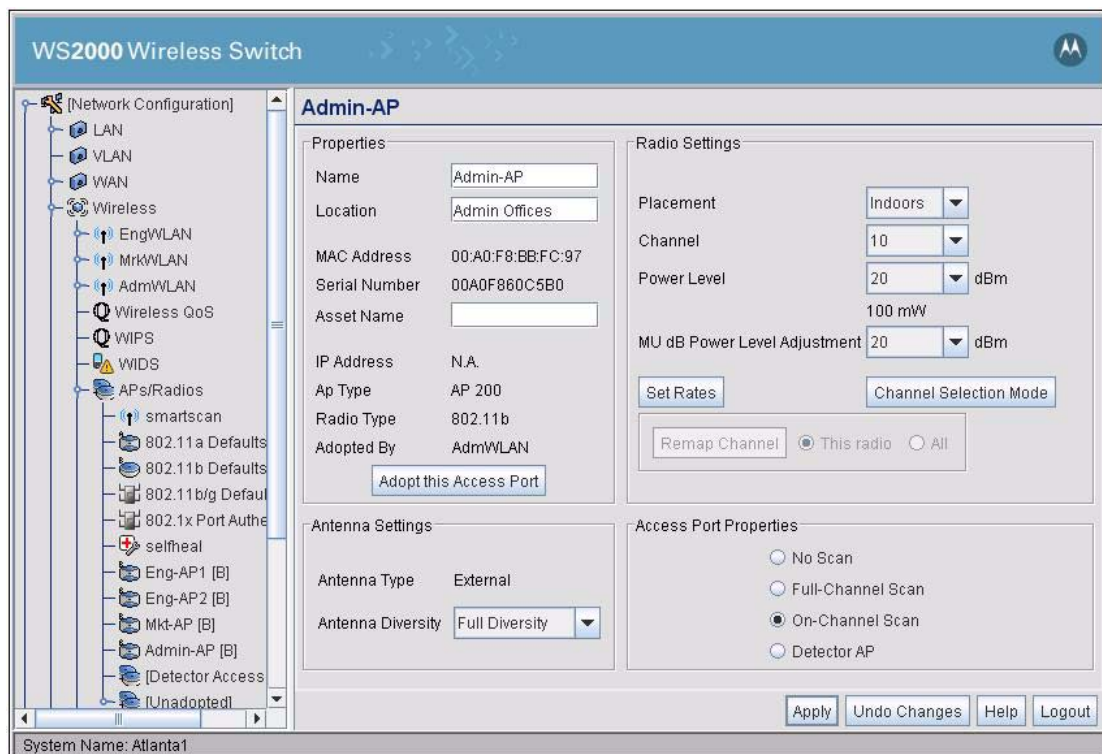
Leo then selects the third Access Port in the left menu. This will be the sales and marketing Access Port. Leo configures it similarly, but uses channel 7.





Leo clicks **Apply** to save his changes.

To avoid interference with the sales and marketing AP, Leo chooses channel 10 for the administration Access Port. He then enters the **Access Port Name** and **Location**.



Leo clicks the **Apply** button to save the changes for the administration Access Port.

The Access Ports are now configured. The next step is to specify access levels between the subnets.

## 12.26 Configuring Subnet Access

Leo selects the **Firewall --> Subnet Access** item in the left menu. This screen determines what subnet-to-subnet traffic is allowed.

The screenshot shows the 'Subnet Access' configuration screen in the WS2000 Wireless Switch interface. The left-hand navigation menu is expanded to show 'Subnet Access' under the 'Firewall' category. The main area displays a matrix for configuring access between subnets. The matrix has columns for 'To' (WAN, Eng-SN, SalesSN, AdminSN) and rows for 'From' (Eng-SN, SalesSN, AdminSN). A legend on the right indicates that green represents 'Full Access', yellow represents 'Limited Access', and red represents 'No Access'. The matrix shows Full Access (green) for all connections except for SalesSN to Eng-SN and AdminSN, which are currently set to Full Access (green).

	From	WAN	Eng-SN	SalesSN	AdminSN
Eng-SN	Full Access	Full Access	Full Access	Full Access	
SalesSN	Full Access	Full Access	Full Access	Full Access	
AdminSN	Full Access	Full Access	Full Access	Full Access	

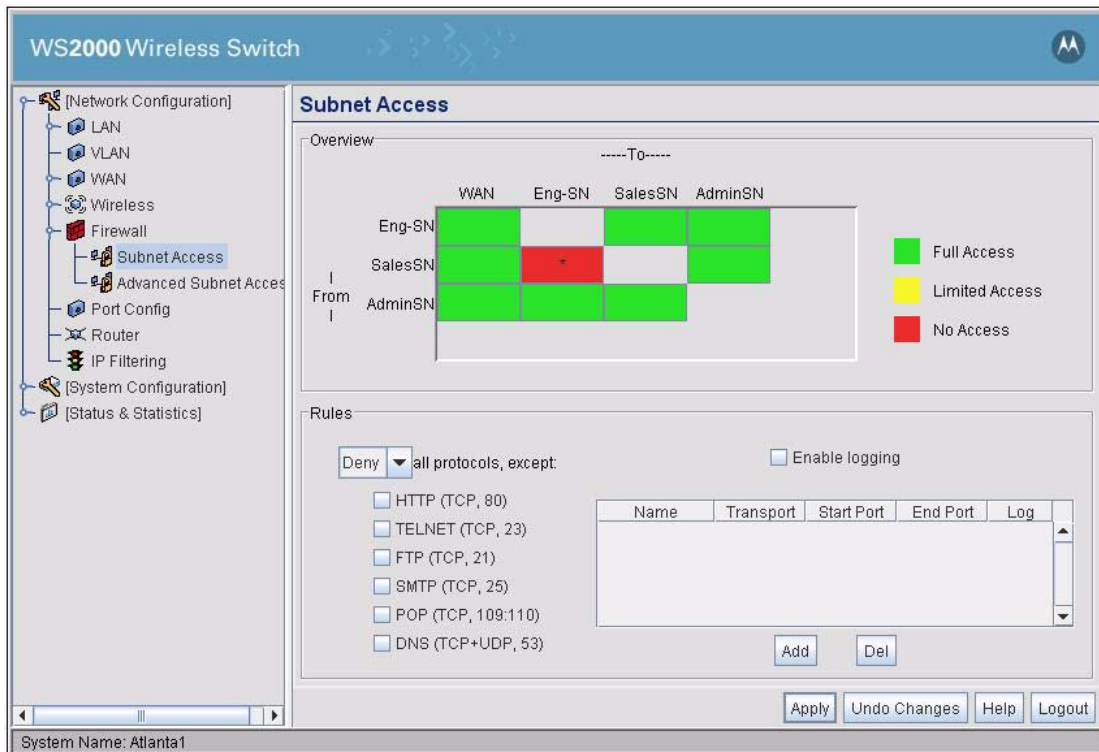
Buttons at the bottom right include Apply, Undo Changes, Help, and Logout. The system name is Atlanta1.

The subnet access defaults every subnet having access to every other subnet and full access to the WAN. Leo wants to restrict subnet access so that marketing has no access to the engineering subnet and no access to the administration subnet. He would also like to restrict all of the subnets to HTTP, SMTP, and POP access to the WAN.

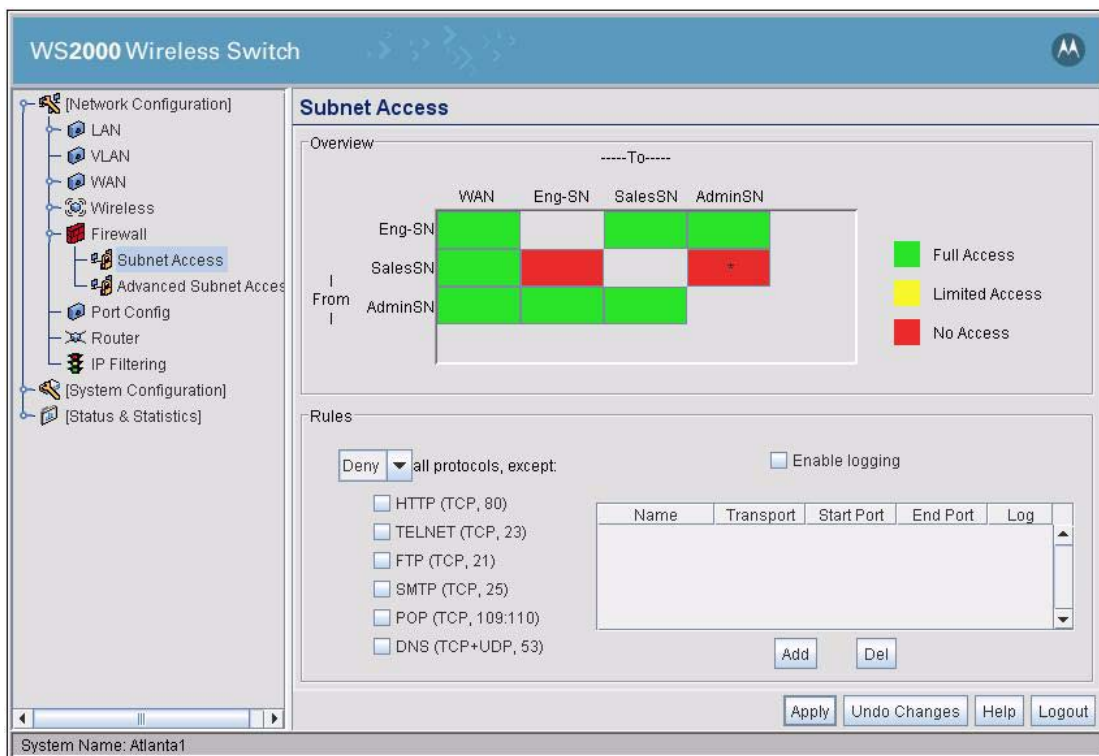
First Leo will restrict access from the marketing subnet to the other subnets. He selects the cell in the matrix defined by **From SalesSN** on the left and by **To Eng-SN** above. Then, in the Rules section, he pulls down the menu to the left of all protocols and selects **Deny**. This will block all traffic originating in the marketing subnet and going to the engineering subnet except the named protocols. No protocols were selected, so no traffic will be allowed.

Leo clicks on the **Apply** button to record this subnet access configuration.

