

Arada Systems, Inc.

MaxR-3210 Single Band Wireless-N Access Point User Manual

This document helps you to configure and use the
MaxR-3210 Single Band Wireless-N Access Point

Dec 2009

Book Version: 1.1



Arada Systems Inc.,

1024 Morse Avenue,
Sunnyvale, CA - 94089.

Tel: +1 (408) 773 9298
www.aradasystems.com

Contents

About This Manual

Conventions, Formats, and Scope	i
---------------------------------------	---

Chapter 1

Introduction

About the MaxR-3210 Single Band Wireless-N Access Point	1-1
Key Features and Standards	1-1
Supported Standards and Conventions	1-2
Key Features	1-2
802.11b/g/n Standards-based Wireless Networking	1-4
Autosensing Ethernet Connections with Auto Uplink	1-4
System Requirements	1-4
What's In the Box?	1-5
Hardware Description	1-5
Rear Panel	1-5

Chapter 2

Basic Installation and Configuration

Wireless Equipment Placement and Range Guidelines	2-2
Understanding MaxR-3210 Wireless Security Options	2-3
Installing the MaxR-3210 Wireless Access Point	2-4
Setting up the MaxR-3210 Wireless Access Point	2-4
Configuring LAN and Wireless Access	2-4
Configuring Time Settings	2-7
Configuring Wireless Access	2-9
Deploying the MaxR-3210 Wireless Access Point	2-9
Verifying Wireless Connectivity	2-10
Logging In Using the Default IP Address	2-10
Setting Basic IP Options	2-11
Wireless Settings	2-13
Configuring 802.11b/bg/ng Wireless Settings	2-13

Configuring Basic QoS Settings	2-16
Setting Up and Testing Basic Wireless Connectivity	2-17
Understanding Security Profiles	2-18
SSID and WEP/WPA Settings Setup Form	2-22
802.11b/bg/ng Configuration	2-22
Configuring the RADIUS Server Settings	2-23
Setting up a Security Profile	2-25
Configuring WEP	2-27
Configuring WPA with RADIUS	2-29
Configuring WPA2 with RADIUS	2-31
Configuring WPA and WPA2 with RADIUS	2-32
Configuring WPA-PSK	2-34
Configuring WPA2-PSK	2-35
Configuring WPA-PSK and WPA2-PSK	2-36
Restricting Wireless Access by MAC Address	2-38

Chapter 3 Management

Remote Management	3-1
Remote Console	3-3
Using the Secure Telnet Interface	3-3
CLI Commands	3-4
Upgrading the Wireless Access Point Software	3-5
Configuration File Management	3-6
Saving Your Configuration Settings	3-7
Restoring Saved Settings	3-7
Restoring the MaxR-3210 to the Factory Default Settings	3-8
Changing the Administrator Password	3-10
Enabling the SysLog Server	3-11
Using Activity Log Information	3-12
Viewing General Summary Information	3-12
Viewing Network Traffic Statistics	3-14
Viewing Available Wireless Station Statistics	3-16
Enabling Rogue AP Detection	3-17
Importing Rogue AP List from a File	3-18
Viewing Rogue AP Statistics	3-19

Packet Capture	3-21
Chapter 4	
Advanced Configuration	
IP Settings for Wireless Clients	4-1
Hotspot Settings	4-3
Configuring Advanced Wireless Settings	4-4
Configuring 802.11b/bg/ng Advanced Wireless Settings	4-4
Configuring Advanced QoS Settings	4-6
Enabling Wireless Bridging	4-8
Configuring an MaxR-3210 as a Point-to-Point Bridge	4-12
Configuring an MaxR-3210 as a Point-to-Multi-Point Wireless Bridge	4-13
Chapter 5	
Troubleshooting and Debugging	
No lights are lit on the Access Point.	5-1
The Wireless LAN activity light does not light up.	5-1
The LAN light is not lit.	5-2
I cannot access the Internet or the LAN with a wireless capable computer.	5-2
I cannot connect to the MaxR-3210 to configure it.	5-3
When I enter a URL or IP address I get a timeout error.	5-3
Using the Reset Button to Restore Factory Default Settings	5-4
Appendix A	
Default Settings and Technical Specifications	
Factory Default Settings	A-1
Technical Specifications	A-3
Appendix B	
Command Line Reference	
Command Sets	B-1
Index	

About This Manual

The *MaxR-3210 Single Band Wireless-N Access Point User Manual* describes how to install, configure and troubleshoot the MaxR-3210 Wireless Access Point. The information in this manual is intended for readers with intermediate computer and Internet skills.


Conventions, Formats, and Scope


The conventions, formats, and scope of this manual are described in the following paragraphs:


- **Typographical Conventions.** This manual uses the following typographical conventions:

<i>Italic</i>	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
<i>italic</i>	URL links

- **Formats.** This manual uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.
-------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------

	Tip: This format is used to highlight a procedure that will save time or resources.
-------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.
-------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------



Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

Chapter 1

Introduction

This chapter describes some of the key features of the MaxR-3210 Single Band Wireless-N Access Point. It also includes the minimum prerequisites for installation ([“System Requirements” on page 1-4.](#)), package contents ([“What’s In the Box?” on page 1-5](#)) and a description of the front and back panels of the MaxR-3210 ([“Hardware Description” on page 1-5](#)).

About the MaxR-3210 Single Band Wireless-N Access Point

The MaxR-3210 Single Band Wireless-N Access Point is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The MaxR-3210 provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) via an antenna. Typically, an individual in-building access point provides a maximum connectivity area of about a 500 foot radius. Consequently, the MaxR-3210 Single Band Wireless-N Access Point can support a small group of users in a range of several hundred feet. Most access points can handle between 10 to 30 users simultaneously per radio.

The MaxR-3210 Single Band Wireless-N Access Point acts as a bridge between the wired LAN and wireless clients. Connecting multiple MaxR-3210 Wireless Access Points via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point to another and still maintain seamless connection to the network.

Key Features and Standards

The MaxR-3210 Wireless Access Point is easy-to-use and provides solid wireless and networking support. It also offers a wide range of security options.

Supported Standards and Conventions

The following standards and conventions are supported:

- **Standards Compliance.** The Wireless Access Point complies with the IEEE 802.11b/g/n standards for Wireless LANs.
- **Full WPA and WPA2 support.** WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPA-PSK and WPA2-PSK preshared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA.
- **Multiple BSSIDs.** Supports multiple BSSIDs. When a Access Point is connected to a wired network and a set of wireless stations, it is called a Basic Service Set (BSS). The Basic Service Set Identifier (BSSID) is a unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network.

The multiple BSSID feature allows you to configure up to 8 SSIDs on your MaxR-3210 access point and assign different configuration settings to each SSID. All the configured SSIDs are active and the network devices can connect to the access point by using any of these SSIDs.

- **DHCP Client Support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The MaxR-3210 can act as a client and obtain information from your DHCP server; it can also act as a DHCP server and provide network information for wireless clients.
- **SNMP Support.** Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.
- **802.1Q VLAN (Virtual LAN) Support.** A network of computers that behave as if they are connected to the same network even though they actually may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user/host management, bandwidth allocation and resource optimization.

Key Features

The MaxR-3210 provides solid functionality, including the following features:

- **2.4Ghz Band Operating Frequency.** The Wireless Access Point operates in the 2.4 GHz frequency band.
- Multiple operating modes:
 - **Wireless Access Point.** Operates as a standard 802.11b/bg/ng access point.

- **Point-to-Point Bridge.** In this mode, the MaxR-3210 only communicates with another bridge-mode wireless access point (with or without clients). Network authentication should be used to protect this communication.
- **Point-to-Multi-Point Bridge.** Select this only if this MaxR-3210 is the “Master” for a group of bridge-mode wireless access points. The other bridge-mode wireless access points send all traffic to this “Master”, and do not communicate directly with each other. Network Authentication should be used to protect this traffic.
- **Hotspot Settings.** You can allow the first HTTP (TCP, port 80) request, on client association, to be captured and redirected to the URL you specify.
- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely. In addition to using Web browser to do so, command-line interface and SNMP can also be used.
- **Rogue AP detection.** The Rogue AP detection feature shows a list of unknown APs to the administrator.
- **Access Control.** The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the MaxR-3210 to gain access to your LAN.
- **Security Profiles.** When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, etc.) for each BSSID.
- **Hidden Mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Secure Telnet Command Line Interface.** The secure Telnet command line interface enables direct secure access over the serial port and easy scripting of configuration of multiple MaxR-3210s across an extensive network via the Ethernet interface. An SSH client is required.
- **Configuration Backup.** Configuration settings can be backed up to a file and restored.
- **Power over Ethernet.** Power can be supplied to the MaxR-3210 over the Ethernet port from any 802.3af compliant mid-span or end-span source.
- **Autosensing Ethernet Connection with Auto Uplink Interface.** Connects to 10/100/1000 Mbps IEEE 802.3 Ethernet networks.
- **LED Indicators.** Power/Test, LAN speed, LAN activity, and wireless activity for each radio mode are easily identified.
- **Wireless Multimedia (WMM) Support.** WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.

- **WMM Power Save Support.** Power Save uses mechanisms from 802.11e and legacy 802.11 to save power (for battery powered equipment) and fine-tune power consumption.
- **VLAN Security Profiles.** Each Security Profile can be assigned a VLAN ID as each Security Profile is modified.

802.11b/g/n Standards-based Wireless Networking

The MaxR-3210 Single Band Wireless-N Access Point provides a bridge between Ethernet wired LANs and 802.11b/g/n compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the MaxR-3210 supports the following wireless features:

- Aggregation Support
- Reduced Inter Frame Spacing support
- Multiple Input, Multiple Output (MIMO) support
- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Auto or long preamble
- Roaming among access points on the same subnet

Autosensing Ethernet Connections with Auto Uplink

The MaxR-3210 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

The access point incorporates Auto Uplink™ technology. The Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a “normal” connection such as to a computer or an “uplink” connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates any concerns about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

System Requirements

Before installing the MaxR-3210, make sure your system meets these requirements:

- A 10/100/1000 Mb/s Local Area Network device such as a hub or switch

- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100-240 V, 50-60 Hz AC power source
- A Web browser for configuration such as Microsoft Internet Explorer 5.0 or above, or Mozilla 3.0 or above
- At least one computer with the TCP/IP protocol installed
- 802.11b/g/n-compliant devices.

What's In the Box?

The product package should contain the following items:

- MaxR-3210 Single Band Wireless-N Access Point
- Three Reverse SMA 5dbi dual band dipole antennas.
- Power adapter and cord (12 V dc, 1.5 A)
- Straight through Category 5 Ethernet cable
- RJ-45 to DB-9 female connector.
- *Resource CD* which includes this manual.
- Support Registration card

Contact your reseller or customer support in your area if there are any missing or damaged parts. You can refer to the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the MaxR-3210 if you need to return it for repair.

Hardware Description

This section describes the rear panel hardware functions of the MaxR-3210.

Rear Panel

The MaxR-3210 rear panel functions are described below:

1. Left, Middle, and Right Detachable Antenna

The MaxR-3210 provides three detachable antennas.

2. Restore to Factory Defaults Button

The restore to default button is located next to the RJ-45 console port and restores the MaxR-3210 to the factory default settings.

3. Serial Console Port

RJ-45 serial console port for serial DTE connections.

4. RJ-45 Ethernet Port

Use the MaxR-3210 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or PoE switch.

5. Power Socket

This socket connects to the MaxR-3210 12V 1.5A power adapter.

Chapter 2

Basic Installation and Configuration

This chapter describes how to set up your MaxR-3210 Single Band Wireless-N Access Point for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b/g/n wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.



Note: Indoors, computers can connect over 802.11b/bg/ng wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The MaxR-3210 Wireless Access Point provides highly effective security features which are covered in detail in [“Understanding Security Profiles”](#) on page 2-18. Deploy the security features appropriate to your needs.

This chapter contains the following sections:

1. [“Wireless Equipment Placement and Range Guidelines](#)
2. [“Understanding MaxR-3210 Wireless Security Options](#)
3. [“Installing the MaxR-3210 Wireless Access Point](#)
4. [“Logging In Using the Default IP Address](#)
5. [“Setting Basic IP Options](#)
6. [“Wireless Settings](#)
7. [“Setting Up and Testing Basic Wireless Connectivity](#)
8. [“Understanding Security Profiles](#)
9. [“SSID and WEP/WPA Settings Setup Form](#)
10. [“Configuring the RADIUS Server Settings](#)
11. [“Setting up a Security Profile](#)
12. [“Configuring WEP](#)
13. [“Configuring WPA with RADIUS](#)

14. [“Configuring WPA2 with RADIUS](#)
15. [“Configuring WPA and WPA2 with RADIUS](#)
16. [“Configuring WPA-PSK](#)
17. [“Configuring WPA2-PSK](#)
18. [“Configuring WPA-PSK and WPA2-PSK](#)
19. [“Restricting Wireless Access by MAC Address](#)

You need to prepare these three things before you can establish a connection through your wireless access point:

- A location for the MaxR-3210 that conforms to the [“Wireless Equipment Placement and Range Guidelines](#) below.
- The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11b/g/n wireless adapters.

Wireless Equipment Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the Access Point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.



Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the MaxR-3210. For complete performance specifications, see [Appendix A, “Default Settings and Technical Specifications.”](#)

For best results, place your Access Point:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.

If you are using multiple access points for 11b/bg/ng, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. Some types of security connections can take slightly longer to establish and can consume more battery power on a notebook computer.

Understanding MaxR-3210 Wireless Security Options

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The MaxR-3210 Wireless Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the MaxR-3210. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, Vista and Unix systems but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP open authentication and WEP data encryption will block all but the most determined eavesdropper.
- **Use WPA or WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.



Note: WEP and TKIP provide only legacy rates of operation. So, AES is the recommended solution to use the 802.11n rates and speed.

Installing the MaxR-3210 Wireless Access Point

Before installing the MaxR-3210 Single Band Wireless-N Access Point, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b/g/n wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on [“System Requirements” on page 1-4](#).

Setting up the MaxR-3210 Wireless Access Point



Tip: Before mounting the MaxR-3210 in a high location, first set up and test the MaxR-3210 to verify wireless network connectivity.

To set up the MaxR-3210 Wireless Access Point:

1. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.
2. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.
3. Connect an Ethernet cable from the MaxR-3210 to the computer.
4. Turn on your computer, connect the power adapter to the MaxR-3210 and verify the following:
 - The PWR power light goes on.
 - The LAN light of the Access Point is lit when connected to a powered on computer.
 - The WLAN LEDs should be blinking.

Configuring LAN and Wireless Access

To configure the MaxR-3210 Ethernet port for LAN access:

1. Connect to the MaxR-3210 by opening your browser and entering **http://192.168.0.237** in the address field. The MaxR-3210 login screen appears (see [Figure 2-1](#)).
2. Enter **admin** for the user name and **password** for the password, both in lower case letters.

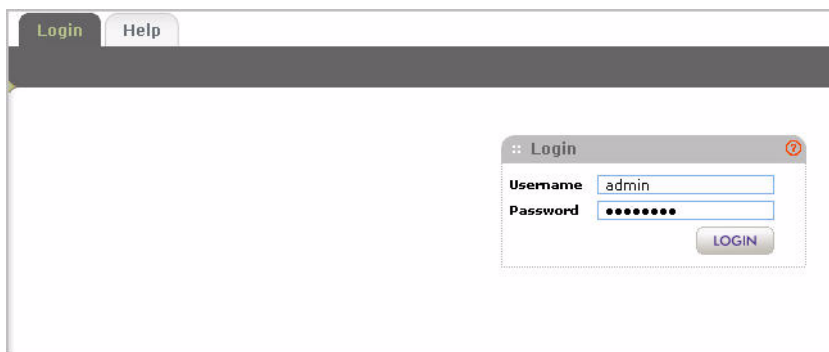


Figure 2-1 Login screen

3. Click **Login**. The main menu of the MaxR-3210 displays as shown in [Figure 2-2](#).
 - When the Access Point is connected to the Internet, under the **Support** tab, select **Documentation** to view the documentation for the Access Point.
 - On the top-right of the screen, select **Logout** to exit the MaxR-3210 setup screens. (You will automatically be logged out of the Access Point after 5 minutes of no activity.)
4. **Access Point Name:** Enter the access point name of the MaxR-3210.

This unique name is the access point NetBIOS name. The default Access Point Name is located on the bottom label of MaxR-3210. The default is aradaxxxxxx, where xxxxxx represents the last 6 digits of the MaxR-3210 MAC address. You may modify the default name with a unique name up to 15 characters long.

5. Select **Time** from the left panel. The Time screen displays, as shown in [Figure 2-2](#).

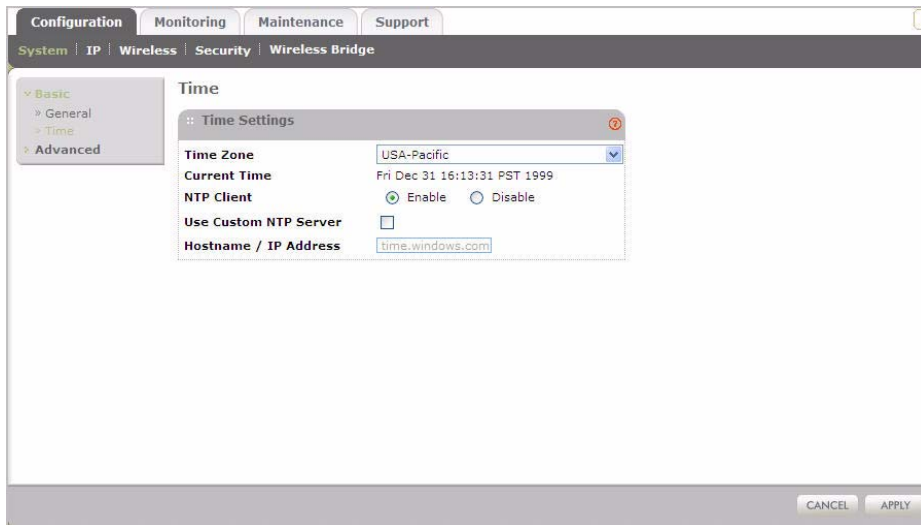


Figure 2-2 Timezone and system time related settings

6. Enter the Time Settings for your area. See the online help or [“Configuring Time Settings” on page 2-7](#) for more information about how to configure the settings on this screen.

7. Select **IP** on the main menu. The IP Settings screen displays, as shown in [Figure 2-3](#).

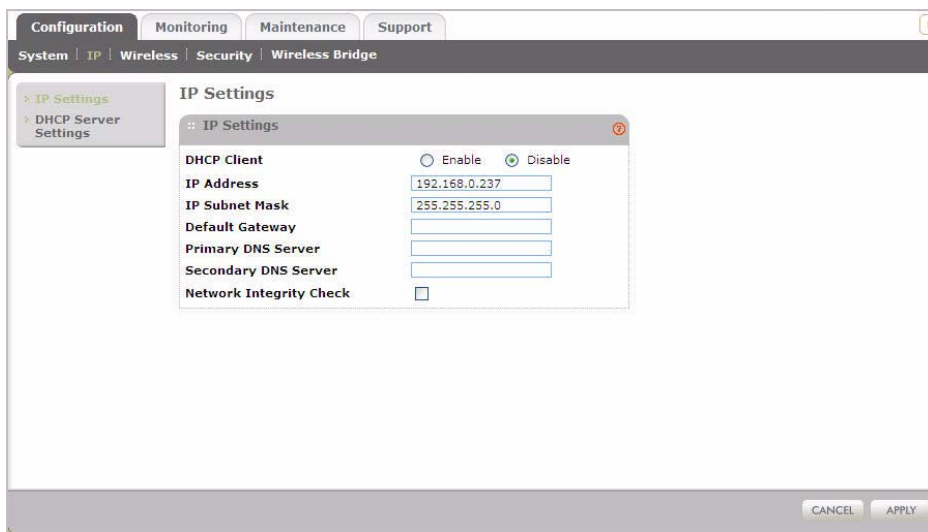


Figure 2-3 IP Settings

8. Configure the IP Address settings appropriate for your network. The default values are suitable for most users and situations. (See the online help or [“Setting Basic IP Options”](#) on [page 2-11](#) for more information about how to configure the settings on this screen.
9. Click **Apply**.

Configuring Time Settings

To configure your time settings:

1. Under the **Configuration** tab, select **System** from the main menu, select **Basic**, and then select **Time**. The Time screen displays, as shown in [Figure 2-4](#).

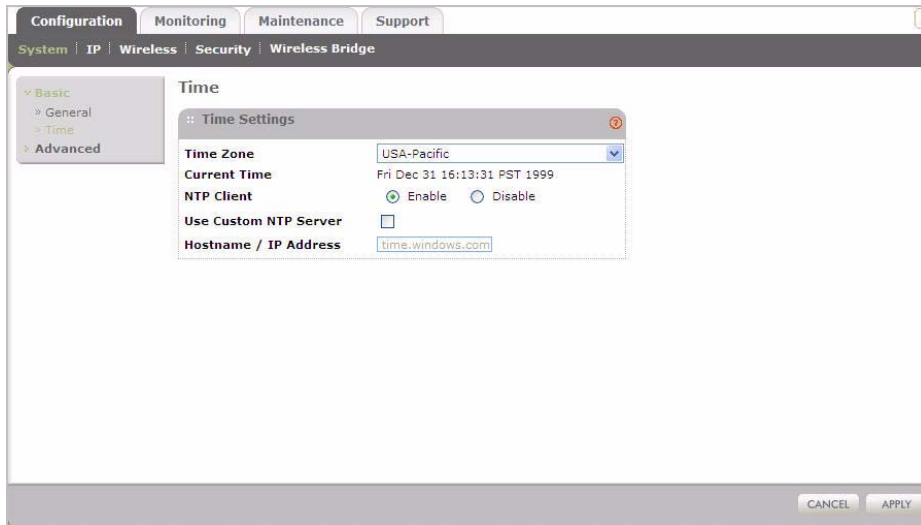


Figure 2-4 Timezone and system time related settings

2. Configure the following information:

- **Time Zone.** From the pull-down menu, select the local time zone for your Access Point from a list of all available time zones. The default is **USA-Pacific**.
- **NTP Client.** Enable NTP Client to synchronize the time of the access point with an NTP Server. The Default is Enabled.

	Note: You must have an Internet connection to get the current time.
-------------------------------------------------------------------------------------	----------------------------------------------------------------------------

- **Use Custom NTP Server.** Check the option if you have a custom NTP server. The default is Disabled.
- **Hostname / IP Address.** Enter the host name or the IP address of the custom NTP server.

3. Click **Apply**.

Configuring Wireless Access

To configure your wireless settings for 11b/bg/ng:

1. From the main menu under **Configuration**, select **Wireless**. The Wireless Settings screen displays, as shown in [Figure 2-5](#).
2. Enter the wireless settings for your area. See the online help or “[Wireless Settings](#)” on [page 2-13](#).
3. Click **Apply** to save your settings.

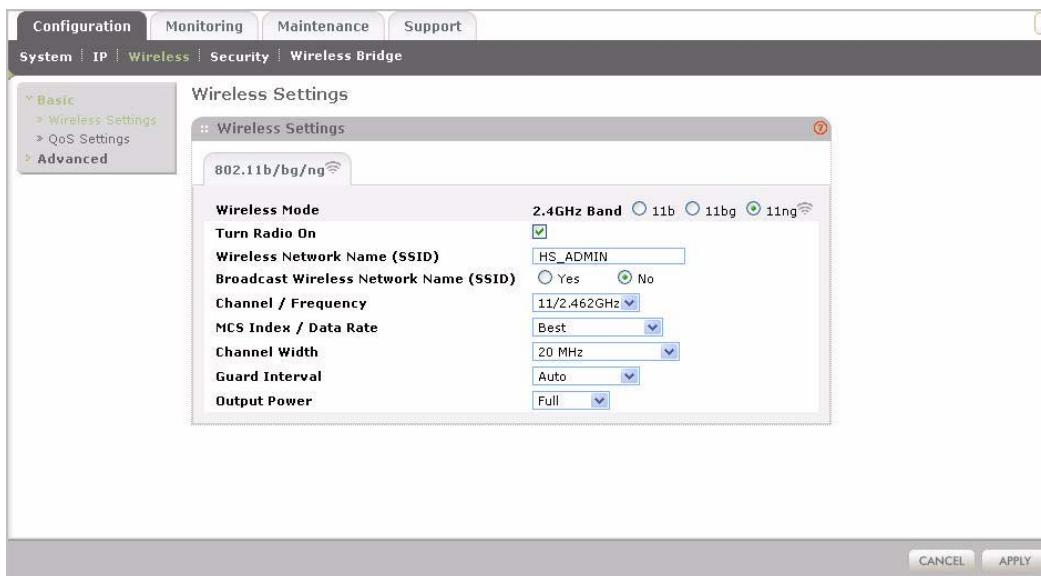


Figure 2-5 Basic Wireless Settings for 802.11b/bg/ng

When you have completed the setup steps, you can deploy the MaxR-3210 in your network. If needed, you can now reconfigure the computer you used in step 1 (from the Static IP) back to its original TCP/IP settings.

Deploying the MaxR-3210 Wireless Access Point

To deploy the MaxR-3210 Wireless Access Point:

1. Disconnect the MaxR-3210 and position it where it will be deployed. The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.
2. Lift the antennae on either side so that they are vertical.

3. Connect an Ethernet cable from your MaxR-3210 Wireless Access Point to a LAN port on your router, switch, or hub.



Note: By default, MaxR-3210 is set with the DHCP client disabled. If your network uses dynamic IP addresses, you must change this setting. To connect to the MaxR-3210 after the DHCP server on your network assigns it a new IP address, enter the Access Point name into your Web browser. The default Access Point name is aradaxxxxxx, where xxxxxx represents the last 6 bytes of the MAC address. The default name is printed on the bottom label of the MaxR-3210.

4. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The PWR, LAN, and Wireless LAN lights and should light up.

Verifying Wireless Connectivity

Using a computer with an 802.11b/bg/ng wireless adapter with the correct wireless settings needed to connect to the MaxR-3210 (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Mozilla Firefox or Internet Explorer to browse the Internet, or check for file and printer access on your network.

The default SSID for the 802.11b/bg/ng wireless mode is ARADA_11g. The SSID of any wireless access adapters must match the SSID configured in the MaxR-3210 Single Band Wireless-N Access Point. If they do not match, no wireless connection will be made.



Note: If you are unable to connect, see [Chapter 5, “Troubleshooting and Debugging.”](#)

Logging In Using the Default IP Address

After you install the MaxR-3210, log in to the Access Point to configure the basic settings and the wireless settings. The MaxR-3210 is set, by default, with the IP address of 192.168.0.237 with DHCP disabled.



Note: The computer you are using to connect to the MaxR-3210 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

To log in using the default IP Address:

1. Open a Web browser such as Internet Explorer or Mozilla Firefox.
2. Connect to the MaxR-3210 by entering its default address of **http://192.168.0.237** into your browser. The login screen displays. Enter **admin** for the user name and **password** for the password, both in lower case letters.

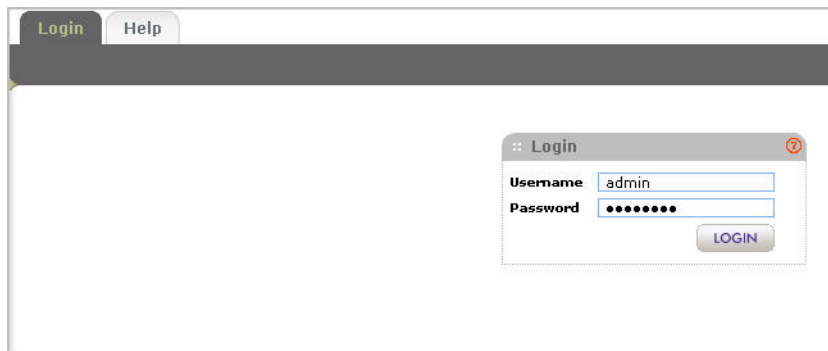


Figure 2-6 Connecting to the Access Point

3. Click **Login**.

Your Web browser should automatically find the MaxR-3210 Wireless Access Point and display the home screen.

Setting Basic IP Options

The basic IP settings for your Access Point are entered on this screen. Most of the default settings will work in most cases. However, if your Access Point is part of a more complex LAN network, then modify the settings to meet the requirements of your network based on the explanation of the various fields.

To configure the basic IP settings of your Access Point:

1. Under **Configuration**, select **IP**, and then IP Settings. The IP Settings screen displays as shown in [Figure 2-7](#) below.

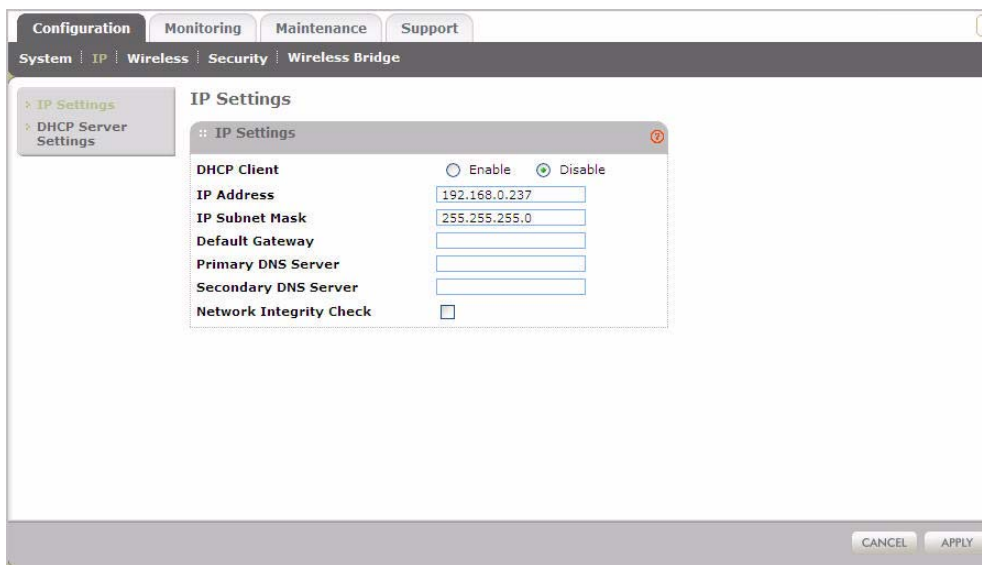


Figure 2-7 Basic IP options

2. Enter the IP Address fields of the MaxR-3210.
 - **DHCP Client.** By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you enable DHCP, the wireless access point will get its IP address, subnet mask and default gateway settings automatically from the DHCP server on your network when you connect the MaxR-3210 to your LAN.
 - **IP Address.** Enter the IP Address of your Access Point. The default IP address is **192.168.0.237**. To change it, enter an unused IP address from the address range used on your LAN; or enable DHCP.
 - **IP Subnet Mask.** The Access Point will automatically calculate the subnet mask based on the IP address that you assign. Otherwise, you can use 255.255.255.0 (the default) as the subnet mask.
 - **Default Gateway.** Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the Access Point is connected.
 - **Primary DNS Servers.** The MaxR-3210 will use this IP address as the primary Domain Name Server used by stations on your LAN.

- **Secondary DNS Servers.** The MaxR-3210 will use this IP address as the secondary Domain Name Server used by stations on your LAN.
- **Network Integrity Check.** Check this box to enable the MaxR-3210 to validate that the upstream link is active before allowing wireless associations. If you set this option you must ensure your default gateway is configured.

3. Click **Apply** to save your basic IP settings.

Wireless Settings

The following sections describe how to configure the wireless settings available in the 802.11b/bg/ng modes.

Configuring 802.11b/bg/ng Wireless Settings

To configure the wireless settings of your 802.11 b/bg/ng Access Point:

1. From main menu under **Configuration**, select **Wireless**. The Wireless Settings screen of your 802.11 b/bg/ng Access Point displays, as shown in [Figure 2-8](#) below.

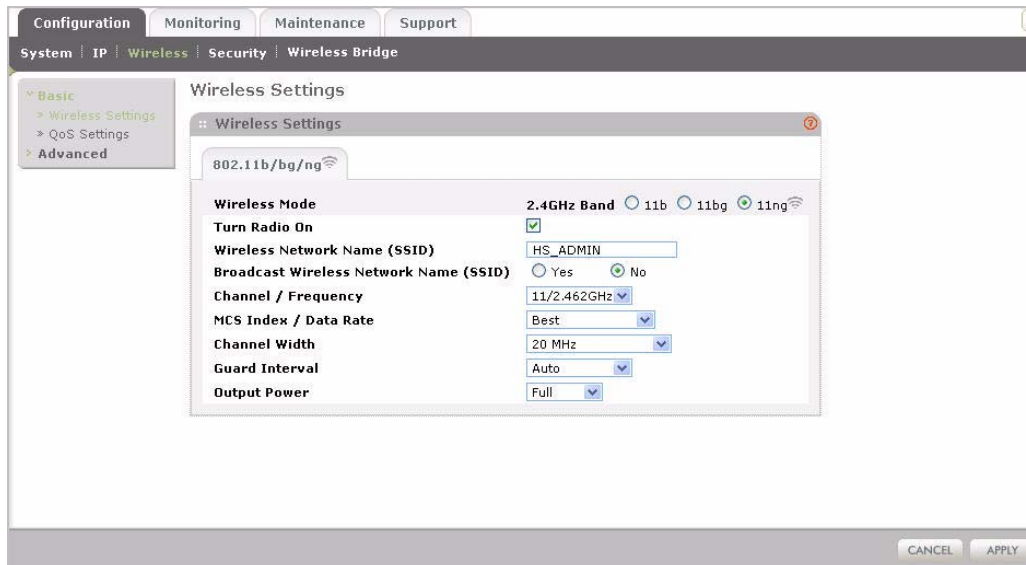



Figure 2-8 Configure wireless settings 802.11b/bg/ng

2. Configure the Wireless LAN settings based on the following field descriptions:

- **Wireless Mode.** Select the desired wireless operating mode. The default is 11ng. The options are:
 - **11b** – All 802.11b wireless stations can be used. (The 802.11g wireless stations can still be used if they can operate in 802.11b mode.)
 - **11bg** – Both 802.11b and 802.11g wireless stations can be supported.
 - **11ng** – All 11b, 11g, and 11ng wireless stations can be used. This is the default. If you select this option, then two additional options, Channel Width and Guard Interval, are displayed.

	Note: If you select one of these option and if other settings on this screen are disabled, then you must select the Turn Radio On radio button to enable available options on this screen.
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- **Turn Radio On.** On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Wireless Network Name (SSID).** This is the name of your wireless network. It is set to ARADA_11g for 802.11b/bg/ng.
- **Broadcast Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, Vista and Unix systems but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. Default is enabled.
- **Channel/Frequency.** From the pull-down menu, select the channel you wish to use on your wireless LAN. The wireless channel in use will be between 1 to 11 for US and Canada, 1 to 13 for Europe and Australia. The default is channel Auto.

It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may need to experiment with different channels to see which is the best. Alternatively, you can select the Auto channel option for the AP to intelligently pick the channel with least interference. When selecting or changing channels, some points to bear in mind:

- Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available

- If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).
- Wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.
- **MCS Index/Data Rate.** From the pull-down menu, select the available transmit data rate of the wireless network. Also, depending on the band selected, the set of rates will vary. The possible data rates supported are:
 - **Data Rates for Channel Width=20MHz and Guard Interval=short (400ms):** Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
 - **Data Rates for Channel Width=20MHz and Guard Interval=long (800ms):** Best, 6.5 Mbps, 13 Mbps, 19.5 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 58.5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps
 - **Data Rates for Channel Width=40MHz and Guard Interval=short:** Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
 - **Data Rates for Channel Width=40MHz and Guard Interval=long:** Best, 13.5 Mbps, 27 Mbps, 40.5 Mbps, 54 Mbps, 81 Mbps, 108Mbps, 121.5 Mbps, 135 Mbps, 27 Mbps, 54 Mbps, 81 Mbps, 108Mbps, 162 Mbps, 216 Mbps, 243 Mbps, 270 Mbps
- **Channel Width.** From the pull-down menu, select the desired channel width.
 - 20 MHz - This is the static, legacy mode. It gives the least throughput.
 - 40 MHz - This is the static, high-throughput mode. Legacy clients will not be able to connect in this mode.
 - 20/40 MHz - This is the dynamic, compatibility mode.
- **Guard Interval.** From the pull-down menu, select the desired guard interval. The guard interval protects from interference from other transmissions. The default is Auto.
- **Output Power.** From the pull-down menu, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more APs are close together and use the same channel frequency. The default is Full. (The transmit power may vary depending on the local regulatory regulations).