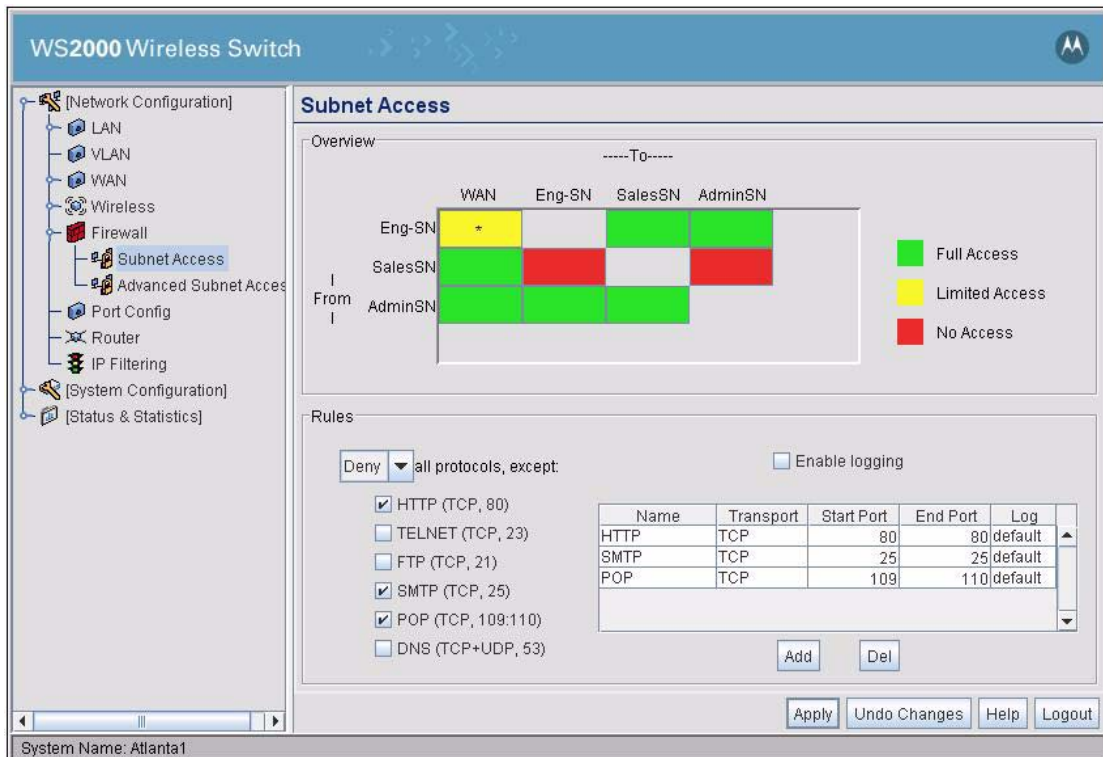




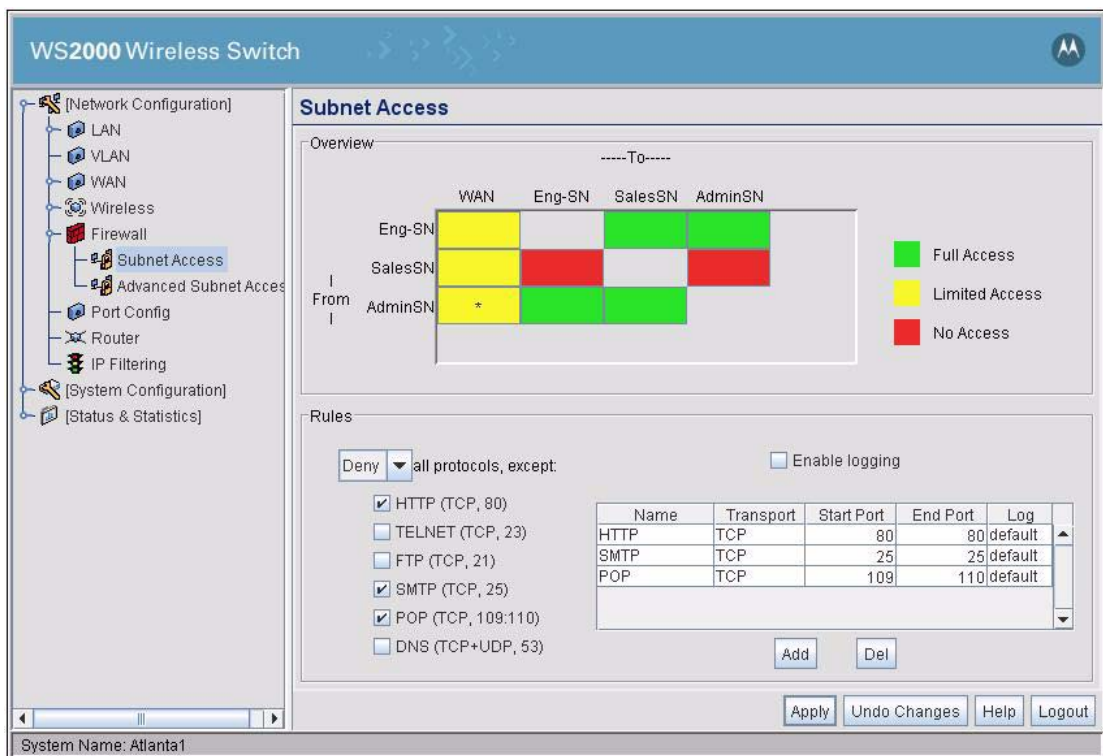
Similarly, Leo restricts access from the marketing subnet to the administration subnet.



Leo would also like to restrict traffic from all subnets to the WAN to just HTTP, SMTP, and POP protocols. He selects the cell in the matrix defined by **From Eng-SN** on the left and **To WAN** above. Then he uses the Rules pull down menu to select **Deny** and specifies that HTTP, SMTP and POP are the exceptions.



Similarly, he restricts the marketing and administration subnets in their access to the WAN.



Leo clicks the **Apply** button to record his changes. The subnet access is configured.

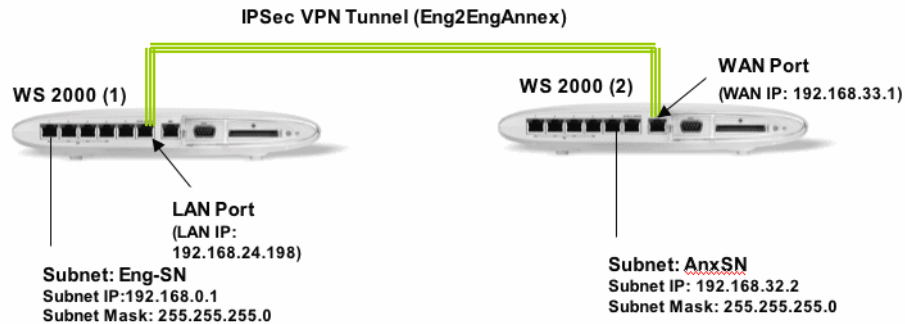
Now Leo needs to set up VPN access to the Engineering Annex and test the installation.

## 12.27 Configuring the VPN

To configure a VPN link between WS2000s, the following must be specified:

- The subnets on each end of the VPN link (tunnel)
- The authentication method for allowing a connection
- The encryption method for the content passed across the link

Both WS2000s must be set up with complimentary information on each other.



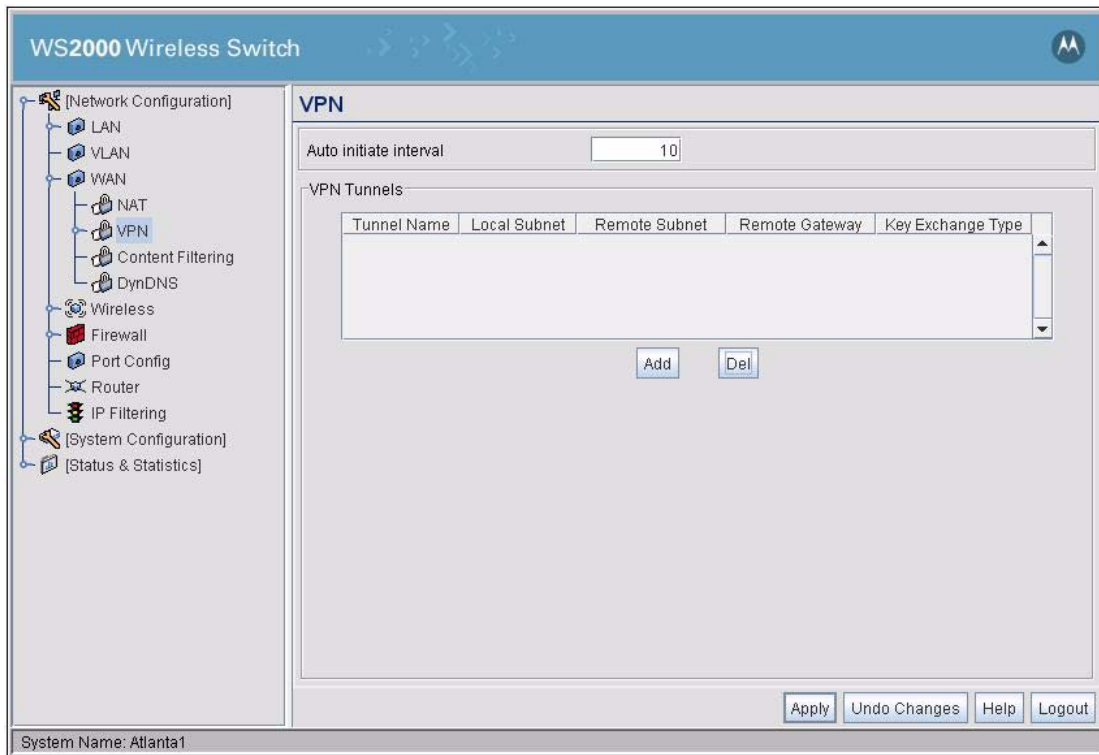
### VPN Tunnel Configuration Settings for WS 2000 (1):

- Tunnel Name: Eng2EngAnnex
- Local Subnet: Eng-SN
- Local LAN IP: 192.168.24.198
- Remote Subnet: 192.168.32.2 [For subnet defined on WS 2000 (2)]
- Remote Subnet Mask: 255.255.255.0
- Remote Gateway: 192.168.33.1 [WAN IP of WS 2000 (2)]

### VPN Tunnel Configuration Settings for WS 2000 (2):

- Tunnel Name: Eng2EngAnx
- Local Subnet: Anx-SN
- Local WAN IP: 192.168.33.1
- Remote Subnet: 192.168.0.1 [For Eng-SN on WS 2000 (1)]
- Remote Subnet Mask: 255.255.255.0
- Remote Gateway: 192.168.24.198 [LAN Port of WS 2000 (1)]
- Default Gateway: 192.168.24.198 [Set in WAN config of WS 2000 (1)]

Leo toggles open the **WAN** item in the left menu and selects **VPN**. Each VPN link between one subnet and another is called a *tunnel*.



Leo clicks the **Add** button to add a VPN tunnel.

Now Leo specifies the network parameters for the tunnel. The **Tunnel Name** is simply a name by which to distinguish one tunnel from another. Leo names the tunnel "**Eng2EngAnnex.**"

The **Local Subnet** is the subnet that will be networked over the VPN, in this case, the Engineering subnet. The **Local WAN IP** is the IP address for the interface that this WS2000 will show to the WS2000 on the other side of the VPN. Leo enters an unused, internal IP address, 192.168.24.198.

**WS2000 Wireless Switch**

**VPN**

Auto initiate interval: 10

VPN Tunnels

Tunnel Name	Local Subnet	Remote Subnet	Remote Gateway	Key Exchange Type
Eng2EngAnnex	Eng-SN	206.235.208.198	206.235.208.100	Manual

Add Del

VPN Tunnel Config

Tunnel Name: Eng2EngAnnex Default Gateway: 157.235.208.246

Local Subnet: Eng-SN  Manual Key Exchange

Local Wan IP: 192.168.24.198  Auto (IKE) Key Exchange

Remote Subnet: 206.235.208.198

Remote Subnet Mask: 255.255.255.0

Remote Gateway: 206.235.208.100

Manual Key Settings

Auto Key Settings

IKE Settings

Apply Undo Changes Help Logout

System Name: Atlanta1

The **Remote Subnet** specifies the subnet, on the other WS2000, to which the engineering subnet will be connected. The **Remote Gateway** and the **Remote Subnet Mask** describe the network interface on the other WS2000 switch. After Leo fills in these parameters, he clicks **Apply** to record the changes.

Now Leo needs to specify the authentication and encryption methods for the VPN link. He selects the simplest alternative, **Manual Key Settings**, since the link is so short and relatively unexposed.

The **AH Authentication protocol** is used between the two WS2000 switches to authorize initialization of the VPN tunnel. The AH authentication method must match on both switches and the inbound key on one WS2000 must match the outbound key on the other. Leo selects **Secure Hash Algorithm 1** or **SHA1** as the method and enters inbound and outbound 40 character authentication keys.

The **inbound Security Parameter Index (SPI)** for this WS2000 must match the outbound SPI from the other switch and vice versa. Leo enters 100 for the Inbound SPI and 101 for the Outbound SPI.

The **Encapsulating Security Payload** or **ESP** is specified in the lower section. This specifies how the network packets will be encrypted between the two ends of the VPN tunnel. Leo chooses **DES encryption** and specifies the **Inbound ESP Encryption Key** so that it will match the Outbound ESP Encryption Key on the other WS2000. He also specifies the **Outbound ESP Encryption Key** on this WS2000 so that it will match the Inbound ESP Encryption Key on the other switch.

Finally, the **Inbound** and **Outbound SPI** fields in the encryption section on this WS2000 must match the Outbound and Inbound SPIs on the other WS2000. Leo enters 110 for the Inbound SPI and 111 for the Outbound SPI.

Leo clicks **Ok** to record the Manual Key Settings. Then he clicks the **Apply** button to confirm this configuration.

The switch is now configured!

## 12.28 Installing the Access Ports and Testing

The switch is now configured. Leo connects the switch's WAN port to the VPN appliance that goes to the outside world. He gets three laptops and sets each of them to use DHCP for IP address assignment, 802.1x EAP for user authentication, and WPA-TKIP for data encryption over the wireless link. He uses the first laptop to connect to the engineering WLAN, the second to connect to the sales and marketing WLAN, and the third

laptop to connect to the administration WLAN. He makes sure that laptops on each WLAN can connect to the WAN and to each other.

After he has tested the three subnets, he installs the Access Ports in their permanent locations. He test coverage with the laptops, making sure each Access Port is covering its assigned area. He also unplugs each of the engineering Access Ports, in turn, to be sure that both are working properly. When everything seems to be working, he sends an email to the users telling them that the new wireless network is up and running!