3. Click **Apply** to save your 802.11b/bg/ng wireless settings.

Configuring Basic QoS Settings

Wi-Fi Multimedia Support (WMM). Wireless Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the type of data.

Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.

To configure basic wireless QoS settings for 11b/bg/ng:

1. Under the **Configuration** tab, select **Wireless** from the main menu, select **Basic**, and then select **QoS Settings** from the left panel. The QoS Settings screen displays, as shown in [Figure 2-9](#).

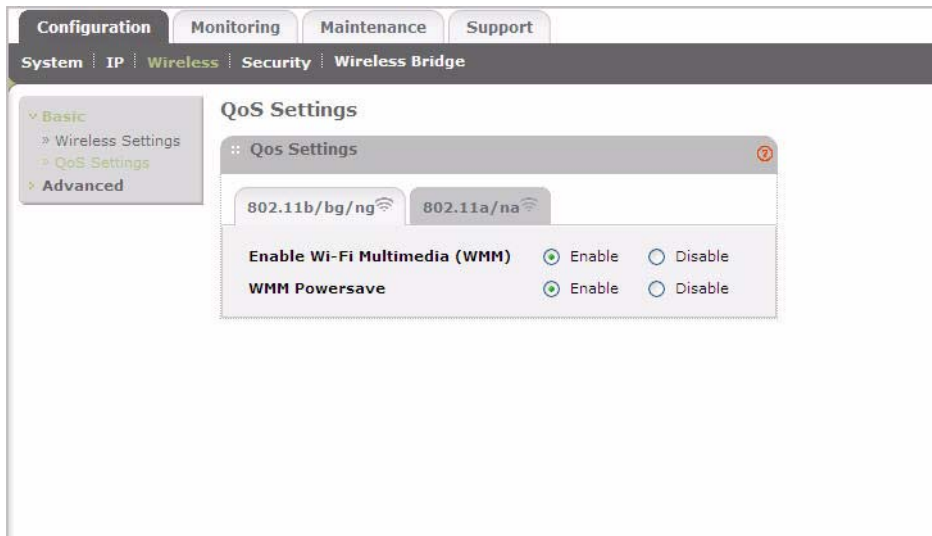


Figure 2-9 Basic QoS settings screen

2. Wi-Fi Multimedia (WMM) is enabled by default. Select the **Disable** radio button to disable WMM support.
3. WMM Power Save is enabled by default. Select the **Disable** radio button to disable WMM power save.
4. Click **Apply** to save your settings

Setting Up and Testing Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. From your Web browser, log in to the MaxR-3210 using its default address of **http://192.168.0.237**. Use the default user name of **admin** and default password of **password**— or use a new LAN address and password if you have set them up.
2. From the main menu under **Configuration**, select **System**.
3. Click **Apply** to save any changes.
4. Under the **Configuration** tab, select **Wireless** from the main menu. Ensure that the auto channel (default) feature is selected for your network. This feature selects a channel that has the least interference.

It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your Access Point.

5. Click **Apply** to save any changes.
6. Under the **Configuration** tab, select **Security** from the main menu. For initial configuration and testing, the Security Profile Settings for Profile 1 (the default profile) are set to Open System and the SSID for 11b/bg/ng set to ARADA_11g (see [“Understanding Security Profiles”](#) on page 2-18 to configure a profile).



Note: The SSID of any station must match the SSID you configured in the MaxR-3210 Wireless Access Point. If they do not match, you will not get a wireless connection to the MaxR-3210.

7. Click **Apply** to save any changes.
8. Configure and test your PCs for wireless connectivity

Program the wireless adapter of your PCs to have the same SSID that you configured in the MaxR-3210. Check that they have a wireless link and are able to obtain an IP address by DHCP from the MaxR-3210.



Note: If you are configuring the MaxR-3210 from a wireless computer and you change the SSID, channel, or Security Profile settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the new settings.

Once your PCs have basic wireless connectivity to the MaxR-3210, you can configure the advanced wireless security functions.

Understanding Security Profiles

Security Profiles let you configure unique security settings for each SSID. You can configure up to eight unique 802.11b/bg/ng wireless security profiles on the MaxR-3210 (see [Figure 2-10](#)).



Note: If you are using a RADIUS Server, configure the RADIUS settings first, as described in the [“Configuring WPA with RADIUS”](#) on page 2-29.

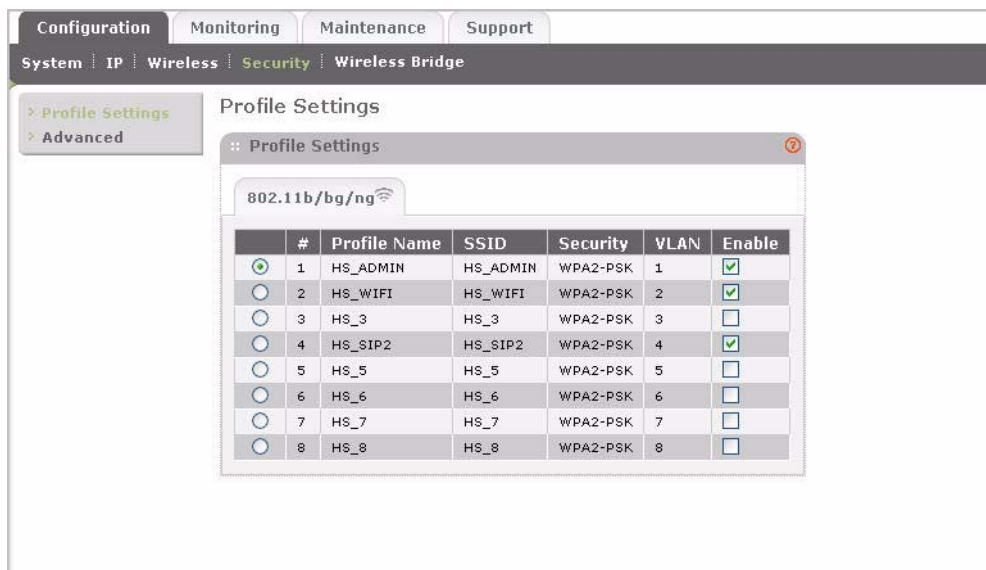


Figure 2-10 Security Profile Settings

An overview of the information that is required to set up a Security Profile follows—including a description of the Network Authentication choices that are available:

- **Profile Definition.** Configure the following settings:
 - **Security Profile Name.** Use a name that makes it easy to recognize the profile—and to tell profiles apart. (The default names are ARADA, ARADA-1, ARADA-2, and so on.) You can enter a value of up to 32 alphanumeric characters.



Note: Only the first profile is enabled by default. The rest of the profiles are disabled and must be enabled if configured.

- **Wireless Network Name (SSID).** This is the name of your wireless network. It is set to the default name of ARADA_11g for 802.11b/bg/ng.
- **Broadcast Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, Vista and Unix systems but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. Default is enabled.

- **Authentication Settings.** Configure the following settings:
 - **Network Authentication.** The MaxR-3210 Access Point is set by default as an open system with no authentication. When setting up Network Authentication, bear in mind the following:
 - If you are using Access Point mode, then all options are available. In bridge mode some options may be unavailable.
 - Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

You can configure the MaxR-3210 to use the types of network authentication shown in the table below.

Table 2-1. Network Authentication Types

Type ^a	Description
Open System	Can be used with WEP encryption or no encryption.
Shared Key	You must use WEP encryption and enter at least one shared key.
Legacy 802.1x	You must configure the RADIUS Server Settings to use this option.
WPA with RADIUS	You must configure the RADIUS Server Settings to use this option.
WPA2 with RADIUS (WPA2 is a later version of WPA.)	Only select this if all clients support WPA2. If selected, you must use AES encryption and configure the RADIUS Server Settings.
WPA and WPA2 with RADIUS	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and configure the RADIUS Server Settings.
WPA-PSK	You must use TKIP or TKIP + AES encryption and enter the WPA passphrase (Network key).
WPA2-PSK (WPA2 is a later version of WPA)	Only select this if all clients support WPA2. If selected, you must use AES or TKIP + AES encryption and enter the WPA passphrase (Network key).
WPA-PSK and WPA2-PSK	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and enter the WPA passphrase (Network key).

a. All options are available if using Access Point mode. In bridge modes some options may be unavailable.

- **Data Encryption.** The available options depend on the Network Authentication setting selected (see [Table 2-1](#) above); otherwise, the default is None. The Data Encryption settings are explained in the table below:

Table 2-2. Data Encryption Settings

Data Encryption Type	Description
None	No encryption is used.
64 bits WEP	Standard WEP encryption, using 40/64 bit encryption.
128 bits WEP	Standard WEP encryption, using 104/128 bit encryption.
152 bits WEP	Proprietary mode that will only work with other wireless devices that support this mode.
TKIP	This is the standard encryption method used with WPA and WPA2.
AES	This is the standard encryption method for WPA2.
TKIP + AES	This setting supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

- Use of Passphrases and Keys are explained below:
 - **Passphrase.** To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.
 - **Key 1, Key 2, Key 3, Key 4.** If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
 - **WPA Preshared Key Passphrase.** If using WPA-PSK or WPA2-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 64 characters in length.
- **Wireless Client Security Separation.** If enabled, the associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.) The default is Disabled.
- **VLAN ID.** If the hubs/switches on your LAN support the VLAN (802.1Q) standard and this feature has been enabled, the default VLAN ID for MaxR-3210 will be associated with each profile. The default Profile VLAN ID must match the IDs used by other network devices.

SSID and WEP/WPA Settings Setup Form

802.11b/bg/ng Configuration

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID:** The Service Set Identification (SSID) identifies the wireless local area network. ARADA_11g is the default MaxR-3210 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

Note: The SSID in the Access Point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:

- **Authentication:**

Circle one: Open System or Shared Key. (Choose Shared Key for more security.)

Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the MaxR-3210.

- **WEP Encryption Keys.**

Circle one: 64, 128, or 152 bits. (Enter all four keys for the Key Size chosen.)

Key 1: _____

Key 2: _____

Key 3: _____

Key 4: _____

- **WPA-PSK (Preshared Key)**

Record the WPA-PSK key. Key: _____

- **WPA RADIUS Settings.** For WPA, record the following settings for the primary and secondary RADIUS servers:

Server Name/IP Address: Primary _____ Secondary _____

Port: _____

Shared Secret: _____

Use the procedures described in the following sections to configure the MaxR-3210. Store this information in a safe place.

Configuring the RADIUS Server Settings

You can setup or modify the RADIUS Server settings to compliment Network Authentication security options. The RADIUS Server must be used with Legacy 802.1x, and can be used with WPA and WPA2 Network Authentication. When using a RADIUS Server, the RADIUS Server settings must be configured before completing the Network Authentication security profile (see [“Configuring WPA with RADIUS” on page 2-29](#), [“Configuring WPA2 with RADIUS” on page 2-31](#), or [“Configuring WPA and WPA2 with RADIUS” on page 2-32](#) for specifics on implementing these security options).



Note: The RADIUS Server Settings apply to all profiles. They only need to be configured once per Access Point.

To set up or modify the RADIUS Server Settings:

1. From your Web browser, log in to the MaxR-3210 using the default LAN address of **http://192.168.0.237**, user name **admin** and password **password**, or use the LAN address and password that you set up.
2. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the left panel, and then select **RADIUS Server Settings**. The RADIUS Server Settings screen displays, as shown in [Figure 2-11](#).

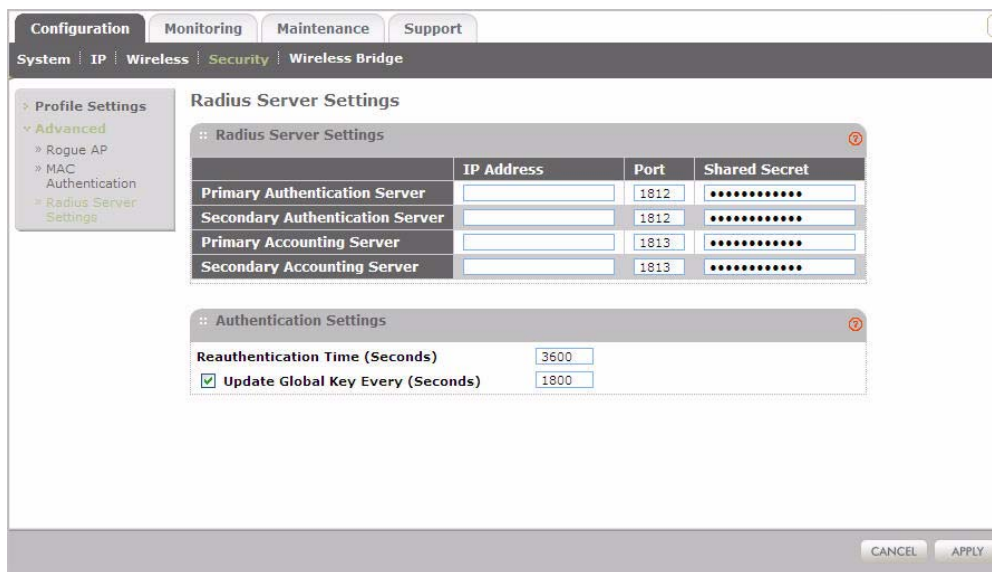


Figure 2-11 RADIUS server settings

- Enter the following RADIUS Server settings:
 - Authentication Server.** This configuration is required for authentication using a RADIUS Server. The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use, if the Primary RADIUS Server fails.
 - IP Address.** The IP address of the RADIUS Server.
 - Port Number.** The port number of the RADIUS Server. The default is 1812.
 - Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).
 - Accounting Server.** This configuration is required for accounting using a RADIUS Server. The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails.
 - IP Address.** The IP address of the RADIUS Server.
 - Port Number.** Port number of the RADIUS Server. The default: 1813

- **Shared Secret.** This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client).

4. Click **Apply** to save your settings.

Setting up a Security Profile

The MaxR-3210 allows you to set up eight different security profiles for 802.11b/bg/ng. Each profile can be configured with a different security option for network authentication.



Note: If you are using a RADIUS Server, configure the RADIUS settings first, as described in the [“Configuring the RADIUS Server Settings”](#) on page 2-23.

Configuration | Monitoring | Maintenance | Support

System | IP | Wireless | **Security** | Wireless Bridge

> Profile Settings
> Advanced

Profile Settings

802.11b/bg/ng

	#	Profile Name	SSID	Security	VLAN	Enable
<input checked="" type="radio"/>	1	HS_ADMIN	HS_ADMIN	WPA2-PSK	1	<input checked="" type="checkbox"/>
<input type="radio"/>	2	HS_WIFI	HS_WIFI	WPA2-PSK	2	<input checked="" type="checkbox"/>
<input type="radio"/>	3	HS_3	HS_3	WPA2-PSK	3	<input type="checkbox"/>
<input type="radio"/>	4	HS_SIP2	HS_SIP2	WPA2-PSK	4	<input checked="" type="checkbox"/>
<input type="radio"/>	5	HS_5	HS_5	WPA2-PSK	5	<input type="checkbox"/>
<input type="radio"/>	6	HS_6	HS_6	WPA2-PSK	6	<input type="checkbox"/>
<input type="radio"/>	7	HS_7	HS_7	WPA2-PSK	7	<input type="checkbox"/>
<input type="radio"/>	8	HS_8	HS_8	WPA2-PSK	8	<input type="checkbox"/>

Figure 2-12 Security profile settings

To configure a Security Profile:

1. From your Web browser, log in to the MaxR-3210 using the default LAN address of **http://192.168.0.237**, user name **admin** and password **password**, or use the LAN address and password that you set up.
2. Under the **Configuration** tab, select **Security** from the main menu. The screen for the Profile Settings displays as shown in [Figure 2-12](#) above.
3. Select the checkbox of the profile you want to modify and click **Edit**. The Security Profile Configuration screen for the selected profile displays (see [Figure 2-13](#)).

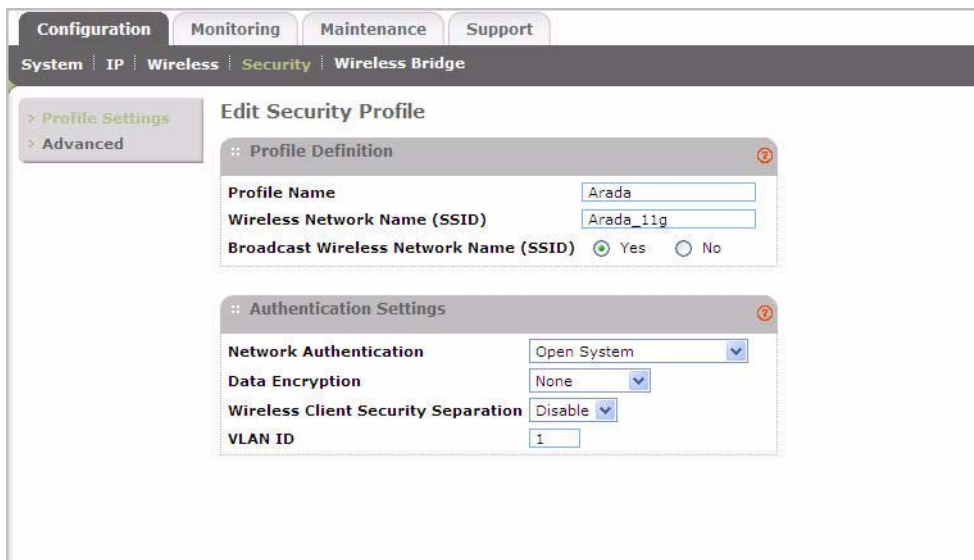


Figure 2-13 Edit a security profile

4. Give your profile a meaningful name so that you can remember it later.
5. The Wireless Network Name (SSID) is set by default to identify it as ARADA_11g.
6. Enable or disable the Broadcast Wireless Network Name (SSID). It is enabled by default. (If it is broadcast, it can be easily detected by other clients.)
7. From the **Network Authentication** pull-down menu, select the Network Authentication Type you want to use for this profile:
 - To configure WEP encryption for Open Systems or Shared Key, see [“Configuring WEP” on page 2-27](#).