# A

## ***Syslog Messages***

A.1 Informational Log Entries .....	A-2
A.2 Notice Log Entries.....	A-4
A.3 Warning Log Entries .....	A-6
A.4 Alert Log Entry .....	A-9
A.5 Error-Level Log Entries .....	A-9
A.6 Debug-Level Log Entries.....	A-23
A.7 Emergency Log Entries .....	A-27

## A.1 Informational Log Entries

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>802.1X Module</b>	LOG_INFO	8021x: 802.1x Authentication success for MU [MAC_ADDR]
<b>802.1X Module</b>	LOG_INFO	Tried max eap-id requests for MU [MAC_ADDR].
<b>Address Lookup Table Module</b>	LOG_INFO	CFG portal exists called with null mac
<b>Cell Controller Module</b>	LOG_INFO	Caught Signal [Number] ignoring it sig
<b>Cell Controller Module</b>	LOG_INFO	ccmain:no free ccb for tx
<b>Cell Controller Module</b>	LOG_INFO	mu remove ioctl failed
<b>Cell Controller Module</b>	LOG_INFO	portal remove ioctl failed
<b>Cell Controller Module</b>	LOG_INFO	Starting
<b>EAP Module</b>	LOG_INFO	Out of turn eap id ([Number]). expected ([Number]). Ignoring
<b>EAP Module</b>	LOG_INFO	rcvd eap-logout from [MAC_ADDR] usmu->mu->addr
<b>EAP Module</b>	LOG_INFO	rcvd eap-notif from supplicant [MAC_ADDR] usmu->mu->addr
<b>EAP Module</b>	LOG_INFO	rcvd eap-start from [MAC_ADDR] usmu->mu->addr
<b>Kerberos Proxy Module</b>	LOG_INFO	kerberos preauth required by KDC [IP_ADDR] from_ip
<b>Kerberos Proxy Module</b>	LOG_INFO	krb5: sending ap_rep (fail) to MU [MAC_ADDR] mu_ptr->addr
<b>MU Association Module</b>	LOG_INFO	Inactivity timer expired for MU [MAC_ADDR] mu_ptr->addr
<b>MU Association Module</b>	LOG_INFO	MU [MAC_ADDR] Associated to [MAC_ADDR] mu_ptr->addr mu_ptr->bss_addr
<b>MU Association Module</b>	LOG_INFO	MU [MAC_ADDR] DisAssociated from [MAC_ADDR]
<b>MU Association Module</b>	LOG_INFO	mu [MAC_ADDR] is a voice mu mu_ptr->addr
<b>MU Association Module</b>	LOG_INFO	mu [MAC_ADDR] needs proxy arp mu_ptr->addr
<b>MU Association Module</b>	LOG_INFO	MU lock period expired. Removing MU [MAC_ADDR]
<b>MU Association Module</b>	LOG_INFO	no ccbs to tx disassoc to mu [MAC_ADDR] from [MAC_ADDR]
<b>MU Association Module</b>	LOG_INFO	No CCBS. MU [MAC_ADDR] DeAuthenticated from [MAC_ADDR]
<b>MU Association Module</b>	LOG_INFO	No RFP. MU [MAC_ADDR] DeAuthenticated from [MAC_ADDR]
<b>MU Association Module</b>	LOG_INFO	Removing MU [MAC_ADDR]mu_ptr->addr
<b>MU Association Module</b>	LOG_INFO	Scheduling MU [MAC_ADDR] for deletion from [MAC_ADDR] mu_ptr->addr mu_ptr->bss_addr
<b>MU Association Module</b>	LOG_INFO	tx disassoc to mu [MAC_ADDR] on bss [MAC_ADDR] mu_addr bss_addr
<b>NTP Client Module</b>	LOG_INFO	local clock is synchronized with ntp server
<b>NTP Client Module</b>	LOG_INFO	ntp: system clock updated to [%s]

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>Encryption Key Exchange Module</b>	LOG_INFO	[Pairwise Transient Key] Unable to get free CC buffer
<b>Encryption Key Exchange Module</b>	LOG_INFO	[Pairwise Transient Key] Group rekey after %u seconds gk_timeout
<b>RADIUS Module</b>	LOG_INFO	rcvd access-accept from [IP_ADDR] for [MAC_ADDR]
<b>RADIUS Module</b>	LOG_INFO	rcvd access-reject from [IP_ADDR] for [MAC_ADDR]
<b>RF Port Module</b>	LOG_INFO	Radio [MAC_ADDR] acs done ch=[Number]
<b>RF Port Module</b>	LOG_INFO	Radio [MAC_ADDR] acs in progress addr
<b>RF Port Module</b>	LOG_INFO	Radio [MAC_ADDR] adopted addr
<b>RF Port Module</b>	LOG_INFO	Radio [MAC_ADDR] inactive prt_ptr->addr
<b>RF Port Module</b>	LOG_INFO	Radio [MAC_ADDR] removed prt_ptr->addr
<b>RF Port Module</b>	LOG_INFO	Radio [MAC_ADDR]:non-acs status has no channel
<b>RF Port Module</b>	LOG_INFO	RF Port [MAC_ADDR] removed rfp_ptr->addr
<b>Rogue AP Detection Module</b>	LOG_INFO	Number of known APs: %u count
<b>Statistics Module</b>	LOG_INFO	Resetting
<b>VLAN Module</b>	LOG_INFO	Mapped port [Number] to subnet [Number]
<b>VLAN Module</b>	LOG_INFO	Mapped wlan [Number] to subnet [Number]
<b>VLAN Module</b>	LOG_INFO	Port [Number] has no subnet mapping port_idx
<b>VLAN Module</b>	LOG_INFO	Subnet [Number] disabled subnet_idx
<b>VLAN Module</b>	LOG_INFO	Subnet [Number] enabled subnet_idx
<b>VLAN Module</b>	LOG_INFO	Wlan [Number] has no subnet mapping wlan_idx
<b>SIP Module</b>	LOG_INFO	SIP:Max number of SIP sessions reached on portal [address]
<b>SIP Module</b>	LOG_INFO	"SIP:Create a new SIP session for call id [identifier], set state to initiated"
<b>SIP Module</b>	LOG_INFO	SIP:Decrementing the number of Active SIP sessions of portal [address] to [number]
<b>SIP Module</b>	LOG_INFO	SIP:Incrementing the number of Active SIP sessions of portal [address] to [number]
<b>WIPS module</b>	LOG_INFO	WIPS is disabled
<b>WIPS module</b>	LOG_INFO	WIPS: Detection in progress
<b>WIPS module</b>	LOG_INFO	Could not send configuration to [MAC] Sensor was not found
<b>WIPS module</b>	LOG_INFO	WIPS: Max number of sensors detected. Not adding any more
<b>WIPS module</b>	LOG_INFO	AP [MAC] is converted to sensor
<b>WIPS module</b>	LOG_INFO	Sensor [MAC] is successfully reverted

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>WIPS module</b>	LOG_INFO	"Sensor [MAC] is no longer responding, removed"
<b>WIPS module</b>	LOG_INFO	Sensor [MAC] timed out waiting for [command]
<b>AP Revert</b>	LOG_INFO	AP [MAC] Reverting to AP4131
<b>AP Revert</b>	LOG_INFO	AP [MAC] Reverting to AP4121
<b>AP Revert</b>	LOG_INFO	old rf image = [name] new rf image = [name] load_now = [truth value]
<b>Port Configuration</b>	LOG_INFO	Port config changed for port idx = [idx]
<b>Port Configuration</b>	LOG_INFO	Port config changed for Wan: port idx = [idx]
<b>Default Gateway</b>	LOG_INFO	Subnet [idx]: DHCP Client is already running
<b>Default Gateway</b>	LOG_INFO	Subnet [idx]: Stopping DHCP Client
<b>Default Gateway</b>	LOG_INFO	Adding the DGW as Subnet [idx]
<b>CF Format</b>	LOG_INFO	CF card Formatted

## A.2 Notice Log Entries

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>802.1X Module</b>	LOG_NOTICE	8021x: final timeout on server [IP_ADDR]. old_ip
<b>802.1X Module</b>	LOG_NOTICE	8021x: Starting WPA/TKIP keying for MU [MAC_ADDR]
<b>802.1X Module</b>	LOG_NOTICE	8021x: WEP keys sent. Starting Keyguard
<b>802.1X Module</b>	LOG_NOTICE	8021x: WEP[Number] keys transmitted to MU [MAC_ADDR]
<b>EAP Module</b>	LOG_NOTICE	EAP code [Number] != EAP_RESPONSE from MU [MAC_ADDR]. Ignoring
<b>EAP Module</b>	LOG_NOTICE	invalid eapol length [Number] from [MAC_ADDR]. ignoring
<b>EAP Module</b>	LOG_NOTICE	invalid eapol version [Number] from [MAC_ADDR].
<b>EAP Module</b>	LOG_NOTICE	invalid etherType 0x%04X) from [MAC_ADDR].
<b>Kerberos Client Module</b>	LOG_NOTICE	krb: ess [%s] authenticated with kdc [IP_ADDR]
<b>Kerberos Proxy Module</b>	LOG_NOTICE	krb: mu [MAC_ADDR] ticket expired. deauthenticating
<b>Kerberos Proxy Module</b>	LOG_NOTICE	krb5: MU [MAC_ADDR] authenticated. Ticket valid for %02u:%02u:%02u hh:mm:ss)
<b>Encryption Key Exchange Module</b>	LOG_NOTICE	[Pairwise Transient Key] Bad ack bit %x %x [MAC_ADDR] *U08 *) &eap_pkt->skd.info_h
<b>Encryption Key Exchange Module</b>	LOG_NOTICE	[Pairwise Transient Key] Bad key type [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_NOTICE	[Pairwise Transient Key] Bad replay ctr [MAC_ADDR] Rcvd %x %x Expected %x %x\n

<b><i>System Component</i></b>	<b><i>Debug Level</i></b>	<b><i>Log Message</i></b>
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] Bad version [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] Funny pkt!! [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] IE no match [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] Ignore packet [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] Ignore packet [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] Ignore packet [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] MIC Error [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] MIC Error [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	[Pairwise Transient Key] req bit set [MAC_ADDR] mu->addr
<b><i>Encryption Key Exchange Module</i></b>	LOG_NOTICE	SSN IE too big - [Number] bytes [MAC_ADDR] eap_pkt->skd.mlen mu->addr

## A.3 Warning Log Entries

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>802.1X Module</b>	LOG_WARNING	8021x: MU [MAC_ADDR] in unknown PAE state [[Number]].
<b>802.1X Module</b>	LOG_WARNING	8021x: no rsp from server [IP_ADDR] count: [Number]
<b>802.1X Module</b>	LOG_WARNING	8021x:Using backup server [IP_ADDR]
<b>802.1X Module</b>	LOG_WARNING	Unable to send EAPOL keys. MPPE keys
<b>802.1X Module</b>	LOG_WARNING	Unable to send EAPOL keys. MPPE keys
<b>802.1X Module</b>	LOG_WARNING	WPA/TKIP keying failure. MPPE keys not
<b>Address Lookup Table Module</b>	LOG_WARNING	altable initialize
<b>EAP Module</b>	LOG_WARNING	eapol length [Number] from [MAC_ADDR] is invalid
<b>EAP Module</b>	LOG_WARNING	ignoring eap frame from MU [MAC_ADDR].
<b>EAP Module</b>	LOG_WARNING	Username in eap-id-rsp from [MAC_ADDR] too long [Number] bytes)
<b>Kerberos Client Module</b>	LOG_WARNING	kerberos services waiting for
<b>Kerberos Client Module</b>	LOG_WARNING	krb: authentication failure from KDC [IP_ADDR] from_ip
<b>Kerberos Client Module</b>	LOG_WARNING	krb: error [Number] in krb5_process_padata) retval
<b>Kerberos Client Module</b>	LOG_WARNING	krb: error [Number] reported by decode_krb5_as_rep) retval
<b>Kerberos Client Module</b>	LOG_WARNING	krb: kerberos error code: [Number] err_reply->error
<b>Kerberos Client Module</b>	LOG_WARNING	krb: principal not known on kdc
<b>Kerberos Client Module</b>	LOG_WARNING	krb: rcvd krb_error from [IP_ADDR] from_ip
<b>Kerberos Proxy Module</b>	LOG_WARNING	Bad Encryption Type from KDC. Check that the
<b>Kerberos Proxy Module</b>	LOG_WARNING	Client name not known to KDC. MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_WARNING	Clock skew reported by KDC for MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_WARNING	KDC reported ecode %u for MU [MAC_ADDR] ecode mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: Client name for MU [MAC_ADDR] not known on KDC
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: clock skew reported for MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: error code = [Number]) in decode_krb_error
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: error [Number] in decode_krb5_ap_req) retval
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: Error [Number] in encode_krb5_ap_rep)
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: Error [Number] in encode_krb5_ap_rep_enc_part)
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: error [Number] in encode_krb5_error) retval
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: Error [Number] in krb5_encrypt_helper)

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: error [Number] in krb5_rd_req_decoded) retval
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: key generation failure!
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: Server name for MU [MAC_ADDR] not known to KDC
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: switch auth not done. ignoring
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: switch auth not done. Ignoring ap_req
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: switch auth not done. Ignoring as_req from
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: switch auth not done. Ignoring sk_req
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: Ticket from MU [MAC_ADDR] already expired.
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: Ticket from MU [MAC_ADDR] not yet valid.
<b>Kerberos Proxy Module</b>	LOG_WARNING	krb5: unknown WNMP msg [Number]) from MU [MAC_ADDR]
<b>Kerberos Proxy Module</b>	LOG_WARNING	Server name not known to KDC. MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_WARNING	Ticket for AP has expired. MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_WARNING	Ticket for AP not yet valid. MU [MAC_ADDR] mu_ptr->addr
<b>MU Association Module</b>	LOG_WARNING	\nUnrecognized subtype %04x ignored sub_type
<b>MU Association Module</b>	LOG_WARNING	Assoc denied to MU [MAC_ADDR]. Capability [Number]) not supp
<b>MU Association Module</b>	LOG_WARNING	Bad SSID from MU [MAC_ADDR]
<b>MU Association Module</b>	LOG_WARNING	Bad Tx_Rates [Number]) for MU [MAC_ADDR]
<b>MU Association Module</b>	LOG_WARNING	Incorrect Seq Num [Number]) in Auth_Req from [MAC_ADDR]\n
<b>MU Association Module</b>	LOG_WARNING	Invalid WPA elem from MU [MAC_ADDR] Rejecting Assoc_Req.
<b>MU Association Module</b>	LOG_WARNING	Max MU capacity reached. Denying Auth to [MAC_ADDR]
<b>MU Association Module</b>	LOG_WARNING	mu [MAC_ADDR] not in acl mu_ptr->addr
<b>MU Association Module</b>	LOG_WARNING	No WPA elem from MU [MAC_ADDR] Rejecting Assoc_Req.
<b>MU Association Module</b>	LOG_WARNING	rx assoc for unknown mu [MAC_ADDR] pkt_ptr->src
<b>MU Association Module</b>	LOG_WARNING	SSID too long [Number]) from MU [MAC_ADDR]
<b>MU Association Module</b>	LOG_WARNING	Unsupported auth algorithm [Number]) from MU [MAC_ADDR]
<b>NTP Client Module</b>	LOG_WARNING	ntp: mode in ntp resp[Number]) != server
<b>NTP Client Module</b>	LOG_WARNING	ntp:li-field in ntp header indicates server is not synced
<b>NTP Client Module</b>	LOG_WARNING	rcvd ntp rsp from unknown server [IP_ADDR]. Ignoring
<b>RF Port Configuration Module</b>	LOG_WARNING	portal [MAC_ADDR] bad radio type [Number]
<b>RF Port Configuration Module</b>	LOG_WARNING	portal [MAC_ADDR] bad radio type [Number]
<b>RF Port Configuration Module</b>	LOG_WARNING	Portal [MAC_ADDR] can't be defaulted prt1_ptr->addr

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>RF Port Configuration Module</b>	LOG_WARNING	Portal [MAC_ADDR] denied adoption in acl prtl_ptr->addr
<b>RF Port Configuration Module</b>	LOG_WARNING	portal [MAC_ADDR] found at idx [Number]
<b>RF Port Configuration Module</b>	LOG_WARNING	portal [MAC_ADDR] not connected & not in acl
<b>RF Port Configuration Module</b>	LOG_WARNING	portal [MAC_ADDR] not found using idx [Number]
<b>RF Port Configuration Module</b>	LOG_WARNING	Portal [MAC_ADDR] replaced by [MAC_ADDR] in slot [Number]
<b>RF Port Configuration Module</b>	LOG_WARNING	Portal [MAC_ADDR]:no country code
<b>RADIUS Module</b>	LOG_WARNING	Radius ID mismatch in rsp from [IP_ADDR]. Ignoring from_ip
<b>RADIUS Module</b>	LOG_WARNING	Radius validation failed for rsp from [IP_ADDR] for [MAC_ADDR]
<b>RADIUS Module</b>	LOG_WARNING	rcvd unexpected rsp from [IP_ADDR] from_ip
<b>RADIUS Module</b>	LOG_WARNING	Unable to read System Name from configuration
<b>RADIUS Module</b>	LOG_WARNING	unexpected Type [[Number]] in rsp from [IP_ADDR] Ignoring!
<b>SecurityPolicy.cpp</b>	LOG_WARNING	Error reading configuration. Not starting Kerberos
<b>Statistics Module</b>	LOG_WARNING	unable to read location for portal [Number] p_idx
<b>Statistics Module</b>	LOG_WARNING	unable to read name for portal [Number] p_idx
<b>Statistics Module</b>	LOG_WARNING	unable to read tx_power for portal [Number] p_idx
<b>Statistics Module</b>	LOG_WARNING	unable to read wlan_map for portal [Number] p_idx



## A.4 Alert Log Entry

<i>System Component</i>	<i>Debug Level</i>	<i>Log Message</i>
<b><i>NTP Client Module</i></b>	LOG_ALERT	errno [Number] updating system clock to ntp time errno

## A.5 Error-Level Log Entries

<i>System Component</i>	<i>Debug Level</i>	<i>Log Message</i>
<b><i>802.1X Module</i></b>	LOG_ERR	Config error! EAP enabled but no valid
<b><i>Access Control List Module</i></b>	LOG_ERR	ACL adopt all read failed
<b><i>Access Control List Module</i></b>	LOG_ERR	ACL adopt all read failed
<b><i>Access Control List Module</i></b>	LOG_ERR	ACL entry count read failed
<b><i>Access Control List Module</i></b>	LOG_ERR	ACL entry count read failed
<b><i>Access Control List Module</i></b>	LOG_ERR	ACL read from cough failed
<b><i>Access Control List Module</i></b>	LOG_ERR	ACL read from cfg failed
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	ACL cannot read radio [Number] cfg mac radio_idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	ACL cannot write radio [Number] cfg mac cfg_list_idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	ACL cannot write radio [Number] cfg mac cfg_list_idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	ACL cannot write radio [Number] cfg status cfg_list_idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	ACL radio [Number] adopt write fail cfg_list_idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	ACL radio [Number] de-adopt write fail cfg_list_idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: cannot read cfg wlan mode
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: cannot read cfg wlan mode
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't get beacon interval
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't get bss primary ess
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't get bss primary ess
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't get bss primary ess
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't get dtim period
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't read cfg bss radio idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't read cfg bss radio idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't read cfg bss radio idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't read cfg bss radio idx
<b><i>Address Lookup Table Module</i></b>	LOG_ERR	altable: can't read cfg bss radio idx

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>Address Lookup Table Module</b>	LOG_ERR	altable: can't read cfg bss radio idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable: can't set bss mac
<b>Address Lookup Table Module</b>	LOG_ERR	altable: can't set bss radio idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable: can't set bss radio idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable: rates configured incorrectly
<b>Address Lookup Table Module</b>	LOG_ERR	altable: unable to read cfg basic rates
<b>Address Lookup Table Module</b>	LOG_ERR	altable: unable to read cfg supported rates
<b>Address Lookup Table Module</b>	LOG_ERR	altable: unknown radio type in rate cfg
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read [Number] indoor setting list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read cfg country code
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read cfg country code
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read cfg ess
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read cfg mu-mu disallow
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read cfg wlan mode
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read mcast addr1
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read mcast addr2
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read radio [Number] channel cfg_list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read radio [Number] diversity cfg_list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read radio [Number] power cfg_list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot read reg [Number] indoor setting list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable:cannot set radio [Number] channel cfg_list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	altable:country code is null in cfg
<b>Address Lookup Table Module</b>	LOG_ERR	altable:radio [Number] conn status is [Number] cfg_list_idx status
<b>Address Lookup Table Module</b>	LOG_ERR	cfg cannot read radio [Number] cfg mac radio_idx
<b>Address Lookup Table Module</b>	LOG_ERR	cfg cannot read radio [Number] cfg mac radio_idx
<b>Address Lookup Table Module</b>	LOG_ERR	cfg cannot write radio [Number] cfg type cfg_list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	cfg cannot write radio [Number] cfg type cfg_list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	cfg default failed:index [Number] radio type [Number]\n
<b>Address Lookup Table Module</b>	LOG_ERR	cfg of radio [Number] invalid: bad rgltry info list_idx
<b>Address Lookup Table Module</b>	LOG_ERR	cfg radio type [Number] not allowed rtype

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>Address Lookup Table Module</b>	LOG_ERR	cfg radio type [Number] not allowed rtype
<b>Address Lookup Table Module</b>	LOG_ERR	rfport list is full
<b>Address Lookup Table Module</b>	LOG_ERR	wlan [Number]: addr1 = [MAC_ADDR] addr2 = [MAC_ADDR] wlan_idx
<b>Cell Controller Module</b>	LOG_ERR	Error [Number] initing sig handlers errno
<b>Cell Controller Module</b>	LOG_ERR	Error [Number] initing stats.cpp errno
<b>Cell Controller Module</b>	LOG_ERR	no shmем!!
<b>Cell Controller Utility Module</b>	LOG_ERR	Get_Mem: errno [Number] opening %s errno str
<b>Cell Controller Utility Module</b>	LOG_ERR	Get_Mem: errno [Number] reading file %s errno str
<b>Cell Controller Utility Module</b>	LOG_ERR	Get_Mem: error parsing file %s str
<b>EAP Module</b>	LOG_ERR	Unable to read ESS from config
<b>EAP Module</b>	LOG_ERR	Unable to read Sys-Name from config
<b>Kerberos Client Module</b>	LOG_ERR	krb: error [Number] in decrypt_as_reply) retval
<b>Kerberos Client Module</b>	LOG_ERR	krb: error [Number] in stash_as_reply) retval
<b>Kerberos Client Module</b>	LOG_ERR	krb: error [Number] in verify_as_reply) retval
<b>Kerberos Client Module</b>	LOG_ERR	krb: error [Number] reported by decode_krb5_error) retval
<b>Kerberos Client Module</b>	LOG_ERR	krb: error [Number] reported by encode_krb5_as_req) retval
<b>Kerberos Client Module</b>	LOG_ERR	krb: error [Number] reported by krb5_obtain_padata) retval
<b>Kerberos Client Module</b>	LOG_ERR	krb: socket bind error. errno [Number] errno
<b>Kerberos Client Module</b>	LOG_ERR	krb: socket creation error. errno [Number] errno
<b>Kerberos Client Module</b>	LOG_ERR	krb: socket recv error. fd [Number]. errno [Number] fd errno
<b>Kerberos Client Module</b>	LOG_ERR	krb: socket send error on fd [Number]. errno [Number] kdc_fd errno
<b>Kerberos Client Module</b>	LOG_ERR	krb5: error [Number] reported by
<b>Kerberos Proxy Module</b>	LOG_ERR	krb5: socket rcv error. errno=[Number] errno
<b>Kerberos Proxy Module</b>	LOG_ERR	krb5: socket send error. errno=[Number] errno
<b>Kerberos Proxy Module</b>	LOG_ERR	krb5: socket send error. errno=[Number] errno
<b>Kerberos Proxy Module</b>	LOG_ERR	Socket bind error. errno: [Number] errno
<b>Kerberos Proxy Module</b>	LOG_ERR	Socket creation error. errno: [Number] errno
<b>NTP Client Module</b>	LOG_ERR	ntp enabled but no valid IP address configured
<b>NTP Client Module</b>	LOG_ERR	ntp rsp [Number] bytes) from [IP_ADDR] is too small
<b>NTP Client Module</b>	LOG_ERR	ntp:error reading configuration