- To configure WPA with RADIUS, see [“Configuring WPA with RADIUS” on page 2-29.](#)
 - To configure WPA2 with RADIUS, see [“Configuring WPA2 with RADIUS” on page 2-31.](#)
 - To configure WPA and WPA2 with RADIUS, see [“Configuring WPA and WPA2 with RADIUS” on page 2-32.](#)
 - To configure WPA-PSK, see [“Configuring WPA-PSK” on page 2-34.](#)
 - To configure WPA2-PSK, see [“Configuring WPA2-PSK” on page 2-35.](#)
 - To configure WPA-PSK and WPA2-PSK, see [“Configuring WPA-PSK and WPA2-PSK” on page 2-36.](#)
8. **Wireless Client Security Separation** is disabled by default. If enabled, the associated wireless clients will not be able to communicate with each other.
 9. If the hubs/switches on your LAN support the VLAN (802.1Q) standard and this feature has been enabled, the default **VLAN ID** for MaxR-3210 will be associated with each profile. The default Profile VLAN ID must match the IDs used by other network devices.
 10. Click **Apply** to save your Security Profile settings.
 11. Click **Back**. Your new settings will appear in the Security Profiles table identified by the Profile Name of the profile. A VLAN ID will also be assigned to your profile.



Note: Security Profiles that share the same type of network authentication need not share the same passphrase or keys.

To enable your Security Profile:

1. Check the radio box in the **Enable** column next to your profile.
2. Click **Apply**. Your Security Profile will be enabled. If you enabled VLAN 802.1Q, your VLAN Profile will also be enabled. (See [“Setting Basic IP Options” on page 2-11](#) to enable VLAN 802.1Q.)

Configuring WEP

To configure WEP data encryption:

1. From the **Network Authentication** drop-down menu, choose either **Open System** or **Shared Key** authentication.

2. From the Data Encryption drop-down menu, select encryption strength (64 bits, 128 bits, or 152 bits).
3. You manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network. Choose either:
 - Automatic – Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
 - Manual – Enter the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit, 26 digits for 128-bit and 32 digits for 152-bit (any combination of 0-9, a-f, or A-F)
Select which of the four keys will be the default.

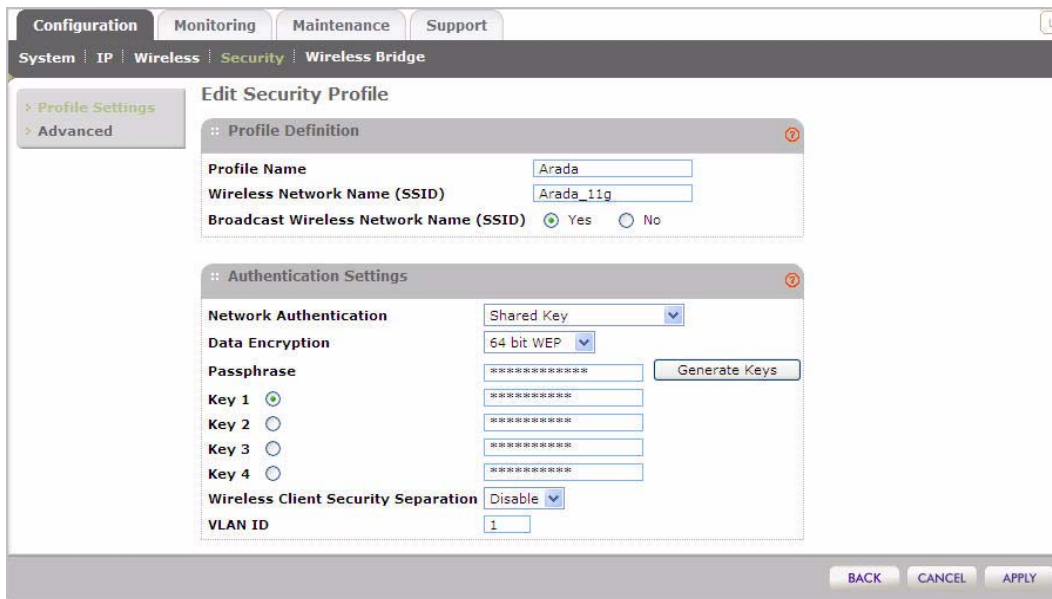


Figure 2-14 Configure WEP Shared Key

4. Select the key to be used as the default key by checking the radio box. (Data transmissions are always encrypted using the default key.)
5. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.)
6. Click **Apply** to save your settings.



Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the Access Point from a wired computer to make any further changes.

Configuring WPA with RADIUS

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA, follow these steps:

1. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the left-hand menu, and then select **RADIUS Server Settings**. The RADIUS Server Settings screen displays.
2. Enter the RADIUS Server Settings as shown in [“Configuring the RADIUS Server Settings” on page 2-23](#).
3. Click **Apply** to save your RADIUS Server settings.

4. Under the **Configuration** tab, select **Security** from the main menu. The screen for Profile Settings displays. When the Security Profile screen displays, check the checkbox of the Security Profile you want to modify and click **Edit**.

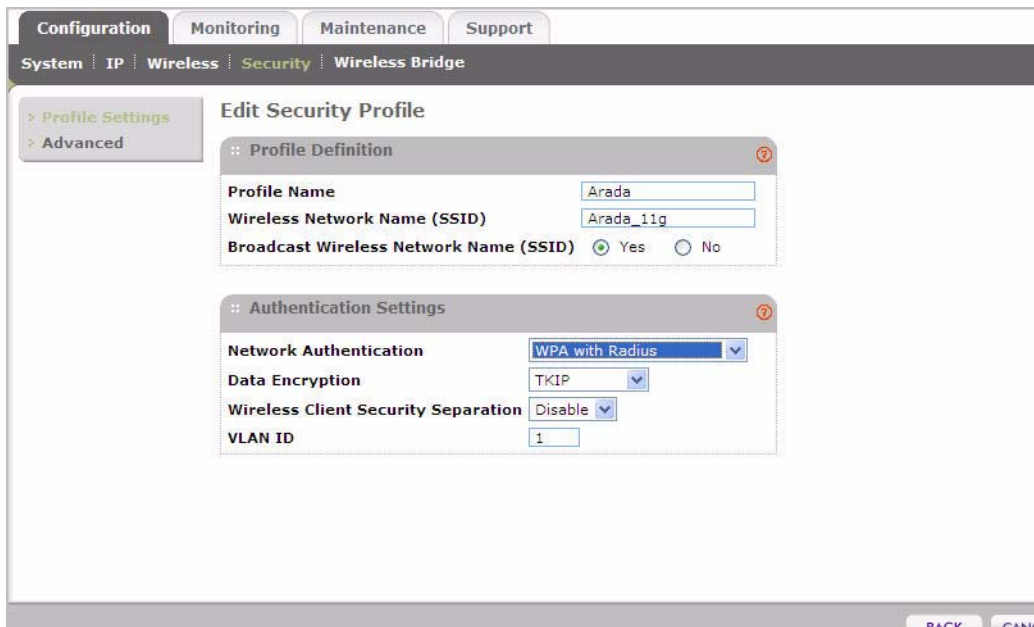


Figure 2-15 Configure WPA with RADIUS

5. Choose **WPA with RADIUS** from the from the Network Authentication drop-down menu. Data Encryption will be set to TKIP by default.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
7. Click **Apply** to save your settings.

Configuring WPA2 with RADIUS

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

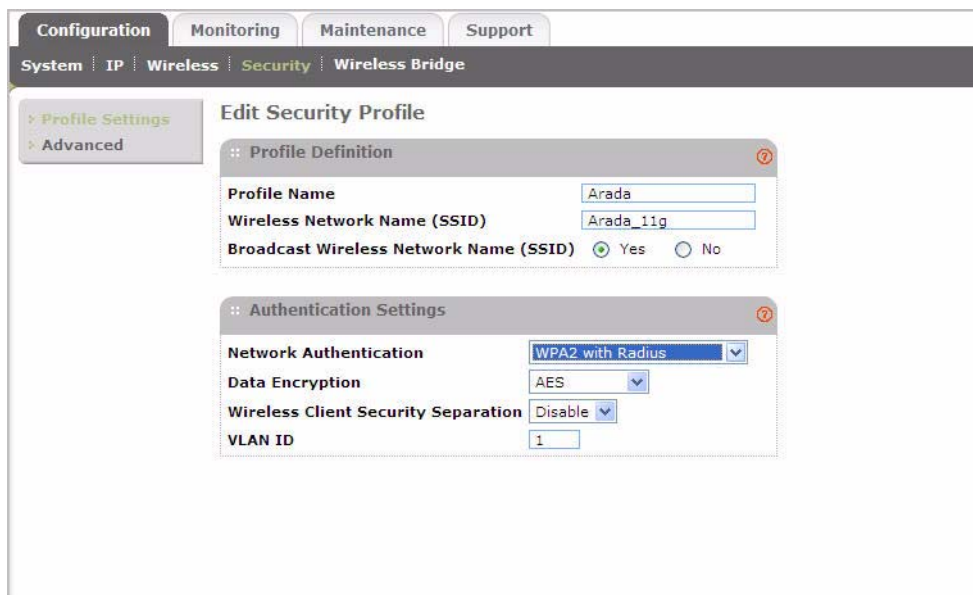


Figure 2-16 Configure WPA2 with RADIUS

To configure WPA2 with RADIUS:

1. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the left panel, and then select **RADIUS Server Settings**. The RADIUS Server Settings screen displays.
2. Enter the RADIUS settings as shown in [“Configuring the RADIUS Server Settings” on page 2-23](#).
3. Click **Apply** to save your RADIUS settings.
4. Under the **Configuration** tab, select **Security** from the main menu. The screen for Profile Settings displays. When the Security Profile screen displays, check the checkbox of the Security Profile you want to modify and click **Edit**.

5. From the Network Authentication drop-down menu, select WPA2 with RADIUS from the list. By default, Data Encryption will be set to AES.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.)
7. Click **Apply** to save your settings.

Configuring WPA and WPA2 with RADIUS

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3, or above, do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.
- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.

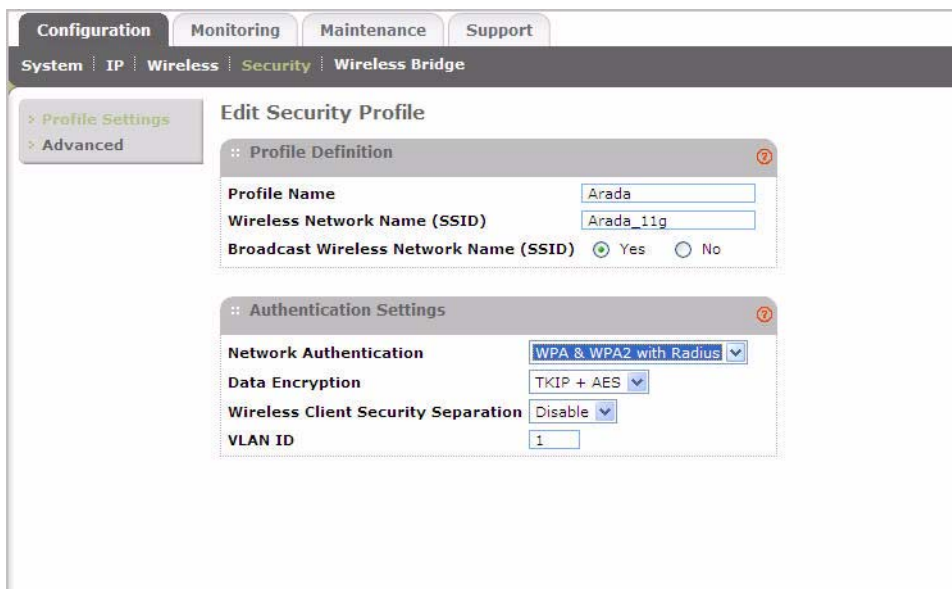


Figure 2-17 Configure WPA and WPA2 with RADIUS

To configure WPA and WPA2 with RADIUS:

1. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the left panel, and then select **RADIUS Server Settings**. The RADIUS Server Settings screen displays.
2. Enter the RADIUS settings as shown in [“Configuring the RADIUS Server Settings” on page 2-23](#).
3. Click **Apply** to save your RADIUS settings
4. Under the **Configuration** tab, select **Security** from the main menu. The screen for Profile Settings displays. When the Security Profile screen displays, check the checkbox of the Security Profile you want to modify and click **Edit**.
5. From the **Network Authentication** drop-down menu, select **WPA & WPA2 with RADIUS** from the list. By default, **Data Encryption** will be set to **TKIP+AES**.
6. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.
7. Click **Apply** to save your settings.

Configuring WPA-PSK

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

The screenshot shows a web-based configuration interface for an access point. The main menu at the top includes 'Configuration', 'Monitoring', 'Maintenance', and 'Support'. The current path is 'System | IP | Wireless | Security | Wireless Bridge'. The left sidebar shows 'Profile Settings' and 'Advanced' options. The main content area is titled 'Edit Security Profile' and contains two sections: 'Profile Definition' and 'Authentication Settings'. In the 'Profile Definition' section, the 'Profile Name' is 'Arada', the 'Wireless Network Name (SSID)' is 'Arada_11g', and 'Broadcast Wireless Network Name (SSID)' is set to 'Yes'. In the 'Authentication Settings' section, 'Network Authentication' is 'WPA-PSK', 'Data Encryption' is 'TKIP + AES', 'WPA Passphrase (Network Key)' is masked with asterisks, 'Wireless Client Security Separation' is 'Disable', and 'VLAN ID' is '1'. At the bottom right, there are 'BACK', 'CANCEL', and 'APPLY' buttons.

Profile Definition	
Profile Name	Arada
Wireless Network Name (SSID)	Arada_11g
Broadcast Wireless Network Name (SSID)	<input checked="" type="radio"/> Yes <input type="radio"/> No

Authentication Settings	
Network Authentication	WPA-PSK
Data Encryption	TKIP + AES
WPA Passphrase (Network Key)	*****
Wireless Client Security Separation	Disable
VLAN ID	1

Figure 2-18 Configure WPA-PSK

To configure WPA-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA-PSK**. By default, **Data Encryption** will be set to **TKIP**.
2. Enter the preshared key passphrase (Network Key).
3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations).
4. Click **Apply** to save your settings.

Configuring WPA2-PSK

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

The screenshot shows a web-based configuration interface for an access point. The main menu at the top includes 'Configuration', 'Monitoring', 'Maintenance', and 'Support'. The current page is 'Edit Security Profile' under the 'Security' section. The profile name is 'Arada' and the SSID is 'Arada_11g'. The 'Authentication Settings' section is expanded, showing 'Network Authentication' set to 'WPA2-PSK', 'Data Encryption' set to 'TKIP + AES', 'WPA Passphrase (Network Key)' masked with asterisks, 'Wireless Client Security Separation' set to 'Disable', and 'VLAN ID' set to '1'. At the bottom right, there are buttons for 'BACK', 'CANCEL', and 'APPLY'.

Figure 2-19 Configure WPA2-PSK

To configure WPA2-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA2-PSK** from the list. By default, **Data Encryption** will be set to **AES**.
2. Enter the preshared key passphrase (Network Key).
3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations).
4. Click **Apply** to save your settings.

Configuring WPA-PSK and WPA2-PSK

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.
- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings

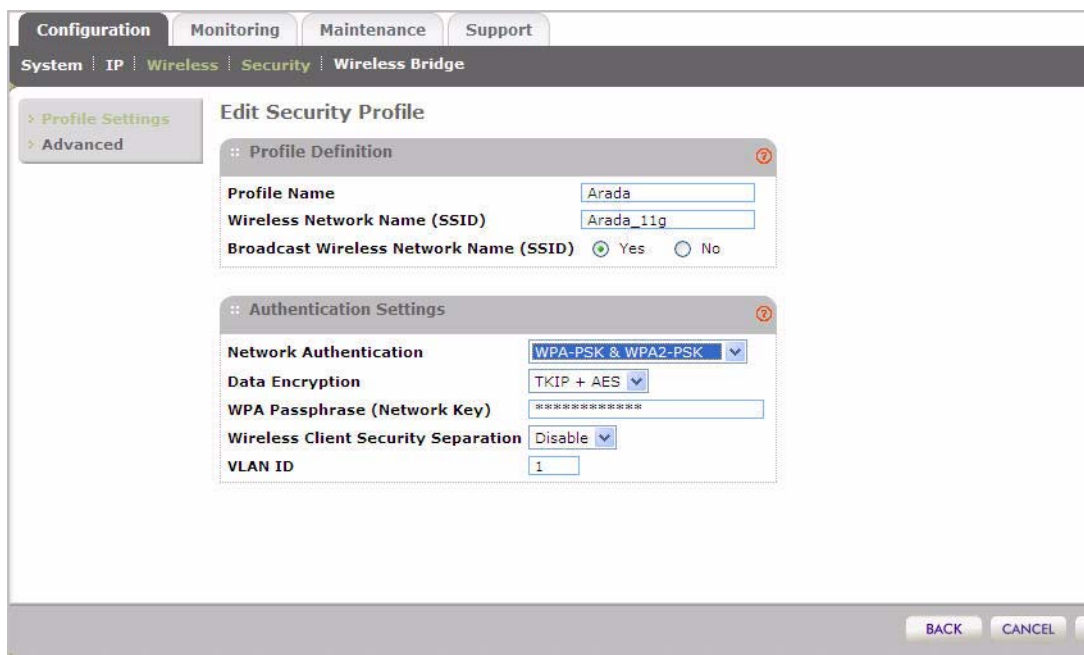


Figure 2-20 Configure WPA-PSK and WPA2-PSK

To configure WPA-PSK and WPA2-PSK:

1. From the **Network Authentication** drop-down menu, select **WPA-PSK & WPA2-PSK**. By default, **Data Encryption** will be set to **TKIP+AES**.
2. Enter the WPA Passphrase (Network Key).
3. **Wireless Client Security Separation** is disabled by default. If enabled, associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations).
4. Click **Apply** to save your settings.

Restricting Wireless Access by MAC Address

The optional Access Control window lets you block the network access privilege of any specified stations through the MaxR-3210 Wireless Access Point. When you enable access control, the access point only accepts connections from clients on the selected access control list. This provides an additional layer of security.



Note: If configuring the MaxR-3210 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click **Apply**. You must then access the Access Point from a wired computer or from a wireless computer that is on the access control list to make any further changes.

To restrict access based on MAC addresses:

1. Log in to the MaxR-3210 using the default address of **http://192.168.0.237**, user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Under the **Configuration** tab, select **Security** on the main menu, select **Advanced** from the left panel, and then select **MAC Authentication**. The MAC Authentication screen displays.

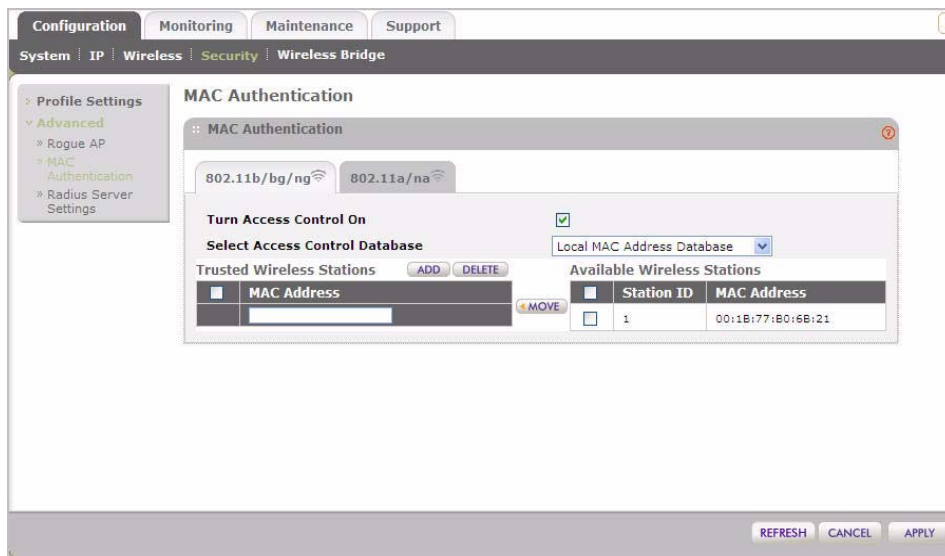


Figure 2-21 Configure MAC authentication

3. Check the **Turn Access Control On** radio box to enable Access Control feature.
4. Select the desired Access Control Database options. The options are:
 - **Local MAC Address Database** – The Access Point will use the local MAC address table for Access Control. This is the default.
 - **RADIUS MAC Address Database** – The Access Point will use the MAC address table located on the external RADIUS server on the LAN for Access Control. If you choose this database, you must configure the RADIUS Server Settings first (see [“Configuring the RADIUS Server Settings”](#) on page 2-23).
5. The **Trusted Wireless Stations** list shows any wireless stations you have entered. If you have not entered any wireless stations this list will be empty. To delete an existing entry, select it and then click **Delete**.
6. Click Refresh to refresh the **Available Wireless Stations** list found in your area.
7. Select the stations from the list of **Available Wireless Stations** found in your area, or enter the MAC address of a station to add a new station manually. (You can usually find the MAC address printed on the bottom of the wireless adapter.)

8. Click **Add** to add the wireless device to the **Trusted Wireless Stations** list. Repeat these steps for each additional device you want to add to the list.
9. Click **Apply** to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the MaxR-3210.

Chapter 3

Management

This chapter describes how to use the management features of your MaxR-3210 Single Band Wireless-N Access Point. To access these features, connect to the MaxR-3210 as described in [“Logging In Using the Default IP Address”](#) on page 2-10. Then select the category under either the **Monitoring** or **Maintenance** headings in the main menu of the browser interface.

This chapter contains the following sections:

1. [“Remote Management](#)
2. [“Remote Console](#)
3. [“Upgrading the Wireless Access Point Software](#)
4. [“Configuration File Management](#)
5. [“Restoring the MaxR-3210 to the Factory Default Settings](#)
6. [“Changing the Administrator Password](#)
7. [“Enabling the SysLog Server](#)
8. [“Using Activity Log Information](#)
9. [“Viewing General Summary Information](#)
10. [“Viewing Network Traffic Statistics](#)
11. [“Viewing Available Wireless Station Statistics](#)
12. [“Enabling Rogue AP Detection](#)
13. [“Viewing Rogue AP Statistics](#)
14. [“Packet Capture](#)

Remote Management

Both the SNMP and Remote Console are enabled by default, which allows for remote management of the MaxR-3210 from a client running SNMP management software, as well as from a secure Telnet console.

To set up an SNMP management interface:

1. Under the **Maintenance** tab, select **Remote Management**, and then select **SNMP** from the left sidebar. The SNMP screen displays, as shown in [Figure 3-1](#) below:

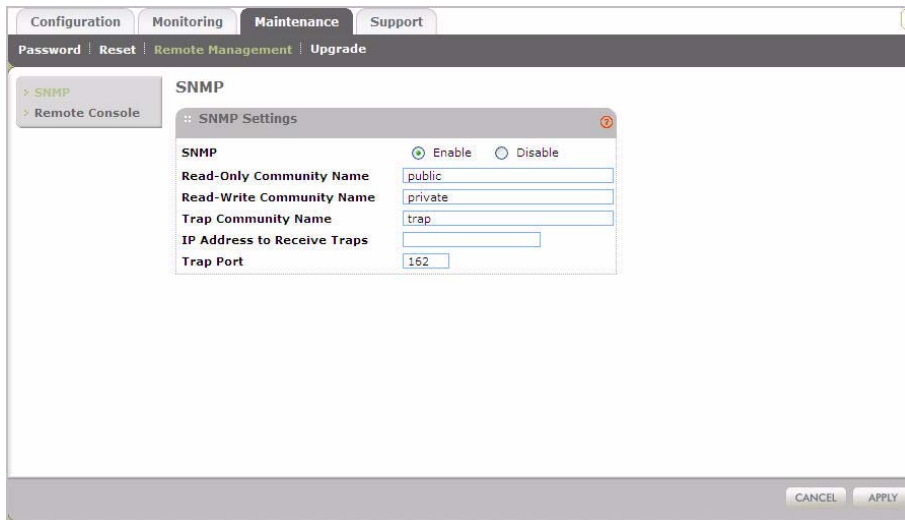


Figure 3-1 Configure SNMP settings

2. Enter the following information in the SNMP fields:
 - **SNMP:** Enable SNMP to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point via SNMPv1/v2 protocol.
 - **Read-Only Community Name:** The community string to allow the SNMP manager to read the wireless access point's MIB objects. The default is Public.
 - **Read-Write Community Name:** The community string to allow the SNMP manager to read and write the wireless access point's MIB objects. The default is Private.
 - **Trap Community Name:** The community string to allow the SNMP manager to send traps. The default is trap.
 - **IP address to Receive Traps:** The IP address of the SNMP manager to receive traps sent from the wireless access point.
 - **Trap Port:** The port number on which the SNMP Manager will receive traps. The default is 162/UDP.

Remote Console

The Remote Console configuration features are located under the **Maintenance** tab, **Remote Management**, and then under **Remote Console**. Enter the following information in the Remote Console screen, as shown in [Figure 3-2](#):

- **Secure Shell (SSH)**: If set to Enable, the Wireless Access Point will only allow remote access via Secure Shell and Secure Telnet. The default is **Enable**.
- **Telnet**: If set to Enable, the Wireless Access Point will only allow remote access via Telnet. The default is **Disable**.

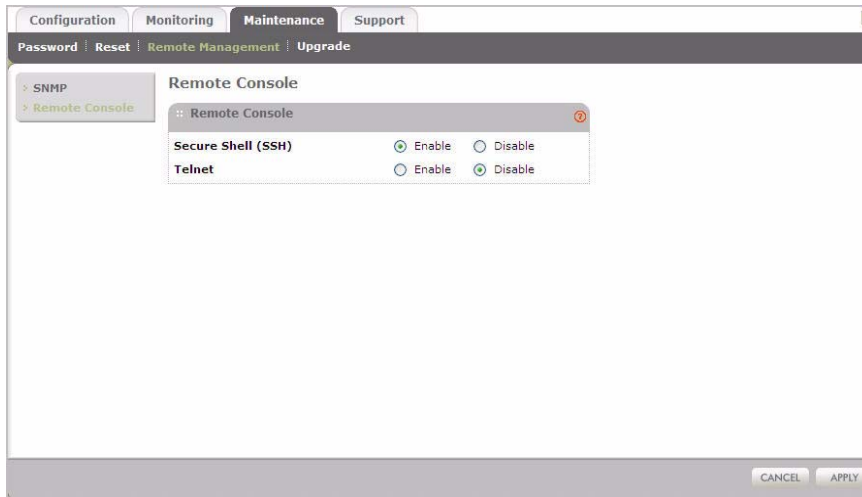


Figure 3-2 Configure Remote Console

Using the Secure Telnet Interface

The MaxR-3210 includes a secure Telnet command line interface (CLI). You can access the CLI from a secure Telnet client over the Ethernet port or over the serial console port.



Note: You must use a secure Telnet client such as Absolute Telnet. Also, when you configure the client, use the SSH1, 3DES option. If you use the Telnet client to connect over the Ethernet port, use the IP address of the MaxR-3210 as the host name.

To use the CLI from a Console Port:

1. Using the null-modem cable, connect a VT100/ANSI terminal or a workstation to the port labeled Console.

If you attached a PC, Apple Macintosh, or UNIX workstation, start a secure terminal-emulation program.

2. Configure the terminal-emulation program to use the following settings:
 - Baud rate: 9600 bps
 - Data bits: 8
 - Parity: none
 - Stop bit: 1
 - Flow control: none

These settings appear below the connector on the back panel.

3. Press **Enter**. The screen shown below in [Figure 3-3](#) should appear.

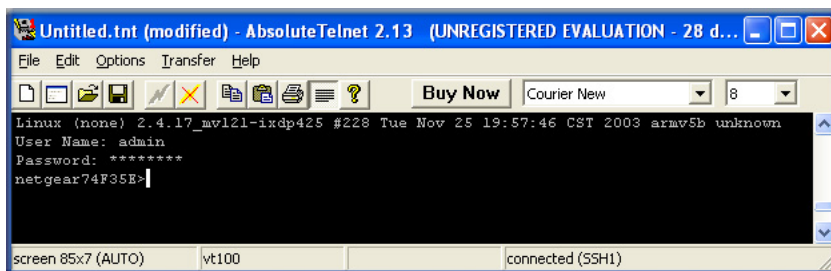


Figure 3-3

4. Enter the login name and password (**admin** and **password** are the defaults).

After successful login, the *<Access Point Name>* prompt should appear. In this example, the prompt is *arada74F35E*.

5. Enter `help` to display the CLI command help.

CLI Commands

The CLI commands are listed in [Appendix B, “Command Line Reference.”](#)

Upgrading the Wireless Access Point Software

The software of the MaxR-3210 Wireless Access Point is stored in FLASH memory, and can be upgraded as new software is released by Arada Systems. Upgrade files can be downloaded from Arada Systems' support web site.. The upgrade file can be sent to the wireless access point using your browser.



Note: The Web browser used to upload new firmware into the MaxR-3210 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above or Mozilla 1.5 or above.

You cannot perform the software upgrade from a computer that is connected to the MaxR-3210 Wireless Access Point with a wireless link. You must use a computer that is connected to the MaxR-3210 Wireless Access Point with a Ethernet cable.



Warning: When uploading software to the MaxR-3210 Wireless Access Point, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, and render the MaxR-3210 completely inoperable.

The Web browser used to upload new firmware into the MaxR-3210 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Firefox 1.5 or above.

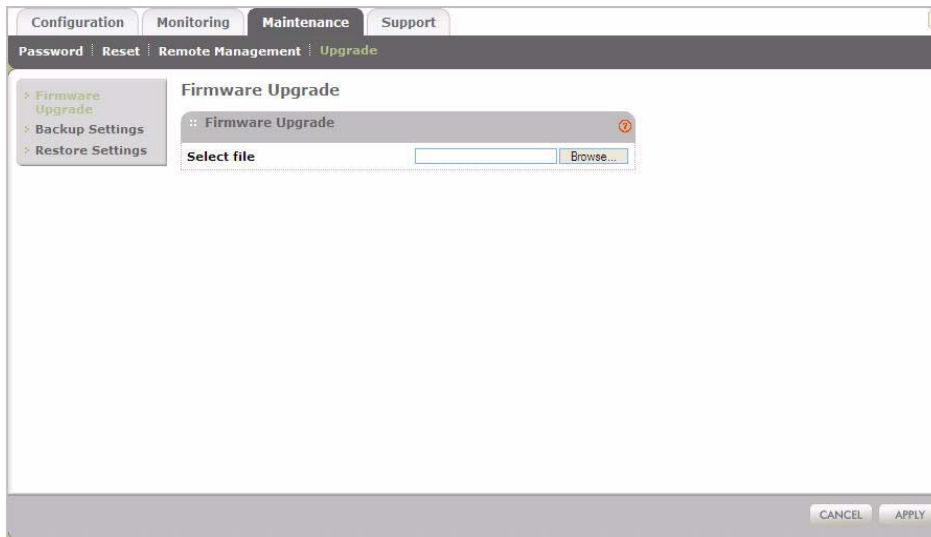


Figure 3-4 Firmware upgrade screen

To upgrade the MaxR-3210 firmware:

1. Download the new software file from the Arada Systems' support website, save it to your hard disk.
2. Under the **Maintenance** tab, select **Upgrade** from the main menu, and then select **Firmware Upgrade**. The Firmware Upgrade screen displays as shown in [Figure 3-4](#) above.
3. Click **Browse** and browse to the location of the upgrade file.
4. Click **Apply**.

When the upload completes, your Access Point will automatically restart. The upgrade process typically takes about 2 minutes.

Configuration File Management

The MaxR-3210 Wireless Access Point settings are stored in the Access Point in a configuration file. This file can be saved (backed up) to a user's computer, retrieved (restored) from the user's computer, or cleared to factory default settings.

Saving Your Configuration Settings

To backup your configuration settings:

Under the **Maintenance** tab on the main menu , select **Upgrade**, then select **Backup Settings** from the left sidebar to back up your current settings. The following screen displays:

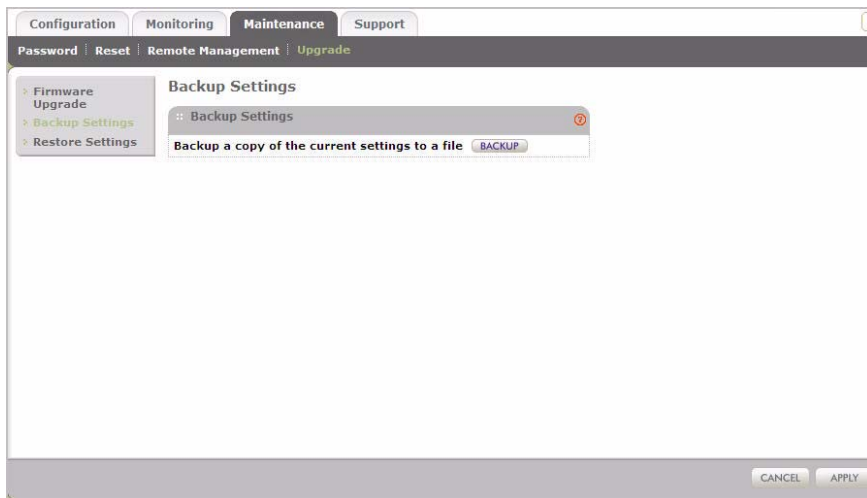


Figure 3-5 Backup configuration settings

1. Click **Backup**. Your browser will extract the configuration settings from the Access Point and prompt you for a location on your computer to store the file.
2. Give the file a meaningful name, such as MaxR-3210.cfg, and click **Save**.

Restoring Saved Settings

To restore your settings from a saved configuration file:

Under the **Maintenance** tab on the main menu, select **Upgrade**, then select **Restore Settings** from the sidebar to back up your current settings. The following screen displays:

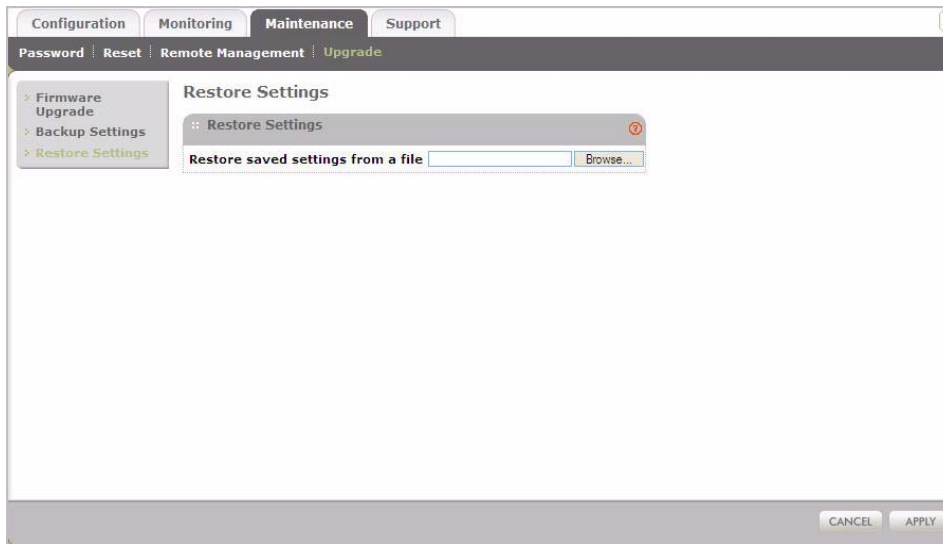


Figure 3-6 Restore Configuration settings from file

1. Enter the full path to the file on your computer or click the **Browse** button to locate the file.
2. When you have located the file, click **Restore** to upload the file. After completing the upload, the MaxR-3210 will reboot automatically.