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>NTP Client Module</b>	LOG_ERR	ntp:socket bind error. errno=[Number] errno
<b>NTP Client Module</b>	LOG_ERR	ntp:socket create error. errno=[Number] errno
<b>NTP Client Module</b>	LOG_ERR	ntp:socket recv error. errno=[Number] errno
<b>NTP Client Module</b>	LOG_ERR	ntp:socket send error. errno=[Number] errno
<b>portalcfg.cpp</b>	LOG_ERR	rfport:error:ess cannot map to multiple bss
<b>RADIUS Module</b>	LOG_ERR	eap code [Number]) != EAP-RSP for [MAC_ADDR]. Ignoring\n
<b>RADIUS Module</b>	LOG_ERR	errno [Number] reading Radius rsp errno
<b>RADIUS Module</b>	LOG_ERR	errno [Number] sending radius request to [IP_ADDR]:[Number].
<b>RADIUS Module</b>	LOG_ERR	Invalid MPPE key size [Number] bytes) ptext[0]
<b>RADIUS Module</b>	LOG_ERR	MPPE Key decrypt failed. Server: [IP_ADDR]
<b>RADIUS Module</b>	LOG_ERR	MPPE key rcvd is too big [(Number) bytes] len
<b>RADIUS Module</b>	LOG_ERR	Msg-Auth check failed for rsp from [IP_ADDR]
<b>RADIUS Module</b>	LOG_ERR	Over [Number] attributes in rsp from [IP_ADDR] Dropping!
<b>RF Port Image Module</b>	LOG_ERR	bad size %ld of RFP Image img_ptr->len
<b>RF Port Image Module</b>	LOG_ERR	bad header len in RFP Image
<b>RF Port Image Module</b>	LOG_ERR	bad magic value in RFP Image
<b>RF Port Image Module</b>	LOG_ERR	can't allocate %ld bytes img_ptr->len + RFP_IMG_CHECKSUM_SIZE
<b>RF Port Image Module</b>	LOG_ERR	Can't allocate image %s img_ptr->img_name
<b>RF Port Image Module</b>	LOG_ERR	can't find eof in RFP Image
<b>RF Port Image Module</b>	LOG_ERR	can't read RFP Image file
<b>RF Port Image Module</b>	LOG_ERR	can't reset stream offset for %s img_ptr->img_name
<b>RF Port Image Module</b>	LOG_ERR	Image header check failed %s img_ptr->img_name
<b>RF Port Module</b>	LOG_ERR	bad cfg seq for [MAC_ADDR]. expected [Number] got [Number].
<b>RF Port Module</b>	LOG_ERR	Cfg rejected by [MAC_ADDR] err=[Number] addr cfg_err
<b>RF Port Module</b>	LOG_ERR	error:[MAC_ADDR] is doing unconfigured acs addr
<b>RF Port Module</b>	LOG_ERR	old status for [MAC_ADDR]. expected [Number] got [Number].
<b>RF Port Module</b>	LOG_ERR	status wait timeout for [MAC_ADDR] resending cfg addr
<b>Rogue AP Detection Module</b>	LOG_ERR	no ccb cannot send WNMP msg
<b>Rogue AP Detection Module</b>	LOG_ERR	Unable to read rogue-detection timeout from cfg
<b>Rogue AP Detection Module</b>	LOG_ERR	Unable to read watched_mac from cfg

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>Rogue AP Detection Module</b>	LOG_ERR	Unable to read watched_ssid from cfg
<b>Receive Packets Module</b>	LOG_ERR	rx data frame of unexpected ethernet
<b>Receive Packets Module</b>	LOG_ERR	rxpkts:bad ctl %04x from [[MAC_ADDR]] pkt_ptr->ctl pkt_ptr->src
<b>Receive Packets Module</b>	LOG_ERR	rxpkts:bad dest [[MAC_ADDR]] from [[MAC_ADDR]] pkt_ptr->src pkt_ptr->dest
<b>Statistics Module</b>	LOG_ERR	errno [Number] sending trap to SNMPD\n errno
<b>Statistics Module</b>	LOG_ERR	errno [Number] sending trap to SNMPD\n errno
<b>Statistics Module</b>	LOG_ERR	stats driver rcvd unexpected cmd: [Number]\n stats->cmd
<b>VLAN Module</b>	LOG_ERR	%s:cannot open %s __FILE__ SW_DEV_PATH_NAME
<b>VLAN Module</b>	LOG_ERR	Error: Port [Number] assigned to [Number] vlans
<b>VLAN Module</b>	LOG_ERR	Invalid subnet value [Number] in cfg
<b>VLAN Module</b>	LOG_ERR	Invalid subnet value [Number] in cfg
<b>Wireless Switch Protocol Module</b>	LOG_ERR	deleting prev rfport instance [MAC_ADDR] rx_wh->src
<b>Wireless Switch Protocol Module</b>	LOG_ERR	portal [[MAC_ADDR]][Number] not allowed in cfg prt_ptr->addr prt_ptr->state
<b>Wireless Switch Protocol Module</b>	LOG_ERR	resetting rf port [[MAC_ADDR]] rfp_ptr->addr
<b>Wireless Switch Protocol Module</b>	LOG_ERR	RF Port [MAC_ADDR] no free rfp rx_wh->src
<b>Wireless Switch Protocol Module</b>	LOG_ERR	RF Port [MAC_ADDR] no free rfp rx_wh->src
<b>Wireless Switch Protocol Module</b>	LOG_ERR	Rx device info from [MAC_ADDR] rx_wh->src
<b>Wireless Switch Protocol Module</b>	LOG_ERR	wisp:could not find rfport image
<b>RF Port Image Module</b>	LOG_ERR	can't open image file
<b>SIP Module</b>	LOG_ERR	Cannot create any more SIP sessions - max limit reached
<b>SIP Module</b>	LOG_ERR	SIP:Invite received with NULL call id
<b>SIP Module</b>	LOG_ERR	SIP:Cancel received with NULL call id
<b>SIP Module</b>	LOG_ERR	SIP:Cancel received for an invalid call id [ identifier ]
<b>SIP Module</b>	LOG_ERR	SIP:Ack received with NULL call id
<b>SIP Module</b>	LOG_ERR	SIP:Ack received for an invalid call id [identifier]
<b>SIP Module</b>	LOG_ERR	SIP:Bye received for an invalid call id [identifier]

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>SIP Module</b>	LOG_ERR	SIP:Bye received with NULL call id
<b>SIP Module</b>	LOG_ERR	SIP:Status message received with NULL status code
<b>SIP Module</b>	LOG_ERR	SIP:Status message received with NULL call id
<b>SIP Module</b>	LOG_ERR	SIP:Status message received for an invalid call id [identifier]
<b>SIP Module</b>	LOG_ERR	SIP:Status message received at invalid state for call id [identifier]
<b>SIP Module</b>	LOG_ERR	SIP:Status message received at invalid state for call id [identifier]
<b>SIP Module</b>	LOG_ERR	SIP:status message received with invalid error code [number]
<b>WIPS module</b>	LOG_ERR	Could not read WIPS state
<b>WIPS module</b>	LOG_ERR	Could not open socket
<b>WIPS module</b>	LOG_ERR	Could not bind to socket
<b>WIPS module</b>	LOG_ERR	Could not set socket options
<b>WIPS module</b>	LOG_ERR	Error in receiving command
<b>WIPS module</b>	LOG_ERR	Bad sensor command received
<b>WIPS module</b>	LOG_ERR	WIPS: Invalid AD command [command] received
<b>WIPS module</b>	LOG_ERR	Invalid AP MAC. Can not convert to sensor
<b>WIPS module</b>	LOG_ERR	Can not convert the non-existing AP300 [MAC] to sensor
<b>WIPS module</b>	LOG_ERR	Invalid AP MAC. Can not revert to AP
<b>WIPS module</b>	LOG_ERR	Could not revert. Sensor [MAC] was not found
<b>WIPS module</b>	LOG_ERR	Could not get free buffer
<b>WIPS module</b>	LOG_ERR	Invalid AP MAC. Can not send cfg to sensor
<b>WIPS module</b>	LOG_ERR	AD packet with invalid MAC is received
<b>WIPS module</b>	LOG_ERR	Ack from an unknown sensor
<b>WIPS module</b>	LOG_ERR	Could not remove sensor [MAC]
<b>WIPS module</b>	LOG_ERR	Config from an unknown sensor
<b>WIPS module</b>	LOG_ERR	Configuration with bad length is received from [MAC]
<b>WIPS module</b>	LOG_ERR	Unexpected config reply from [MAC]
<b>WIPS module</b>	LOG_ERR	Could not send back data
<b>WIPS module</b>	LOG_ERR	Error reading configuration
<b>WIPS module</b>	LOG_ERR	Could not find RF port [MAC]
<b>WIPS module</b>	LOG_ERR	Invalid AP MAC. Can not get sensor config

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>AP Revert</b>	LOG_ERR	RF Port [MAC] no free rfp
<b>Port Configuration</b>	LOG_ERR	Port Auto-neg Get failed for port [port idx]
<b>Port Configuration</b>	LOG_ERR	Port Speed Get failed for port [port idx]
<b>Port Configuration</b>	LOG_ERR	Port Duplex Get failed for port [port idx]
<b>Port Configuration</b>	LOG_ERR	ioctl Read failed for Lan Port [port idx]
<b>Port Configuration</b>	LOG_ERR	Read failed for Wan registers
<b>Port Configuration</b>	LOG_ERR	Write failed for Wan registers
<b>Port Configuration</b>	LOG_ERR	"GET ERR in port cfg, sw registers may not set for port = [idx]"
<b>Port Configuration</b>	LOG_ERR	"GET ERR in port cfg, sw registers may not set for wan."
<b>CF Format</b>	LOG_ERR	Could not format cf card
<b>CF Format</b>	LOG_ERR	Error in sending the CF format message
<b>CF Format</b>	LOG_ERR	Could not open cf format status file
<b>CF Format</b>	LOG_ERR	Could not lock cf format status file
<b>CF Format</b>	LOG_ERR	Could not read cf format status file
<b>CF Format</b>	LOG_ERR	Could not unlock cf format status file
<b>IP Filter Module</b>	LOG_ERR	Invalid Row returning -1
<b>IP Filter Module</b>	LOG_ERR	Error reading config id [config id value]
<b>IP Filter Module</b>	LOG_ERR	Error: Bad parameters passed
<b>IP Filter Module</b>	LOG_ERR	Error: Could not get total entries from WLAN_TRUNK Filter Table
<b>IP Filter Module</b>	LOG_ERR	Error: Could not get entries from WLAN_TRUNK Filter Table
<b>IP Filter Module</b>	LOG_ERR	Error: Invalid context
<b>IP Filter Module</b>	LOG_ERR	Error: Could not get total entries from Global IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Error: Could not get entries from Global IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Error: Config read error for WLAN default incoming deny
<b>IP Filter Module</b>	LOG_ERR	Error: Config read error for WLAN default outgoing deny
<b>IP Filter Module</b>	LOG_ERR	Error: Config read error for TRUNK default incoming deny
<b>IP Filter Module</b>	LOG_ERR	Error: Config read error for TRUNK default outgoing deny
<b>IP Filter Module</b>	LOG_ERR	Error: Config read error for WLAN IP Filter Mode
<b>IP Filter Module</b>	LOG_ERR	Error: Config read error for TRUNK IP Filter Mode
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get total entries from Global IP Filter Table

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get Global IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	[Function Name]: Invalid pointer passed
<b>IP Filter Module</b>	LOG_ERR	[Function Name]: Invalid pointer passed
<b>IP Filter Module</b>	LOG_ERR	[Function Name]: Invalid pointer passed
<b>IP Filter Module</b>	LOG_ERR	Invalid Length Passed for IP Filter table [length]
<b>IP Filter Module</b>	LOG_ERR	Error reading config id
<b>IP Filter Module</b>	LOG_ERR	Invalid Length Passed for WLAN Filter table [length]
<b>IP Filter Module</b>	LOG_ERR	[Function Name:]error getting tot entries glob ipf
<b>IP Filter Module</b>	LOG_ERR	[Function Name:]error getting glob ipf
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilter
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for handler registration
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for table registration info
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for iterator info
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilter
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:WLAN index is other than type int
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:WLAN index out of bound
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:tmp->next_variable NULL pointer
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:list index is other than type int
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:list index out of bound
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	problem encountered in ccWlanFilterTable_Handler: unknown column
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:reqinfo->mode = MODE_SET_FREE
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:reqinfo->mode = MODE_SET_UNDO
<b>IP Filter Module</b>	LOG_ERR	problem encountered in ccWlanFilterTable_Handler: unknown column
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for handler registration
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for table registration info



<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for iterator info
<b>IP Filter Module</b>	LOG_ERR	Could not get total entries from WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Could not get total entries from WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Could not get total entries from WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get total entries from WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Duplicate filter name in WLAN [wlan-index] IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get filter policy name required for deletion
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get filter policy direction required for deletion
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not check whether the entry present in the Global IP Table
<b>IP Filter Module</b>	LOG_ERR	Could not write Global IP Filter into the configuration
<b>IP Filter Module</b>	LOG_ERR	Could not get config IDs for the WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Could not get total entries from WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Could not get total entries from WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Could not delete entry from WLAN IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	problem encountered in ccWlanIpFilterPolicyTable: unknown column
<b>IP Filter Module</b>	LOG_ERR	Could not write Global IP Filter into the configuration
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalid index supplied.
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	problem encountered in ccWlanIpFilterPolicyTable_Handler: unknown column
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:IP Filter mode is disabled on WLAN [wlan-index] Enable it before adding/deleting any entries
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	No such row.

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Row already exists.
<b>IP Filter Module</b>	LOG_ERR	Unable to process set request in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column [column-number] in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[column-number] in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[column-number] in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[column-number] in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Problem encountered in ccWlanIpFilterPolicyTable_Handler: unsupported mode
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Could not get TRUNK IP Filter Mode
<b>IP Filter Module</b>	LOG_ERR	Could not get TRUNK IP Filter default incoming action
<b>IP Filter Module</b>	LOG_ERR	Could not get TRUNK IP Filter default outgoing action
<b>IP Filter Module</b>	LOG_ERR	Unknown param [magiv value decimal](magic value in hex) requested from ccWanTrunkIpFilterMIB
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for handler registration
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for table registration info
<b>IP Filter Module</b>	LOG_ERR	Unable to allocate memory for iterator info
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Duplicate filter name in TRUNK IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	"Invalid filter name, add corresponding entry in the Global IP Filter Table"
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWanTrunkIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get filter name at index[filter policy index]

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Duplicate filter name in TRUNK IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWanTrunkIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWanTrunkIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get filter policy name required for deletion
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get filter policy direction required for deletion
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not check whether the entry present in the Global IP Table
<b>IP Filter Module</b>	LOG_ERR	Could not write Global IP Filter into the configuration
<b>IP Filter Module</b>	LOG_ERR	Could not get Trunk IP Filter Table config Ids
<b>IP Filter Module</b>	LOG_ERR	Could not delete entry from Trunk IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	problem encountered in ccWanTrunkIpFilterTable: unknown column
<b>IP Filter Module</b>	LOG_ERR	Could not write Global IP Filter into the configuration
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalid index supplied.
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWlanIpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	problem encountered in ccWanTrunkIpFilterTable_Handler: unknown column
<b>IP Filter Module</b>	LOG_ERR	Config read/write error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	IP Filter mode is disabled on the TRUNK Port Enable it before adding/deleting any entries
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWanTrunkIpFilter
<b>IP Filter Module</b>	LOG_ERR	No such row.
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in ccWanTrunkIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	Row already exists.
<b>IP Filter Module</b>	LOG_ERR	Unable to process set request in ccWanTrunkIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable
<b>IP Filter Module</b>	LOG_ERR	problem encountered in [Function Name]: unsupported mode
<b>IP Filter Module</b>	LOG_ERR	Could not get total entries from TRUNK IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	[Function Name]:Could not get total entries from TRUNK IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Duplicate filter name in TRUNK IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	Unable to register cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Unable to register cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Unable to register cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	The filter name is used by either WLAN/TRUNK IP Filter Table\n delete it before deleting from Global IP Filter Table
<b>IP Filter Module</b>	LOG_ERR	“Config GET/SET error in cclpFilterPolicyTable”””
<b>IP Filter Module</b>	LOG_ERR	Start IP is greater than the End IP of either SRC or DEST\
<b>IP Filter Module</b>	LOG_ERR	problem encountered in cclpFilterPolicyTable: unknown column
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalid index supplied.
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	problem encountered in cclpFilterPolicyTable_Handler: unknown column
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	No such row.
<b>IP Filter Module</b>	LOG_ERR	Config GET/SET error in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Row already exists.
<b>IP Filter Module</b>	LOG_ERR	Unable to process set request in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[wlan-index]in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[wlan-index]in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[wlan-index]in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	Invalidation request rcvd for column[wlan-index]in cclpFilterPolicyTable
<b>IP Filter Module</b>	LOG_ERR	problem encountered in cclpFilterPolicyTable_Handler: unsupported mode
<b>DynDNS module</b>	LOG_ERR	ERROR while Get CFG_ID_TEST_INT5 (periodic interval)
<b>DynDNS module</b>	LOG_ERR	ERROR while Get DYNDNS_USERNAME
<b>DynDNS module</b>	LOG_ERR	ERROR while Get DYNDNS_PASSWORD
<b>DynDNS module</b>	LOG_ERR	ERROR Adding DynDNS Service Result: [Result]
<b>DynDNS module</b>	LOG_ERR	ERROR while Get DYNDNS_MODE
<b>DynDNS module</b>	LOG_ERR	ERROR while Get PPPPOE MODE
<b>DynDNS module</b>	LOG_ERR	ERROR while Get DYNDNS_HOSTNAME
<b>DynDNS module</b>	LOG_ERR	ERROR Adding DynDNS Interface Result [Result]
<b>DynDNS module</b>	LOG_ERR	ERROR in getting wan ip address
<b>DynDNS module</b>	LOG_ERR	ERROR Adding DynDNS Service Result:%d
<b>DynDNS module</b>	LOG_ERR	ERROR Delete Interface record
<b>DynDNS module</b>	LOG_ERR	ERROR Delete Service record

<b><i>System Component</i></b>	<b><i>Debug Level</i></b>	<b><i>Log Message</i></b>
<b><i>DynDNS module</i></b>	LOG_ERR	ERROR while retrieving DynDNS MODE
<b><i>DynDNS module</i></b>	LOG_ERR	ERROR adding Interface record

## A.6 Debug-Level Log Entries

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>802.1X Module</b>	LOG_DEBUG	Deauthenticating MU [MAC_ADDR] mu_ptr->addr
<b>Cell Controlled Module</b>	LOG_DEBUG	Not catching signal [Number] i
<b>EAP Module</b>	LOG_DEBUG	rcvd [Number] bytes of EAP payload from [MAC_ADDR]
<b>EAP Module</b>	LOG_DEBUG	sending eap-%s to [MAC_ADDR]
<b>EAP Module</b>	LOG_DEBUG	sending eap-id-req to [MAC_ADDR] usmu->mu->addr
<b>EAP Module</b>	LOG_DEBUG	sending eapol-key to [MAC_ADDR] usmu->mu->addr
<b>EAP Module</b>	LOG_DEBUG	sending eap-req to [MAC_ADDR] usmu->mu->addr
<b>Kerberos Client Module</b>	LOG_DEBUG	krb: AS_REQUEST sent to [IP_ADDR] sa.sin_addr.s_addr
<b>Kerberos Client Module</b>	LOG_DEBUG	krb: received AS_RESPONSE from [IP_ADDR] from_ip
<b>Kerberos Proxy Module</b>	LOG_DEBUG	krb5: as_request sent to [IP_ADDR] ip
<b>Kerberos Proxy Module</b>	LOG_DEBUG	krb5: error desc from KDC: %s err_reply->text.data
<b>Kerberos Proxy Module</b>	LOG_DEBUG	krb5: rcvd ap_req from MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_DEBUG	krb5: rcvd as_req from MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_DEBUG	krb5: rcvd sk_req from MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_DEBUG	krb5: rcvd tgs_req from MU [MAC_ADDR] mu_ptr->addr
<b>Kerberos Proxy Module</b>	LOG_DEBUG	krb5: tgs_request sent to [IP_ADDR] ip
<b>Kerberos Proxy Module</b>	LOG_DEBUG	rcvd WNMP message of type: [Number] from MU [MAC_ADDR]
<b>MU Association Module</b>	LOG_DEBUG	Ignoring Assoc_EID Field [Number]) from MU [MAC_ADDR]
<b>MU Association Module</b>	LOG_DEBUG	MU [MAC_ADDR] not present in MU table pkt_ptr->src
<b>MU Association Module</b>	LOG_DEBUG	MU [MAC_ADDR] not present in MU table pkt_ptr->src
<b>MU Association Module</b>	LOG_DEBUG	MU [MAC_ADDR] not present in MU table pkt_ptr->src
<b>MU Association Module</b>	LOG_DEBUG	Received Association-Req from [MAC_ADDR]
<b>MU Association Module</b>	LOG_DEBUG	Received Authentication-Req from [MAC_ADDR]
<b>MU Association Module</b>	LOG_DEBUG	Received DeAuthentication from [MAC_ADDR]
<b>MU Association Module</b>	LOG_DEBUG	Received ReAssociation-Req from [MAC_ADDR]
<b>MU Association Module</b>	LOG_DEBUG	Sending Auth-Resp to [MAC_ADDR] pkt_ptr->src
<b>NTP Client Module</b>	LOG_DEBUG	ntp is disabled in configuration
<b>NTP Client Module</b>	LOG_DEBUG	ntp request sent to [IP_ADDR] sa.sin_addr.s_addr
<b>NTP Client Module</b>	LOG_DEBUG	ntp server version [Number]) not same as our version
<b>NTP Client Module</b>	LOG_DEBUG	ntp: local: %ld.%ld server:%ld.%ld Drift = %ld.%ld\n

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>NTP Client Module</b>	LOG_DEBUG	rcvd ntp response from [IP_ADDR] sa.sin_addr.s_addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] rcv message #2 [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] rcv message #4 [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] rcv message #6 [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] starting key exchange a) [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] starting key exchange b) [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] xmit message #1 [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] xmit message #3 [MAC_ADDR] mu->addr
<b>Encryption Key Exchange Module</b>	LOG_DEBUG	[Pairwise Transient Key] xmit message #5 [MAC_ADDR] mu->addr
<b>RADIUS Module</b>	LOG_DEBUG	access-req sent to [IP_ADDR]:[Number] for [MAC_ADDR]
<b>RADIUS Module</b>	LOG_DEBUG	Msg-Auth absent in rsp from [[IP_ADDR]] from_ip
<b>RADIUS Module</b>	LOG_DEBUG	radius rsp from [IP_ADDR] for [MAC_ADDR] rcvd after timeout
<b>RADIUS Module</b>	LOG_DEBUG	rcvd access-challenge from [IP_ADDR] for [MAC_ADDR]
<b>Rogue AP Detection Module</b>	LOG_DEBUG	Adding AP: [MAC_ADDR] ESS: %s to reported_ap_list
<b>Rogue AP Detection Module</b>	LOG_DEBUG	Sent rogue-list req to [MAC_ADDR]! mu_ptr->addr
<b>Rogue AP Detection Module</b>	LOG_DEBUG	starting rogue detection requests
<b>Security Policy Module</b>	LOG_DEBUG	Using src: [IP_ADDR] for dst: [IP_ADDR] my_addr.sin_addr.s_addr dst_ip
<b>Security Policy Module</b>	LOG_DEBUG	Wlan %x; ESS %s; Auth %s; Enc %s i+1 ess
<b>Statistics Module</b>	LOG_DEBUG	errno [Number] sending trap to SNMPD\n errno
<b>SIP Module</b>	LOG_DEBUG	SIP:Decrementing the number of Inactive SIP sessions of portal [address] to [number]
<b>SIP Module</b>	LOG_DEBUG	SIP:Decrementing the number of Roamed SIP sessions of portal [address] to [number]
<b>SIP Module</b>	LOG_DEBUG	SIP:Decrementing the number of SIP sessions of MU [address] to [number]
<b>SIP Module</b>	LOG_DEBUG	SIP:Incrementing the number of SIP sessions of MU [address] to [number]
<b>SIP Module</b>	LOG_DEBUG	SIP:Cancel received in invalid state for call id [identifier]
<b>SIP Module</b>	LOG_DEBUG	SIP:Changing the state of the SIP session call id [identifier] to completed