Restoring the MaxR-3210 to the Factory Default Settings

It is sometimes desirable to restore the Access Point to the factory default settings. This can be done by using the Restore Defaults option, which restores all factory settings.

To access this function:

1. Under the **Maintenance** tab on the main menu, select **Reset**, and then select **Restore Defaults** from the sidebar. The Restore Defaults screen displays, as shown in [Figure 3-7](#) below.

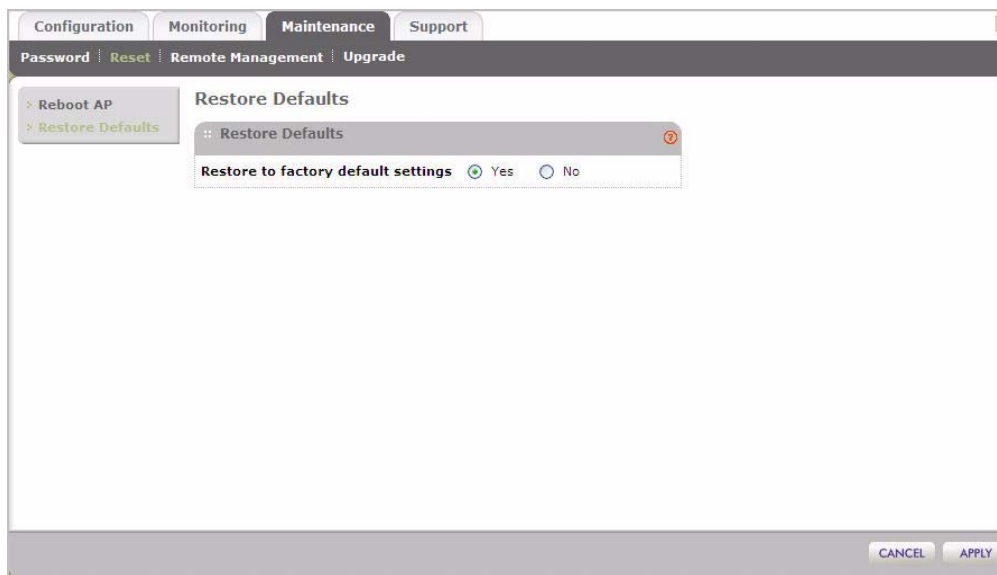


Figure 3-7 Restore to factory defaults

2. On the Restore Defaults screen, enable the **Restore to factory default settings** option by selecting the **Yes** radio button.
3. Click **Apply** to reset to the factory default settings.

After a restore, the Access Point password will be **password**, the default LAN IP address will be **192.168.0.237**, and the access point name will reset to the name printed on the label on the bottom of the unit.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the Access Point. The reset button has two functions:

- **Reboot.** When pressed and released, the Wireless Access Point will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear all data and restore all settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the MaxR-3210.

2. Use something with a small point, such as a pen, hold the Reset button for 5 seconds while you Power On the MaxR-3210.
3. Continue holding the Reset Button until the LEDs blink twice.
4. Release the Reset Button.

The factory default configuration has now been restored and the MaxR-3210 is ready for use.

Changing the Administrator Password

The default password is **password**. You should change this password to a more secure password, since you cannot change the administrator login name.

To change the Administrator password:

1. Under the **Maintenance** tab on the main menu, select **Password**, and then select **Change Password**. The Change Password screen displays as shown in [Figure 3-8](#) below.

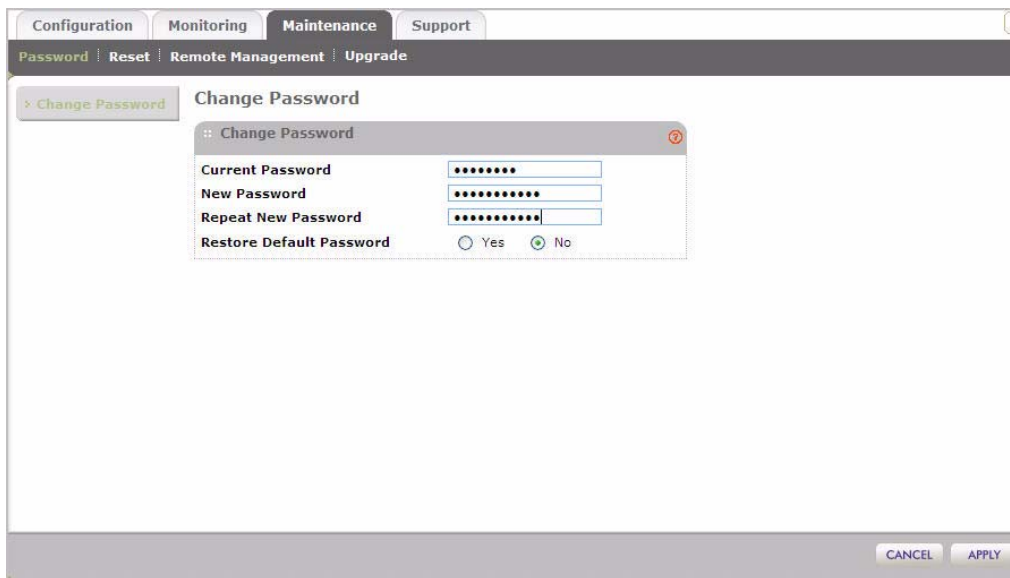


Figure 3-8 Change administrator password

2. First enter the old password in the **Current Password** field.

3. Then enter the new password twice—once in the **New Password** field and again in the **Repeat New Password** field.
4. Click **Apply** to save your change.

Enabling the SysLog Server

The SysLog screen allows you to enable the SysLog option if you have a SysLog server on your LAN.

To enable a SysLog server:

1. Under the **Configuration** tab on the main menu, select **System**, then select the **Advanced** option, and select **SysLog** to view the screen shown in [Figure 3-9](#).

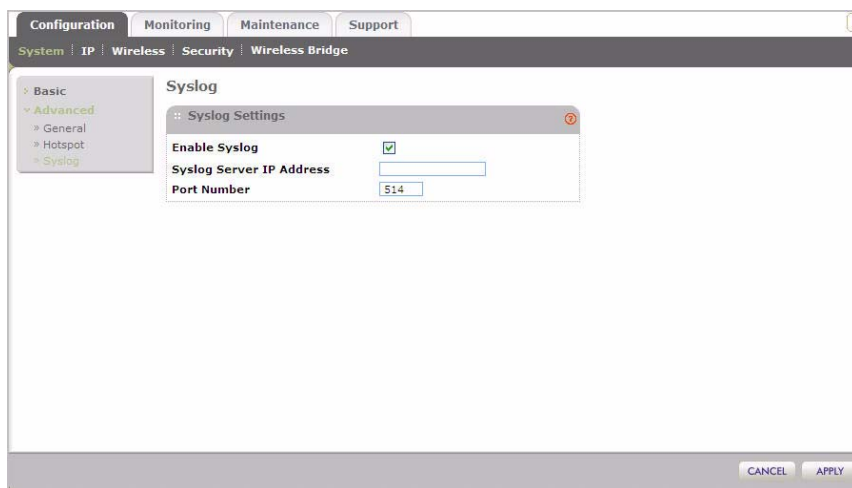


Figure 3-9 Enable Syslog server

2. **Enable SysLog** – Enable this option if you have a SysLog server on your LAN. If enabled, you must enter the IP address of your SysLog server and the port number your SysLog server is configured to use. The default is Disabled.
3. **SysLog Server IP Address** –The access point will send all the SysLog to the specified IP address if SysLog option is enabled.
4. **Port Number** – The port number configured in the SysLog server on your LAN. Default is 514.

5. Click **Apply** to save your Syslog settings.

Using Activity Log Information

The Activity Log screen displays the Access Point system activity.

To view the Activity Log, under the **Monitoring** tab on the main menu, click **Logs**. The Activity Logs screen displays as shown in [Figure 3-10](#) below.

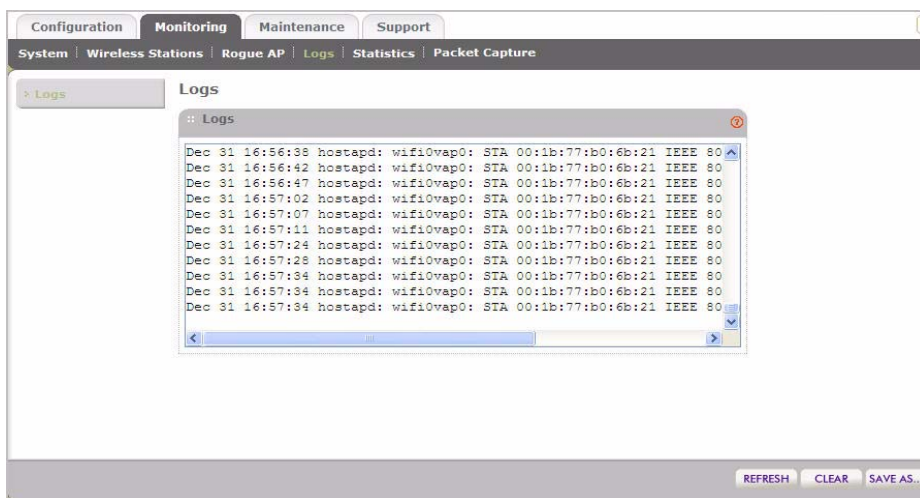


Figure 3-10 View activity logs

The Activity Log Window displays the Access Point system activity.

Click **Refresh** to update the display, click **Clear** to clear the log content, or click **Save As** to save the log contents into a file on a disk drive.

Viewing General Summary Information

The System screen, under the **Monitoring** tab provides a summary of the current MaxR-3210 configuration settings, including current IP settings and current Wireless settings. This information is read only, so any changes must be made on other pages.

To access the System screen:

Under the **Monitoring** tab on the main menu, select **System** to view the System screen, shown in [Figure 3-11](#) below. This screen shows the parameters listed in [Table 3-1](#):

Table 3-1. System Information Fields

Field	Description
Access Point Information	
Access Point Name	Indicates the NetBIOS name. The default name may be changed, if desired.
Ethernet MAC Address	Displays the Media Access Control address (MAC address) of the Access Point's Ethernet port.
Wireless MAC address for 2.4GHz	Displays the Media Access Control address (MAC address) of the Access Point's wireless card when operating at 2.4GHz
Firmware Version	The version of the firmware currently installed.
Current Time	Displays the current system time of the access point.
Current IP Settings	
IP Address	The IP address of the Access Point.
Subnet Mask	The subnet mask for IP address of the Access Point.
Default Gateway	The default gateway for the Access Point communication.
DHCP Client	Enabled indicates that the current IP address of the AP was obtained from a DHCP server on your network. Disabled indicated a static IP configuration.
Current Wireless Settings for 802.11b/bg/ng	
Operating Mode	Identifies the 802.11 operating mode of the MaxR-3210.
Channel/Frequency	Identifies the channel the wireless port is using. 'Auto' is the default channel setting.
Rogue AP Detection	Identifies whether the Rogue AP detection feature is enabled or disabled.

The screenshot displays the web interface of the MaxR-3210 Wireless-N Access Point. The top navigation bar includes tabs for Configuration, Monitoring, Maintenance, and Support. Below this, a secondary navigation bar shows System, Wireless Stations, Rogue AP, Logs, Statistics, and Packet Capture. The main content area is titled 'System' and contains three expandable sections:

- Access Point Information:**

Access Point Name	HSxxxxxx
Ethernet MAC Address	00:77:88:00:77:88
Wireless MAC Address	00:77:88:00:77:80
Country / Region	United States
Firmware Version	ARADA-PB44_HEALTHSENSE-PB44_1.0-BETA2.0
Current Time	Fri Dec 31 18:48:15 CST 1999
- Current IP Settings:**

IP Address	172.20.1.120
Subnet Mask	255.255.255.0
Default Gateway	172.20.1.23
DHCP Client	Enabled
- Current Wireless Settings for 802.11ng:**

Access Point Mode	Access Point
Channel / Frequency	11
Rogue AP Detection	Disabled

Figure 3-11 View system information

Viewing Network Traffic Statistics

The Statistics screen displays information for both wired (LAN) and wireless (WLAN) interface network traffic.

To access Statistics information:

1. Under the **Monitoring** tab on the main menu, select **Statistics**. The Statistics screen displays, as shown in [Figure 3-12](#) below.

	Received	Transmitted
Packets	10258	16892
Bytes	1280492	23289923

Wireless 802.11ng		
	Received	Transmitted
Unicast Packets	1314	0
Broadcast Packets	228	304
Multicast Packets	5	75
Total Packets	1547	379
Total Bytes	74537	80523

Wireless 802.11na		
	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	0

Figure 3-12 View network statistics

2. Click **Refresh** to update the Statistics information for each interface. .

Table 3-2, shown below, describes the information fields detailed on the Statistics screen.

Table 3-2. Statistics Fields

Field	Description
Wired Ethernet	
Packets	The number of packets sent and received since the MaxR-3210 was restarted.
Bytes	The number of bytes sent and received since the MaxR-3210 was restarted.
Wireless 11b/bg/ng	
Unicast Packets	The Unicast packets sent and received in 802.11n/g mode since the MaxR-3210 was restarted.
Broadcast Packets	The Broadcast packets sent and received in 802.11n/g mode since the MaxR-3210 was restarted.
Multicast Packets	The Multicast packets sent and received in 802.11n/g mode since the MaxR-3210 was restarted.

Table 3-2. Statistics Fields

Field	Description
Total Packets	The Wireless packets sent and received in 802.11n/g mode since the MaxR-3210 was restarted.
Total Bytes	The Wireless bytes sent and received in 802.11n/g mode since the MaxR-3210 was restarted.

Viewing Available Wireless Station Statistics

The Available Wireless Stations List (AWSL) contains a table of all IP devices associated with this Access Point in the wireless network defined by the Wireless Network Name (SSID). For each device, the table shows the MAC address, BSSID, SSID, Channel, Rate, State (whether the device is allowed to communicate with the Access Point or not), Type, AID, Mode, and Status.



Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This enables extending the reach of the wireless network and allows users to roam from one access point to another, providing seamless network connectivity. Under these circumstances, be aware that only the stations associated with this access point will be presented in the Available Station List.

To view the Available Wireless Stations List:

1. Under the **Monitoring** tab, select **Wireless Stations** on the main menu. The Available Wireless Stations list displays, as shown in [Figure 3-13](#).

Wireless Stations										
:: Available Wireless Stations (802.11ng)										
	MAC Address	BSSID	SSID	Channel	Rate	State	Type	AID	Mode	Status
	00:1B:77:80:6B:21	00:13:45:02:01:10	Arada_11g	1	0.00	QOS/ERP	open	1	11bg	Associated

:: Available Wireless Stations (802.11na)										
	MAC Address	BSSID	SSID	Channel	Rate	State	Type	AID	Mode	Status

Figure 3-13 Available Wireless Stations list

2. Click **Refresh** to update the list.



Tip: If the Access Point is rebooted, the table data is lost until the Access Point rediscovers the devices. To force the Access Point to look for associated devices, click the **Refresh** button.

Enabling Rogue AP Detection

The MaxR-3210 can detect rogue APs and wireless stations and show their details to the administrator.

To enable Rogue AP Detection:

1. Under the **Configuration** tab on the main menu, select **Security**, select **Advanced** from the sidebar, and then select **Rogue AP**. The Rogue AP screen displays, as shown in [Figure 3-8](#) below.

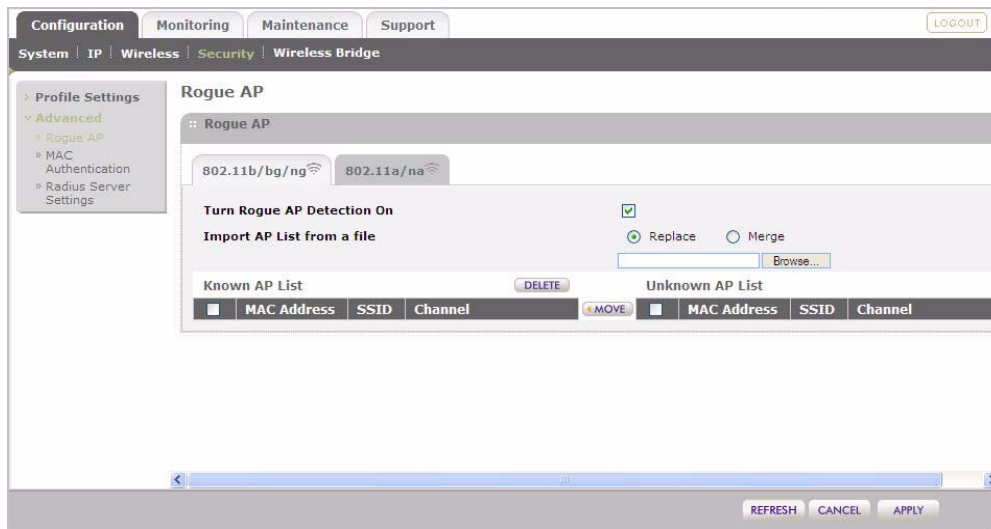


Figure 3-14 Enable Rogue AP detection

2. Check the **Turn Rogue AP Detection On** radio box to enable rogue AP detection and click **Apply**.

If you enable Rogue AP Detection, the AP continuously scans the wireless network and collects information about all APs heard on its channel.

3. You can Import AP List from a File. See [“Importing Rogue AP List from a File”](#) on page 3-18 for more information.
4. Under the Unknown AP List, click **Refresh** to discover the APs.
5. Click **Move** to add any AP to the Known AP List.
6. Click **Delete** to remove an AP from the Known AP List.
7. Click **Apply** to save your change.

Importing Rogue AP List from a File

To replace the existing AP list:

1. Create a text file that contains the MAC address of each known AP, separated by a space. The following example shows a list of six known APs that an administrator might upload to the AP:

```
00:0c:41:d7:ee:a5 00:0f:b5:92:cd:49 00:12:17:70:85:3d  
00:14:bf:ae:b1:e4 00:40:f4:f8:47:03 00:0c:41:d7:ee:b4
```

2. Select **Replace** to replace the existing list of known APs, or select **Merge** to add the new MAC addresses to the existing list.
3. Click **Browse** and navigate to the location where you saved the text file.
4. Select the file and click **Open**.
5. Click **Import** to upload the list to the AP.