<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>SIP Module</b>	LOG_DEBUG	SIP:Ack received in invalid state for call id [identifier]
<b>SIP Module</b>	LOG_DEBUG	SIP:Changing the state of the SIP session call id [identifier] to terminated
<b>SIP Module</b>	LOG_DEBUG	SIP:Changing the state of the SIP session call id [identifier] to processed
<b>SIP Module</b>	LOG_DEBUG	SIP:Removing the SIP session call id [identifier]
<b>SIP Module</b>	LOG_DEBUG	SIP:Timer expired for call id [identifier]
<b>SIP Module</b>	LOG_DEBUG	SIP: MU [addr] associated with different portal [addr]
<b>SIP Module</b>	LOG_DEBUG	SIP: SIP clean up timer called for MU [addr]
<b>SIP Module</b>	LOG_DEBUG	SIP: SIP clean up timer registered for MU [addr]
<b>SIP Module</b>	LOG_DEBUG	SIP: SIP clean up timer de-registered for MU [addr]
<b>WIPS module</b>	LOG_DEBUG	WIPS: Converting to sensors .....
<b>WIPS module</b>	LOG_DEBUG	WIPS: Resetting [MAC] .....
<b>WIPS module</b>	LOG_DEBUG	WIPS: Sending REVERT command to sensor [MAC] ...
<b>WIPS module</b>	LOG_DEBUG	WIPS: Detection started .....
<b>WIPS module</b>	LOG_DEBUG	Sending configuration to [MAC].....
<b>WIPS module</b>	LOG_DEBUG	WIPS: ACK received
<b>WIPS module</b>	LOG_DEBUG	WIPS: PINGREPLY received
<b>WIPS module</b>	LOG_DEBUG	WIPS: CONFIGREPLY received
<b>WIPS module</b>	LOG_DEBUG	WIPS: Unknown AD packet is received
<b>WIPS module</b>	LOG_DEBUG	WIPS: Adding sensor [MAC]
<b>WIPS module</b>	LOG_DEBUG	WIPS: Sensor already exists
<b>WIPS module</b>	LOG_DEBUG	"WIPS: Newly detected sensor, getting configuration..."
<b>WIPS module</b>	LOG_DEBUG	Configuration updated for [MAC]
<b>WIPS module</b>	LOG_DEBUG	Unexpected Ack received
<b>WIPS module</b>	LOG_DEBUG	Configuration received from [MAC]
<b>WIPS module</b>	LOG_DEBUG	"Converted AP [MAC] did not respond for unicast pings, removing from AP list"
<b>WIPS module</b>	LOG_DEBUG	WIPS: Unicast ping is sent to [MAC]
<b>AP Deny List</b>	LOG_DEBUG	RF Port [MAC] is denied for adoption
<b>AP2AP Beaconing</b>	LOG_DEBUG	Num MUs data received for MU probe request = [num mus]
<b>AP Revert</b>	LOG_DEBUG	Revert image sent successfully for AP [MAC]
<b>AP Revert</b>	LOG_DEBUG	"Image found: img_id1 = [image name], id received = [image name]"

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>Port Configuration</b>	LOG_DEBUG	Register value received for Port [idx] = [register value]
<b>Port Configuration</b>	LOG_DEBUG	Register value to be set for Port [idx] = [register value]
<b>Port Configuration</b>	LOG_DEBUG	Writing Register values for Wan = [register value]
<b>Port Configuration</b>	LOG_DEBUG	Setting Wan port configuration.
<b>Default Gateway</b>	LOG_DEBUG	Deleting Default gateway Interface [interface name]
<b>Default Gateway</b>	LOG_DEBUG	Adding Default gateway: Executing command [cmd]
<b>CF Format</b>	LOG_DEBUG	CF format message sent ot msg task
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from TRUNK OUTGOING context
<b>IP Filter Module</b>	LOG_DEBUG	Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	Allowing packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called before BCMC_LAN from TRUNK INCOMING context
<b>IP Filter Module</b>	LOG_DEBUG	IPF: Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from TRUNK INCOMING context
<b>IP Filter Module</b>	LOG_DEBUG	IPF: Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from WLAN[wlan-index]OUTGOING context
<b>IP Filter Module</b>	LOG_DEBUG	IPF: Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from PS_Switch_Defrag_Data WLAN[wlan-index] INCOMING context
<b>IP Filter Module</b>	LOG_DEBUG	IPF: Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from WLAN[wlan-index]OUTGOING context
<b>IP Filter Module</b>	LOG_DEBUG	IPF: Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from WLAN[wlan_index]INCOMING context
<b>IP Filter Module</b>	LOG_DEBUG	""IPF: Dropping packet""
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from BCMC_LAN WLAN[wlan_index]OUTGOING context
<b>IP Filter Module</b>	LOG_DEBUG	IPF: Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filtering is called from BCMC_ESS WLAN OUTGOING context
<b>IP Filter Module</b>	LOG_DEBUG	IPF: Dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	IP Filter Hash Table is locked dropping packet
<b>IP Filter Module</b>	LOG_DEBUG	match found
<b>IP Filter Module</b>	LOG_DEBUG	ip address mismatch
<b>IP Filter Module</b>	LOG_DEBUG	Port mismatch

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>IP Filter Module</b>	LOG_DEBUG	Protocol mismatch
<b>IP Filter Module</b>	LOG_DEBUG	direction mismatch[incoming/outgoing]
<b>IP Filter Module</b>	LOG_DEBUG	Hash entry pointing to NULL
<b>IP Filter Module</b>	LOG_DEBUG	Packet Source IP [ip address]
<b>IP Filter Module</b>	LOG_DEBUG	Packet Destination IP [ip address]
<b>IP Filter Module</b>	LOG_DEBUG	Packet protocol [protocol number]
<b>IP Filter Module</b>	LOG_DEBUG	Packet port [port number]
<b>IP Filter Module</b>	LOG_DEBUG	Packet direction[incoming/outgoing]
<b>IP Filter Module</b>	LOG_DEBUG	Default Action
<b>IP Filter Module</b>	LOG_DEBUG	Action [Allowing/Dropping] packet
<b>DynDNS Module</b>	LOG_DEBUG	No Change in Hostname and WAN IP
<b>DynDNS Module</b>	LOG_DEBUG	DynDNS: Duplicate record
<b>DynDNS Module</b>	LOG_DEBUG	[function]: Adding Service and Interface record DONE
<b>DynDNS Module</b>	LOG_DEBUG	"DynDNS Status: [Status] IP [IP address], Hostname [hostname] "

## A.7 Emergency Log Entries

<b>System Component</b>	<b>Debug Level</b>	<b>Log Message</b>
<b>Cell Controller Module</b>	LOG_EMERG	Caught Signal [Number] Aborting with core dump!
<b>Cell Controller Module</b>	LOG_EMERG	Assertion failed. Aborting with core dump!
<b>Cell Controller Module</b>	LOG_EMERG	bind failure: address in use. Check
<b>Cell Controller Utility Module</b>	LOG_EMERG	Assert Fail File %s Line [Number]; Exiting\n file
<b>Rogue AP Detection Module</b>	LOG_EMERG	memory allocation failure!
<b>Rogue AP Detection Module</b>	LOG_EMERG	Memory allocation failure!
<b>Security Policy Module</b>	LOG_EMERG	Config read failure. File: %s Line: [Number] \
<b>Security Policy Module</b>	LOG_EMERG	Couldn't init Security Policy for WLAN [Number] reverting to defaults i+1
<b>AP2AP Beaconing</b>	LOG_EMERG	memory allocation failure!



# Index

## Numerics

1 to 1 NAT	4-12
1 to Many NAT	4-12
802.11 b/g mode	5-23
802.11i encryption	5-13
802.1x EAP authentication	
advanced settings	5-9
configuring	5-8
RADIUS accounting	5-9
reauthentication settings	5-9
Syslog setup	5-9

## A

access	
administrator	6-2
configuring for subnets	3-7
control, setting	12-6, 12-34
points, rogue, <i>see</i> rogue APs	
types	6-2
user policy	6-13, 8-8
Access Control List, <i>see</i> ACL	
Access Ports	
adopting	5-5, 12-43
adoption requirements	5-17
advanced properties	5-25
advanced radio settings	5-24
advanced settings	5-23
allowed number per switch	5-17
antenna settings	5-25
approved list	5-33
associating to WLANs	12-19
authentication	5-29
changing name and location	5-18
configuring	5-16, 12-15, 12-49
error information	11-15
general information	11-14
installing and testing	12-60
interfaces information	11-6
managing	1-3
POS	12-17
printer	12-17
radio settings	5-18, 5-20
RF status	11-15
rogue, <i>see</i> rogue APs	

setting defaults	5-19, 12-15
setting rates	5-21
specialized radio settings	5-22
specifications	1-3
statistics	11-12
summary information	11-12
traffic information	11-14
traps	7-54
ACL	
MU access to WLAN	2-11, 5-16
setting up	7-51
administration support overview	7-2
administrator access	
AirBEAM software	6-4
authentication	6-3
changing password	6-4
configuring	6-2
RADIUS setup	6-3
settings	6-2
aggressive mode	4-24
AirBEAM software	
CF Card access	6-3
description	12-6
setting up access	6-4
settings	12-35
allow rules	4-25
antenna settings	5-21, 5-25
AP300 Access Port authentication	5-29
attacks, types	4-6
authentication	
802.1x EAP	5-8
administrator	6-3
CHAP	2-9, 4-4
EAP types	6-5
EAP-TTLS	6-6
GTC	6-6
header	3-9, 3-11, 3-16
IKE	4-24
Kerberos	5-10
LDAP	6-7
MSCHAP-V2	6-6
none	5-15
PAP	2-9, 4-4
RADIUS server	6-3, 6-6
RIP	4-16

setting method	2-11
setting up for AP300	5-29
user, configuring	6-5
WAN methods	2-9, 4-4
WLANs	5-7
authorization levels	7-50
automatic key exchange	
description	4-19
setting up	4-21

**B**

bandwidth, Share Mode settings	5-28
beacon settings	5-22, 5-27
blocking	
outbound FTP actions	4-30
outbound HTTP requests	4-29
SMTP commands	4-29
broadcast ESS, answering	5-7
browser recommendations	1-2

**C**

Cell Controller services	1-6
certificates	
importing CA	6-14
managing digital	6-14
request form	6-16
selecting	6-6
self, <i>see</i> self certificates	
specifying for IKE	4-27
types	6-14
CF Card	
contents, view	7-59
enable logging to	7-59
erase a	7-9
firmware updates	7-8
format a	7-9
redirect pages, hotspot	8-6
unmount a	7-59
channel, radio	5-20
CHAP authentication	2-9, 4-4
Clear To Send (CTS)	5-21
clients, configuring	12-29
commands, blocking	4-29
communication	
configuring	2-2
protocols	3-8
compatibility	
java	2-2
configuration	
basic settings	2-4, 12-33
LAN interface	2-5
PPPoE	2-8
SNMP default	2-5
Subnet1	2-6
WAN interface	2-7

WLANs	2-9
connections, testing	12-29
connectivity testing	2-12
content filtering, configuring	4-29
conventions, typographical	1-2
country settings, changing	7-3

**D**

DATA command	4-29
database, local	6-9
DDNS	
all subnets, updating DNS entries for	9-5
enabling	9-2
overview	9-2
single subnets, updating DNS entries for	9-4
updating DNS entries	9-4
destination ports, description	3-12
DHCP	
advanced settings	3-5
configuration	3-5
description	2-7
firmware upload options	7-9
setting up server	7-10
Diffie-Hellman groups	4-25
digital certificates, managing	6-14
dimensions	1-4
Domain Name Service (DNS) protocol	3-8
downloads, updated firmware	7-7
DTIM period	5-22, 5-23, 5-27
Dynamic Host Configuration Protocol, <i>see</i> DHCP	

**E**

EAP	
configuring authentication	5-8
Protected EAP	6-5
Tunneled TLS EAP	6-5
type options	6-5
email address, administrator	2-4
Encapsulating Security Protocol (ESP)	3-9, 3-11, 3-16
encryption	
algorithm types	4-20
KeyGuard	5-14
none	5-15
setting method	2-11, 5-11
WEP	2-11, 5-11
WPA2-CCMP	5-13
WPA-TKIP, <i>see</i> WPA2-CCMP	5-12
environmental specifications	1-4
error information	
Access Ports	11-15
WLAN	11-12
ESSID, WLAN	5-6
EXP command	4-30
Extensible Authentication Protocol, <i>see</i> EAP	

**F**

files, sample configuration file	7-13
filters	
content	4-29
firewall	4-6, 12-42
firewall	
blocking attacks	4-6
configurable filters	4-6
configuring	4-5, 4-31
confirming configuration	12-42
disabling	4-5
inspecting	12-14
rules settings	3-10
security	1-3
transport protocols	3-11
firmware update	
completing update	7-8
perform	7-8
using CF Card	7-8
using FTP	7-8
using TFTP	7-8
firmware, updating	7-7
forward NAT	3-12
FQDN ID type	4-24
FTP	
blocking outbound actions	4-30
bounce attacks	4-7
exporting and importing settings	7-11
firmware updates	7-8
protocol description	3-8

**G**

gateway services	1-6
General Routing Encapsulation (GRE)	3-9, 3-12, 3-16
Generic Token Card (GTC) authentication	6-6
graphs, displaying statistics in	11-19
groups	
access policy	6-13, 8-8
adding or deleting	6-9
guest users	
adding	6-10
quick creation of	6-10

**H**

hardware overview	1-4
HELO command	4-29
hotspot	
configuring	8-4
enabling on WAN	8-3
handling login and redirection	8-9
hotspot state of mobile unit, defining	8-8
RADIUS accounting	8-9
RADIUS accounting, logs	8-5
RADIUS authentication	8-9
RADIUS, configuring	8-4

redirect pages	8-6
redirect pages, Get External URL	8-6
redirect pages, Get from Clipboard	8-6
redirect pages, Use CF Card	8-6
requirements for	8-2
white list	8-5

## hotspots

configuring	8-2
hotspot, system	8-2
Hypertext Transfer Protocol (HTTP)	3-8

**I**

## IKE

allow rules	4-26
authentication modes	4-24
description	4-19
operation modes	4-24
setting up	4-23
specifying certificates	4-27
installation	2-2
interfaces, port information	11-6
Internet Control Message Protocol (ICMP)	3-9, 3-11, 3-16
Internet Key Exchange, <i>see</i> IKE	
IP addresses, planning	12-7
IP unaligned timestamp attacks	4-7
IPS	
definition	4-9
packet direction	4-10
protocol anomaly detection	4-11
signature categories	4-10

**J**

## java

compatibility with	2-2
JRE 1.4	2-2

**K**

Kerberos authentication, configuring	5-10
key exchange types	4-19
KeyGuard encryption settings	5-14

**L**

## LAN

configuration screen	3-2
configuring	12-35
configuring interface	2-5
enabling Subnet1	2-5
Layer 3 VLANs	3-14, 10-3
LED functions	1-5
Lightweight Directory Access Protocol (LDAP), configuring	6-7
local area network, <i>see</i> LAN	
local ID vs. remote ID	4-27
location variable	
changing	7-3

entering	2-4
log	
enable logging to CF card	7-59
system server, setup	7-58
logging in	
AirBEAM name and password	6-4
default name	6-2
procedure	2-3
log, system	7-58

**M**

MAC addresses	
description	5-17
start and end range	5-5
MAIL command	4-29
manual key exchange	
configuring	4-19
description	4-19
Mesh Settings	
mesh base settings	5-44
mesh client settings	5-44
mesh settings	5-43
MIME flood attacks	4-7
mobile units	
ACL	2-11, 5-16
MU to MU communications settings	5-6
settings	5-9
statistics	11-16
traps	7-54
MSCHAP-V2 authentication	6-6
multicast address voice prioritization	5-29

**N**

name variable, changing	
switch	7-3
WLAN	5-6
NAT	
1 to 1	4-12
1 to Many	4-12
configuring	4-12, 12-13
forward vs. reverse	3-12
selecting type	4-12
setting up	12-41
Network Address Translation, <i>see</i> NAT	
network traps	7-53
NTP server, specifying	7-56

**O**

operating system services	1-6
---------------------------	-----

**P**

PAP authentication	2-9, 4-4
passwords	
AirBEAM	6-4

changing for administrator	6-4
default	6-2
entering	2-3
settings	7-50
placement, radio	5-20
Point-to-Point Protocol over Ethernet, <i>see</i> PPPoE	
port-based VLANs	3-14, 10-3
ports	
destination, description	3-12
forwarding options	4-13
hardware configuration	1-4
source, description	3-12
POS subnet, configuring	12-8
Post Office Protocol (POP)	3-8
power level, radio	5-20
power specifications	1-4
PPPoE, setting up	2-8, 4-3
preamble length	5-23, 5-25
Pre-Shared Key (PSK)	5-12
primary WLAN	5-22
printer subnet, configuring	12-9
Protected EAP (PEAP) authentication	6-5
proxy configuration, setting up	6-8

**Q**

quality of service (QoS)	
Bandwidth Share Mode	5-28
configuration	5-27
QUIT command	4-29

**R**

radio settings	
Access Port options	5-18, 5-20
advanced	5-24
specialized	5-22
RADIUS server	
accounting	5-9
administrator access	6-3
authentication options	6-5
client authentication	6-6
configuring	6-5
data source	6-5
hotspot	
accounting	8-9
authentication	8-9
configuring for	8-4
LDAP settings	6-7
local user database	6-9
proxy configuration	6-8
shared secret	5-9
user access policy	6-13, 8-8
RCPT command	4-29
redundancy	
configuring	7-6
modes	7-6



- operational status ..... 7-7
  - remote ID
    - types ..... 4-24
    - vs. local ID ..... 4-27
  - RESET command ..... 4-30
  - restarting the switch ..... 7-2
  - reverse NAT ..... 3-12
  - RF status
    - Access Ports ..... 11-15
    - WLAN ..... 11-11
  - robust security network (RSN) ..... 5-13
  - rogue APs
    - containment ..... 5-34
    - detection ..... 5-30
    - examining and approving ..... 5-33
    - getting details ..... 5-35
    - listing ..... 5-33
    - maintaining rule list ..... 5-32
    - rogue detector, getting details about ..... 5-36
    - setting SNMP traps ..... 5-36
    - setting up detection ..... 5-31
    - traps ..... 7-54
  - Round Robin ..... 5-28
  - routes
    - special requirements ..... 4-26
    - static, *see* static routes
    - user defined ..... 4-15
  - Routing Information Protocol (RIP) configuration ..... 4-15
  - RTS threshold ..... 5-21, 5-26
  - rules
    - firewall ..... 3-10
    - maintaining lists ..... 5-32
  - RX fields, statistics ..... 11-2, 11-5
- S**
- SAML command ..... 4-30
  - security
    - authorization levels ..... 7-50
    - available settings and protocols ..... 1-3
    - beacon settings ..... 5-22
    - firewall ..... 1-3
    - SA negotiation ..... 4-19
    - setting up ..... 12-46
    - VPNs ..... 1-3, 4-19
    - WLAN ..... 1-3, 2-10, 5-7
  - self certificates
    - creating ..... 6-16
    - description ..... 6-14
    - request form ..... 6-16
    - selecting ..... 6-6
  - Self Heal
    - definition ..... 5-42
    - interference avoidance ..... 5-43
    - neighbor recovery ..... 5-42
  - SEND command ..... 4-29
  - sequence number prediction attacks ..... 4-7
  - settings, exporting and importing ..... 7-11
  - setup, step by step ..... 2-2
  - shared secrets, setting up ..... 6-6
  - short preamble ..... 5-23, 5-25
  - Smart Scan ..... 5-41
  - SMTP
    - blocking commands ..... 4-29
    - protocol description ..... 3-8
  - SNMP
    - access ..... 6-3
    - configuring ..... 7-48
    - default configuration ..... 2-5
    - setting version configuration ..... 7-49
    - v1/v2 community definitions ..... 7-49
    - v3 community definitions ..... 7-50
  - SNMP traps, setting
    - categories and descriptions ..... 7-53
    - configuration ..... 7-51
    - rate traps ..... 7-55
    - rogue APs ..... 5-36
    - selecting ..... 7-52
    - threshold types ..... 7-55
    - v1/v2 ..... 7-51
    - v3 ..... 7-52
  - software
    - Cell Controller ..... 1-6
    - gateway services ..... 1-6
    - operating system ..... 1-6
    - overview ..... 1-6
  - source ports, description ..... 3-12
  - source routing attacks ..... 4-6
  - specifications
    - Access Ports ..... 1-3
    - dimensions ..... 1-4
    - hardware overview ..... 1-4
    - power and environment ..... 1-4
  - SSH, configuring connection parameters ..... 6-3
  - stand-alone mode ..... 7-6
  - static routes, configuring ..... 4-14
  - statistics
    - Access Ports ..... 11-12
    - interfaces ..... 11-6
    - mesh ..... 11-17
    - mesh base ..... 11-17
    - mesh client ..... 11-17
    - mobile units ..... 11-16
    - received fields ..... 11-2, 11-5
    - STP stats ..... 11-6
    - subnet ..... 11-3
    - subnet lease ..... 11-3
    - subnet stats ..... 11-5
    - transmitted fields ..... 11-3, 11-6
    - viewing in graph form ..... 11-19
    - WAN ..... 11-2
    - WLAN ..... 11-8
  - subnet access

advanced settings	3-10
allowing or denying	3-8
configuring	3-7, 12-27, 12-54
level descriptions	3-7
protocols	3-8
subnets	
access, <i>see</i> subnet access	
changing features	3-3
configuring	3-3
configuring Subnet1	2-6
defining	3-2
enabling Subnet1	2-5
interface information	11-6
mapping to VLANs	3-15
POS	12-8
printer	12-9
summary information	2-5, 3-3
SYN flood attacks	4-6
Syslog setup	5-9
system	
basic information	2-4
basic settings	12-5, 12-33
changing name	7-3
configuring settings	12-31
DDNS	9-2
hotspot	8-2
overview	1-3
settings	7-3
traps	7-53
updating firmware	7-7
viewing log	7-58
VLAN	10-2
VLAN Trunking <i>see</i> system, VLAN	10-2
<b>T</b>	
technical specifications	1-4
TELNET protocol	3-8
Temporal Key Integrity Protocol (TKIP)	5-12
TFTP	
exporting and importing settings	7-11
firmware updates	7-8
timeout settings	6-4
transform sets	4-19
Transmission Control Protocol (TCP)	3-9, 3-11, 3-16, 4-6
transport protocol descriptions	3-9
traps, <i>see</i> SNMP traps, setting	
Tunneled TLS EAP (EAP-TTLS) authentication	6-6
tunnels	
Advanced Subnet Access	4-25
DHCP addresses	4-28
setting up without WAN address	4-27
trouble establishing	4-27
VPN, creating	4-18
TX fields, statistics	11-3, 11-6
typographical conventions	1-2

**U**

UFQDN ID type	4-24
uniform spreading	5-22
update firmware <i>see</i> firmware update, perform	7-8
URL extensions, blocking	4-29
URL Filtering	
black list	3-18
blacklist table	3-19
filtering rules order	3-19
keyword	3-18
keyword table	3-19
order of, filtering rules	3-19
permitted access	3-18
reverse dns lookup failure	3-18
table, blacklist	3-19
table, keyword	3-19
table, trusted hosts	3-19
table, whitelist	3-19
trusted hosts table	3-19
trusted IPs	3-18
whitelist table	3-19
use cases	
field office example	12-30
retail example	12-3
User Datagram Protocol (UDP)	3-9, 3-11, 3-16, 4-6
user-defined routes, creating	4-15
users	
access policy	6-13, 8-8
adding guest users	6-10
adding to database	6-10
authentication, configuring	6-5
database, managing	6-9
guest users, adding <i>see</i> guest users, adding	
ID, entering	2-3
RADIUS server settings	6-5

**V**

Virtual Local Area Networks, <i>see</i> VLANs	
Virtual Private Networks, <i>see</i> VPNs	
VLAN	
overview	10-2
packets, assigning tags to	10-2
VLAN Trunking	
configuring	10-3
installing and default settings	10-2
packets, assigning tags to	10-2
WLANs, mapping to	10-4
VLANs	
configuration	3-14
description	3-14
mapping to subnets	3-15
voice prioritization, configuring	5-29
VPNs	
allow rules	4-25
configuring	4-17, 12-57

creating tunnels .....	4-18
FAQs .....	4-25
security .....	1-3
setting up security .....	4-19
troubleshooting .....	4-25
VRFY command .....	4-30

## W

WAN	
configuring interface .....	2-7, 4-2, 12-12, 12-40
description .....	4-2
enabling hotspot .....	8-3
external communication .....	2-7, 4-2
statistics .....	11-2
Weighted Round Robin .....	5-28
WEP encryption	
configuring .....	5-11
key settings .....	5-11
modes .....	5-11
selecting .....	2-11
Wide Area Network, <i>see</i> WAN	
WIDS	
configuration .....	5-39
configuring	
anomaly violation .....	5-39
excessive violation .....	5-39
filtered MUs .....	5-40
setup .....	5-38
Winnuking attacks .....	4-6
WIPS	
configuration .....	5-37
Wired Equivalent Privacy, <i>see</i> WEP encryption	
Wireless Local Area Networks, <i>see</i> WLANs	
WLANs	
advanced settings .....	5-6
assigning Access Ports .....	5-5
authentication .....	5-7
bandwidth share .....	5-29
basic information .....	5-3
configuring .....	5-6, 12-19, 12-45
configuring security .....	2-10
displaying summary information .....	11-8
enabling .....	2-9, 5-3
error information .....	11-12
ESSID .....	5-6
general information .....	11-11
primary .....	5-22
RF status .....	11-11
security .....	1-3, 5-7
statistics .....	11-8
summary of settings .....	2-9
traffic information .....	11-11
VLAN Trunking, mapping to .....	10-4
voice prioritization .....	5-29
WPA2-CCMP (802.11i) encryption, configuring .....	5-13
WPA-TKIP encryption, configuring .....	5-12







**MOTOROLA INC.**  
**1303 E. ALGONQUIN ROAD**  
**SCHAUMBURG, IL 60196**  
**<http://www.motorola.com>**

**72E-121350-01 Revision A**  
**February 2009**