To import the list from an existing file:

1. Click **Browse** and navigate to the location where you saved the text file.
2. Select the file and click **Open**.
3. Click **Import** to upload the list to the AP.

Viewing Rogue AP Statistics

The MaxR-3210 can detect rogue APs and wireless stations and show a complete list of unknown or known APs to the administrator.

To view the Rogue AP list:

1. Under the **Monitoring** tab on the main menu, select **Rogue AP**. Select **Unknown AP List**. The following screen displays with a list of unknown APs:

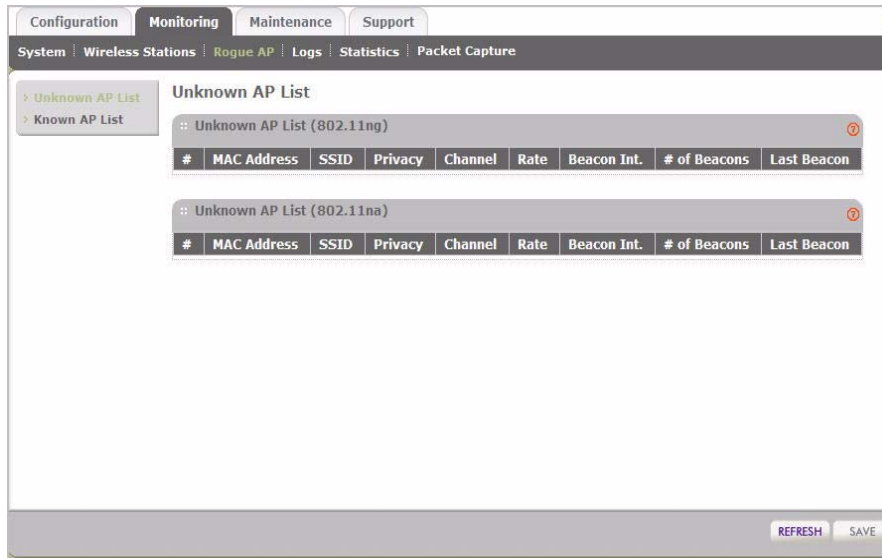


Figure 3-15 Unknown APs list

2. Click **Refresh** to refresh the list.
3. Click **Save** to export the list of unknown APs to a file. A window opens so you can browse to the location where you want to save the file.

To view the list of known APs:

1. Under the **Monitoring** tab on the main menu, select **Rogue AP**. Select **Known AP List**. The following screen displays with a list of known APs:

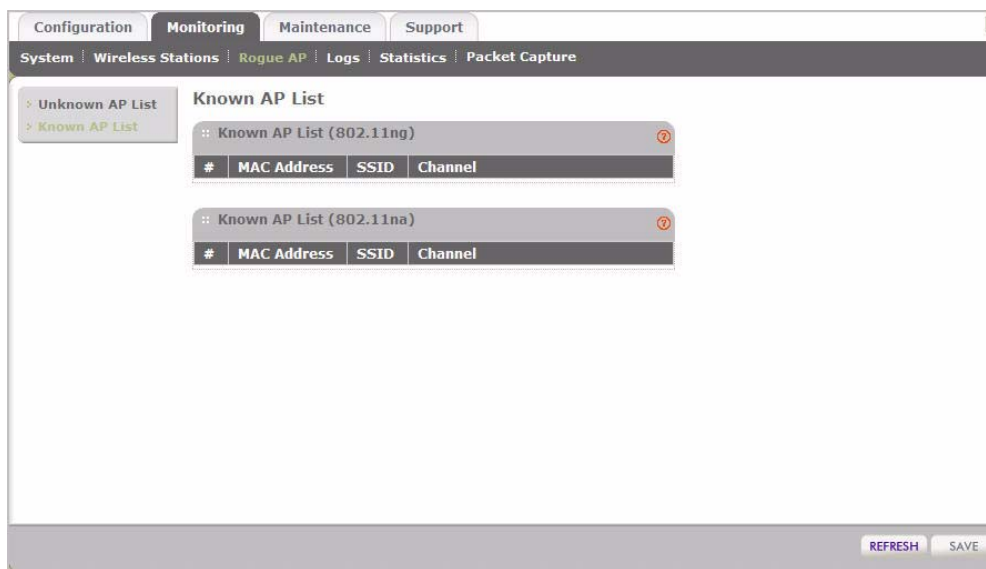


Figure 3-16 Known APs list

2. Click **Refresh** to refresh the list.
3. Click **Save** to export the list of known APs to a file. A window opens so you can browse to the location where you want to save the file.

Packet Capture

The packet capture option is available under the **Monitoring > Packet Capture** tab. Use this option for troubleshooting association problems. You can capture all packets transmitted and received by the AP and save them in `pcap` format for analysis by any standard sniffer tool such as *WireShark* or *OmniPeek*.

The packet capture screen is shown below:



Figure 3-17 Packet capture screen

Chapter 4

Advanced Configuration

This chapter describes how to configure the advanced features of your MaxR-3210 Single Band Wireless-N Access Point. The advanced configuration features are located under the **Advanced** sections of various sub-menus under **Configuration** and provide the following functions:

- **IP Settings.** Using the Access Point as a DHCP server for wireless clients (“[IP Settings for Wireless Clients](#)”).
- **Hotspot settings.** Enabling HTTP redirect (“[Hotspot Settings](#)”).
- **Wireless Settings:** Configuring advanced wireless LAN parameters (“[Configuring Advanced Wireless Settings](#)”).
- **Advanced QoS Settings:** Configuring advanced QoS settings (“[Configuring Advanced QoS Settings](#)”).
- **Access Point Settings:** Enabling wireless bridging modes (“[Enabling Wireless Bridging](#)”).

IP Settings for Wireless Clients

You can turn the MaxR-3210 into a DHCP Server for wireless clients for both DHCP-enabled wireless clients. The default advanced IP wireless settings usually work well. This feature is intended for use by a systems administrator. By default, this feature is not enabled.

To use this Access Point as a DHCP server:

1. From the main menu under **Configuration**, select **IP**, and then select **DHCP Server Settings**. The DHCP Server Settings screen displays (see [Figure 4-1](#)).
2. DHCP Server is disabled by default. Select the **Enable** radio button to enable this wireless access point as a DHCP server.

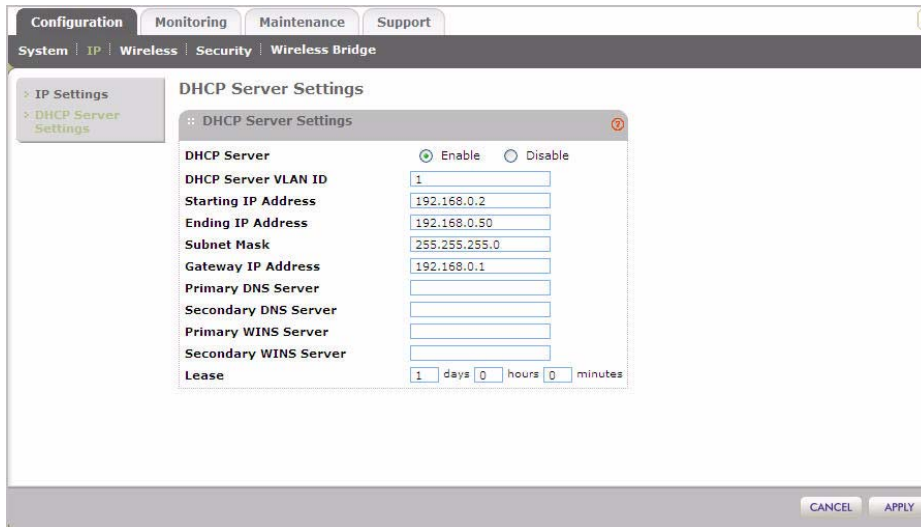


Figure 4-1 DHCP server settings

3. Configure the following TCP/IP configurations for using the MaxR-3210 as a DHCP Server for wireless clients.
 - **DHCP Server:** By default, the Dynamic Host Configuration Protocol (DHCP) server on the AP is disabled. If you enable it, all the wireless clients associated with the AP will get their IP addresses, subnet mask and default gateway settings automatically from the AP.
 - **DHCP Server VLAN ID:** All the stations that are part of the configured VLAN ID will get their IP addresses only from the AP.
 - **Starting IP Address:** Enter the starting IP address that can be assigned from the DHCP server on this Access Point.
 - **Ending IP Address:** Enter the Ending IP address that can be assigned from the DHCP server on this Access Point
 - **Subnet Mask:** The Access Point will assign the specified subnet mask to the connected wireless stations.
 - **Gateway Address:** The Access Point will assign this IP address as the default gateway for any traffic beyond the local network.
 - **Primary DNS Server:** The Access Point will assign this IP address as the primary Domain Name Server used by the connected wireless stations.

- **Secondary DNS Server:** The Access Point will assign this IP address as the secondary Domain Name Server used by the connected wireless stations.
- **Primary WINS Server:** The Access Point will assign this IP address as the primary WINS Server used by the connected wireless stations.
- **Secondary WINS Server:** The Access Point will assign this IP address as the secondary WINS Server used by the connected wireless stations.
- **Lease:** The lease time for the IP address assigned. The wireless client user is required to renew the IP address as soon as the lease is expired.

4. Click **Apply** to save your settings.

Hotspot Settings

If you want the Access Point to capture and redirect the first HTTP (TCP, port 80) request, use this feature to “capture” and redirect the HTTP request to the specified URL. For example, a hotel might want all wireless connections to go to its server to start a billing transaction.

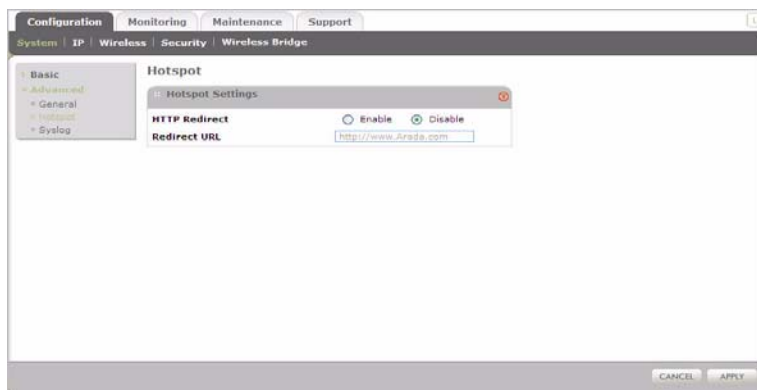


Figure 4-2 Hotspot settings

To set up a Hotspot server:

1. From the main menu under **Configuration**, select **System**, then select **Advanced**.
2. From the sidebar, select **Hotspot**. The Hotspot screen displays, as shown in [Figure 4-2.](#), with the following fields:
 - **HTTP Redirect:** Enable HTTP Redirect..

- **Redirect URL:** Enter the URL of the Web server where you wish to redirect HTTP (port 80) requests.
3. Click **Apply**. All port 80 requests will now be redirected to the specified URL.

Configuring Advanced Wireless Settings

The **Advanced** option of the Wireless Settings menu is used to configure and enable various wireless LAN parameters for the 11b/bg/ng modes. The default wireless LAN parameters usually work well. However, you can use these settings to fine tune the overall performance of your Access Point for your environment.

The Wireless Settings option of the Advanced menu is used to configure the Wireless LAN parameters. The default advanced wireless LAN parameter settings usually work well.

Configuring 802.11b/bg/ng Advanced Wireless Settings

To configure advanced Wireless Settings:

1. Under the **Configuration** tab, select **Wireless**.
2. From the sidebar, select **Advanced**, and then select **Wireless Settings**.

3. The Advanced Wireless Settings screen displays, as shown in [Figure 4-3.](#),

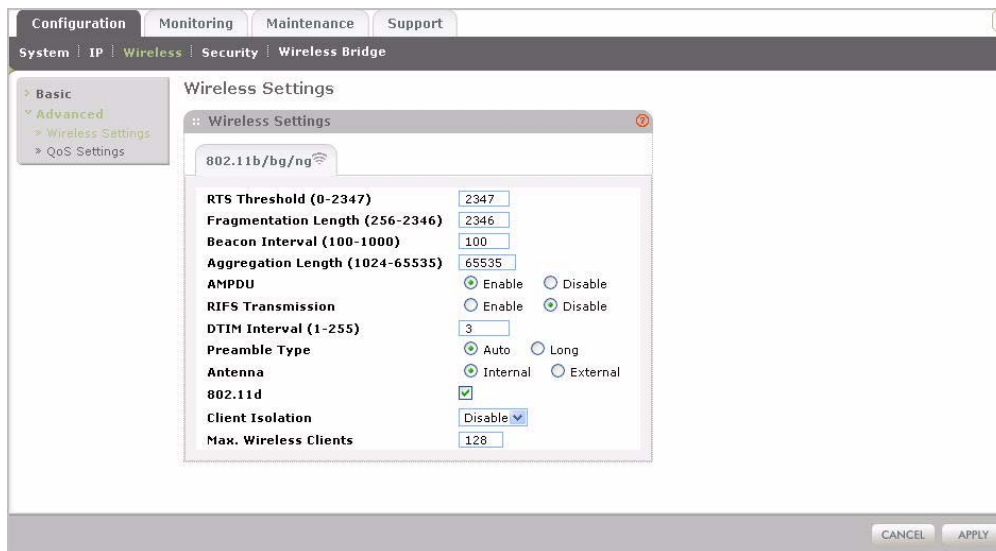


Figure 4-3 Advanced Wireless Settings - 802.11b/bg/ng

4. Enter the appropriate information in the fields described below:
- **RTS Threshold (0 - 2347):** Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2347.
 - **Fragmentation Length (256 - 2346):** This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragmentation threshold value must be larger than the RTS threshold value. The default is 2346.
 - **Beacon Interval (100 - 1000):** The Beacon Interval. Specifies the interval time between 100ms and 1000ms for each beacon transmission, which allows the access point to synchronize the wireless network. The default is 100.

- **Aggregation Length (1024-65535) (11ng):** The aggregation length defines the size of aggregated packets. Larger aggregation lengths may sometimes lead to better network performance. The default is 65535.
- **A-MPDU (11ng):** Aggregated MAC Protocol Data Unit. Aggregates several MAC frames into a single large frame to achieve higher throughput. The default is enabled.
- **RIFS Transmission (11ng):** Reduced Interframe Space. RIFS transmissions are shorter than other interframe spaces, and if enabled allow transmission of successive frames at different transmit powers. The default is disabled.
- **DTIM Interval:** The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. The default is 3.
- **Preamble Type (11b/bg only):** A long transmit preamble may provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The Auto settings automatically handles both long and short preambles. The default is Auto.
- **Antenna:** Not supported.
- **802.11d:** Enable this option to include support for "additional regulatory domains" that are not in the current standard.
- **Max Wireless Clients:** The number of wireless clients that can associate with the AP at one time. The default is 63.

5. Click **Apply** to enable the Wireless Settings.

Configuring Advanced QoS Settings

Wireless Multimedia Extension (WME) or Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WME allows wireless traffic to have a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WME to function correctly, Wireless clients must also support WME.

Figure 4-4 shows the Quality of Service (QoS) screen. For most networks, the default QoS queue parameter settings work well. Quality of Service provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic, like Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data.

To configure advanced QoS settings, on the **Configuration** tab select **Wireless**, select **Advanced**, and then select **QoS Settings**. The QoS Settings screen displays:

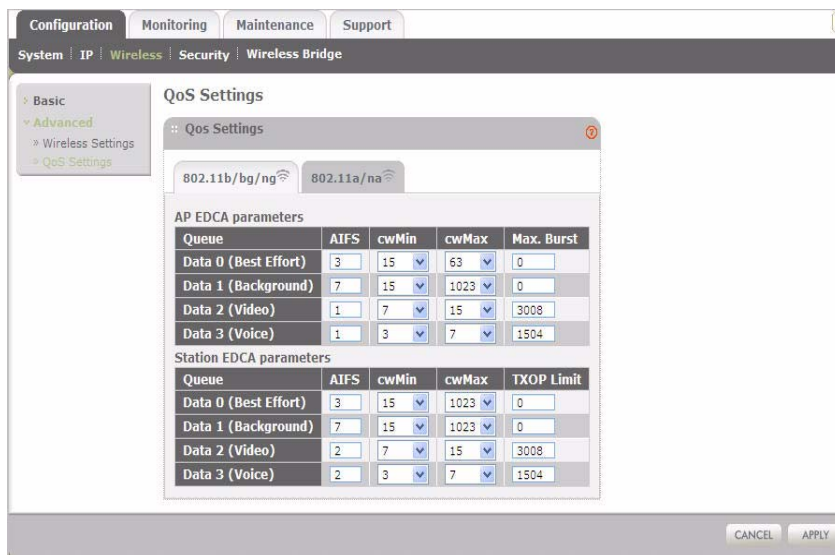


Figure 4-4 Advanced QoS settings

The QoS options on the MaxR-3210 are as follows:

- **AP EDCA Parameters.** Specify the AP EDCA (Enhanced Distributed Channel Access) parameters for different types of data transmitted from the MaxR-3210 Wireless Access Point to the wireless client.
- **Station EDCA Parameters.** Specify the Station EDCA parameters for different types of data transmitted from the wireless client to the MaxR-3210 Wireless Access Point. If WMM is disabled, you cannot configure Station EDCA parameters.

Table 4-1 describes the settings for QoS Queues.

Table 4-1. QoS Queues and Parameters

QoS Queue	Description
Data 0 (Voice)	High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
Data 1 (Video)	High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
Data 2 (Best Effort)	Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

Table 4-1. QoS Queues and Parameters

QoS Queue	Description
Data 3 (Background)	Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Arbitration Inter-Frame Space)	Specifies a wait time (in milliseconds) for data frames. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	Upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. Valid values for the “cwmin” are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwMin must be lower than the value for cwMax.
cwMax (Maximum Contention Window)	Upper limit (in milliseconds) for the doubling of the random backoff value. Valid values for the “cwmax” are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwMax must be higher than the value for cwMin.
Max. Burst Length	Specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0.0 through 999.9.

Enabling Wireless Bridging

The MaxR-3210 Single Band Wireless-N Access Point lets you build large bridged wireless networks. Select the desired Access Point mode for your environment:

- **Wireless Point-to-Point Bridge.** In this mode, the MaxR-3210 can communicate with another bridge mode wireless access point—with wireless clients if you select the **Enable Wireless Client Association** check box.

When you click the **Edit** button, you must enter the Profile Name and the MAC address (physical address) of the other Bridge mode wireless access point in the fields provided. WEP, WPA-PSK, or WPA2-PSK are supported. WPA2-PSK can (and should) be used to protect this communication.

- **Wireless Point-to-Multi-Point Bridge.** Select this only if this MaxR-3210 is the “Master” for a group of bridge-mode wireless access points. Select the **Enable Wireless Client Association** option to enable wireless clients to associate with this access point.

The other bridge-mode wireless access points must be set to point-to-point bridge mode, using the MAC address of this MaxR-3210. They then send all traffic to this “Master”, rather than communicate directly with each other.

When you click the **Edit** button, you must enter the profile name and the MAC address (physical address) of the other bridge mode wireless station in the fields provided. WEP, WPA-PSK, or WPA2-PSK are supported. WPA2-PSK can (and should) be used to protect this communication.

The screens used to configure these options are located by selecting **Wireless Bridge** under the **Configuration** tab (see [Figure 4-5](#) and [Figure 4-6](#) below).

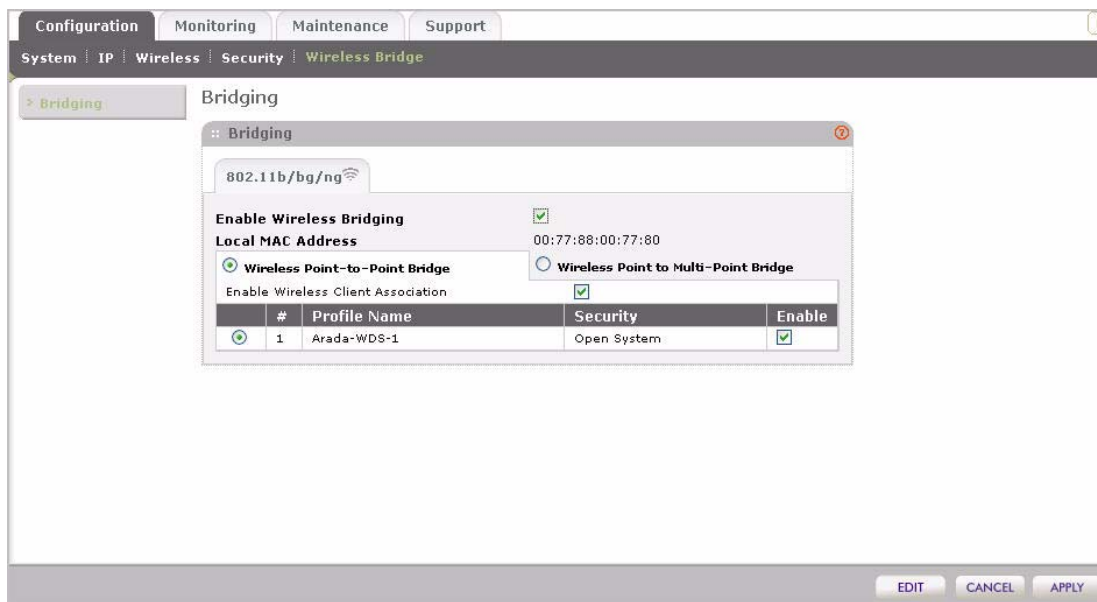


Figure 4-5 Configure Point to Point Bridging

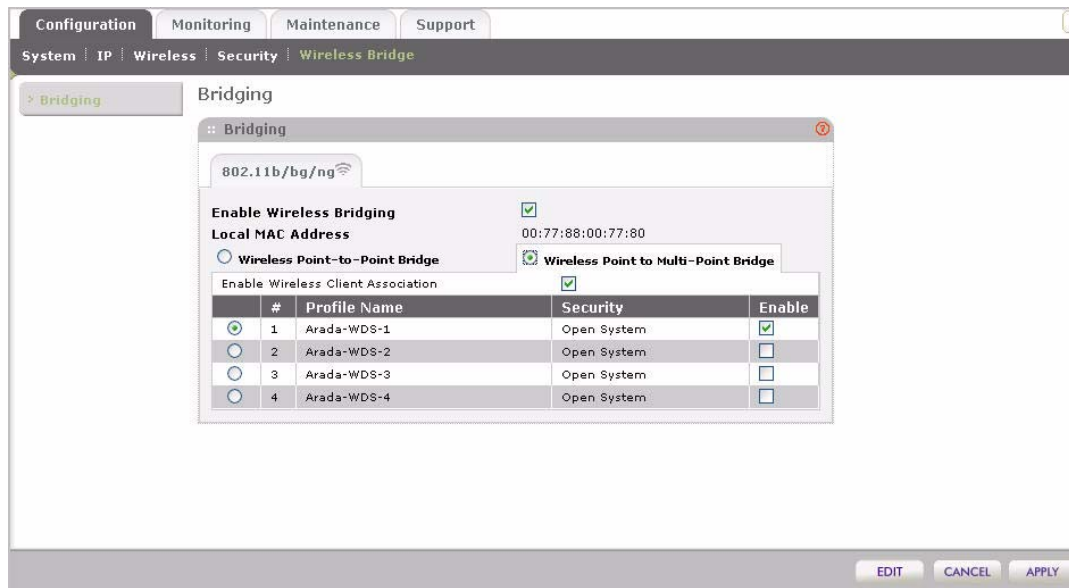


Figure 4-6 Configure Point to Multi-Point bridging

To configure wireless bridging:

1. Click the **Enable Wireless Bridging** checkbox.
2. Select either the **Wireless Point to Point Bridge** or **Wireless Point to Multi-Point Bridge** radio button.
3. Select **Enable Wireless Client Association** if you wish.
4. Select the profile you want to edit.
5. Click **Edit**.

The Edit Security Profile screen displays, as shown in [Figure 4-7](#) below.

The screenshot shows a web-based configuration interface for a MaxR-3210 Wireless-N Access Point. The top navigation bar includes tabs for Configuration, Monitoring, Maintenance, and Support. Below this, a breadcrumb trail indicates the current location: System > IP > Wireless > Security > Wireless Bridge. A left-hand sidebar shows a tree view with 'Bridging' selected. The main content area is titled 'Edit Security Profile' and is divided into two sections: 'Profile Definition' and 'Authentication Settings'. The 'Profile Definition' section contains two input fields: 'Profile Name' (with the value 'Arada-WDS-1') and 'Remote MAC Address'. The 'Authentication Settings' section contains two dropdown menus: 'Network Authentication' (set to 'Open System') and 'Data Encryption' (set to 'None'). At the bottom right of the form, there are three buttons: 'BACK', 'CANCEL', and 'APPLY'.

Figure 4-7 Bridging - Edit a WDS Security Profile

To edit a security profile:

1. Enter a profile name.
2. Enter the MAC address of the remote access point.
3. Select a network authentication type.
4. Select an encryption strength.
5. Click **Back**.
6. Enable the profile, if you wish to, on the Bridging screen.

The following sections take you through the physical steps of configuring your MaxR-3210 as a point-to-point or point-to-multipoint wireless beidge.

Configuring an MaxR-3210 as a Point-to-Point Bridge

To configure a point-to-point bridge as shown in [Figure 4-8](#):

1. Under the **Configuration** tab, select **Wireless Bridge**. Then, select **Bridging**. The Bridging screen displays (see [Figure 4-5](#)).
2. Configure the MaxR-3210 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.

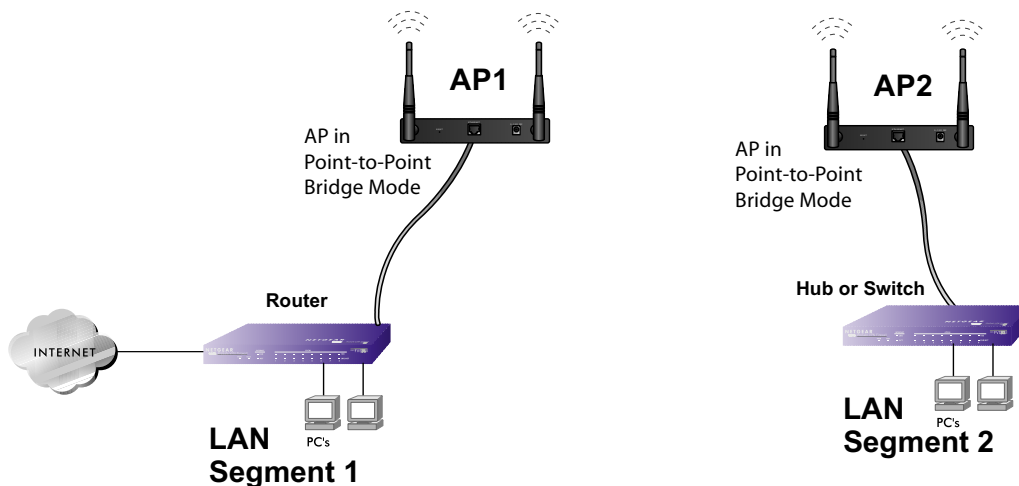


Figure 4-8 Wireless point-to-point bridge setup

3. Configure the MaxR-3210 (AP2) on LAN Segment 2 in Point-to-Point Bridge mode.
AP1 must have AP2's MAC address in its Remote MAC Address field and AP2 must have AP1's MAC address in its Remote MAC Address field.
4. Configure and verify the following parameters for both access points:
 - Verify that the LAN network configuration of the MaxR-3210 Wireless Access Points both are configured to operate in the same LAN network address range as the LAN devices
 - Both use the same ESSID, Channel, authentication mode, if any, and security settings if security is in use.
5. Verify connectivity across the LAN 1 and LAN 2.

A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

- Click **Apply** to save your settings.

Configuring an MaxR-3210 as a Point-to-Multi-Point Wireless Bridge

To configure a point-to-multi-point wireless bridge as shown in [Figure 4-9](#):

- Under the **Configuration** tab, select **Wireless Bridge**. Then, select **Bridging**. The Bridging screen displays (see [Figure 4-6](#)).

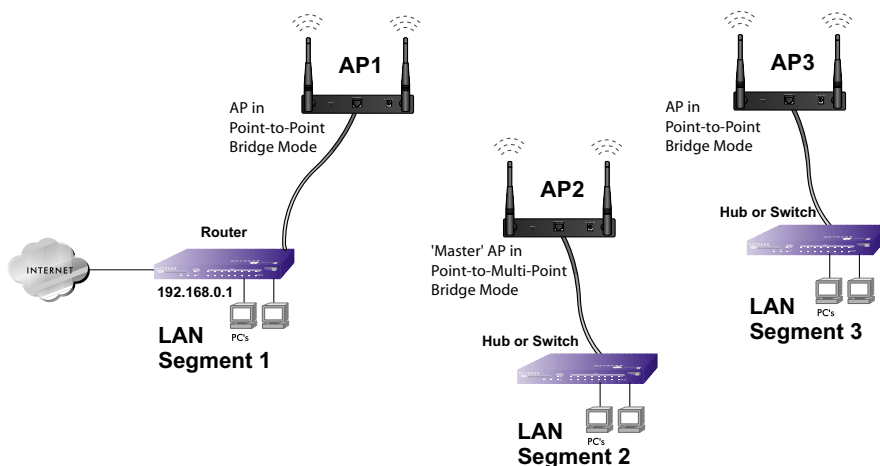


Figure 4-9 Wireless point-to-multipoint bridge setup

- Configure the Operating Mode of the MaxR-3210 Wireless Access Points.
 - MaxR-3210 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
 - Because it is in the central location, configure MaxR-3210 (AP2) on LAN Segment 2 in Point-to-Multi-Point Bridge mode. The MAC addresses of the adjacent APs are required in AP2.
 - Configure the MaxR-3210 (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
- Verify the following parameters for all access points:
 - Verify that the LAN network configuration the MaxR-3210 Wireless Access Points are configured to operate in the same LAN network address range as the LAN devices

- Only one access point is configured in Point-to-Multi-Point Bridge mode, and all the others are in Point-to-Point Bridge mode.
 - All access points must be on the same LAN. That is, all the APs LAN IP address must be in the same network.
 - If using DHCP, all MaxR-3210 Wireless Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
 - All MaxR-3210 Wireless Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
 - All Point-to-Point Access Points must have the AP2 MAC address in its Remote AP MAC address field.
4. Verify connectivity across the LANs.
- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
 - Wireless stations will be able to connect to the MaxR-3210 Wireless Access Points in the illustration above. If you require wireless stations to access any LAN segment, you can add additional MaxR-3210 Wireless Access Points configured in Wireless Access Point mode to any LAN segment.
5. Click **Apply** to save your settings.



Note: You can extend this multi-point bridging by adding additional MaxR-3210s configured in Point-to-Point mode for each additional LAN segment.

Chapter 5

Troubleshooting and Debugging

This chapter provides information about troubleshooting your MaxR-3210 Single Band Wireless-N Access Point. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the MaxR-3210 on?
Go to [“Installing the MaxR-3210 Wireless Access Point” on page 2-4](#)
- Have I connected the Access Point correctly?
Go to [“Installing the MaxR-3210 Wireless Access Point” on page 2-4](#).
- I cannot remember the Access Point’s configuration password.
Go to [“Changing the Administrator Password” on page 3-10](#).

If you have trouble setting up your MaxR-3210, check the tips below.

No lights are lit on the Access Point.

It takes a few seconds for the power indicator to light up. Wait a minute and check the power light status on the access point.

If the access point has no power.

- Make sure the power cord is connected to the access point.
- Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure you are using the correct power adapter supplied with your access point.

The Wireless LAN activity light does not light up.

The access point antennas are not working.

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Make sure the antennas are tightly connected to the MaxR-3210.
- Contact ARADA technical support at support@aradasystems.com if the Wireless LAN activity light remains off.

The LAN light is not lit.

There is a hardware connection problem. Check these items:

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router must be installed between the access point and the Ethernet LAN or broadband modem.
- LAN light does not light up if it is a 10 Mbps link. In such cases, the Lan activity light will still blink if there is activity.
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

I cannot access the Internet or the LAN with a wireless capable computer.

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows the Network Properties is set to “Obtain an IP address automatically.”
- The access point’s default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.

I cannot connect to the MaxR-3210 to configure it.

Check these items:

- The MaxR-3210 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is green to verify that the Ethernet connection is OK.
- The default configuration of the MaxR-3210 is for a static IP address of 192.168.0.237 and a Mask of 255.255.255.0 with DHCP disabled. Make sure your network configuration settings are correct.
- If you are using the NetBIOS name of the MaxR-3210 to connect, ensure that your computer and the MaxR-3210 are on the same network segment or that there is a WINS server on your network.
- If your computer is set to “Obtain an IP Address automatically” (DHCP client), restart it.
- If your computer uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the MaxR-3210. The MaxR-3210 default IP Address is 192.168.0.237 and the default Subnet Mask is 255.255.255.0. If you are not sure about these settings, follow the instructions for [“Installing the MaxR-3210 Wireless Access Point” on page 2-4.](#)

When I enter a URL or IP address I get a timeout error.

A number of things could be causing this. Try the following troubleshooting steps.

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the MaxR-3210 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the MaxR-3210 is configured correctly, check your Internet connection (DSL/Cable modem etc.) to make sure that it is working correctly.
- Try again.

Using the Reset Button to Restore Factory Default Settings

The Reset button (see “[Rear Panel](#)” on page 1-5) has two functions:

- **Reboot.** When pressed and released quickly, the MaxR-3210 will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the MaxR-3210 and power it back on.
2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least 5 seconds.
3. Release the Reset button.

The factory default configuration has now been restored, and the MaxR-3210 is ready for use.

Appendix A

Default Settings and Technical Specifications

This appendix provides the factory default settings and technical specifications for the MaxR-3210 Single Band Wireless-N Access Point.

Factory Default Settings

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in [Table A-1](#) below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. Access Point Default Configuration Settings

Feature	Description
AP Login	
User Login URL	192.168.0.237
User Name (case sensitive)	admin
Login Password (case sensitive)	password
Ethernet Connection	
Static IP Address	192.168.0.210
Ethernet MAC Address	See bottom label.
Port Speed	10/100/1000
Local Network (LAN)	
Lan IP	192.168.0.230
Subnet Mask	255.255.255.0
Gateway Address	
DHCP Server	Disabled

Table A-1. Access Point Default Configuration Settings

Feature		Description
	DHCP Client	Disabled
	Time Zone	USA-Pacific
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Enabled, but Trap forwarding disabled
	Spanning Tree Protocol	Disabled
	Secure Telnet	Enabled
Wireless		
	Operating Mode	Access Point
	Access Point Name	aradaxxxxxx where xxxxxx are the last 6 digits of the wireless access point MAC address.
	Wireless Communication	Enabled
	11 b/bg/ng Wireless Network Name (SSID)	ARADA_11g
	Broadcast Network Name SSID	Enabled
	Security	Disabled
	Transmission Speed	Best ^a
	80211.g Radio Frequency Channel	Auto
	Output Power	Full
	Wireless Card Access List	All wireless stations allowed
	WMM Support	Enabled

a. Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

Table A-2. MaxR-3210 Technical Specifications

Parameter	MaxR-3210 Single Band Wireless-N Access Point
802.11g Data Rates	1, 2, 5.5, 11, 12, 18, 24, 36, 38, 54, & 108 Mbps (Auto-rate capable)
802.11ng Data Rates	Data Rates for Channel Width=20MHz and Guard Interval=short (400ms): Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
	Data Rates for Channel Width=20MHz and Guard Interval=long (800ms): Best, 6.5 Mbps, 13 Mbps, 19.5 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 58.5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps
	Data Rates for Channel Width=40MHz and Guard Interval=short: Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
	Data Rates for Channel Width=40MHz and Guard Interval=long: Best, 13.5 Mbps, 27 Mbps, 40.5 Mbps, 54 Mbps, 81 Mbps, 121.5 Mbps, 135 Mbps, 27 Mbps, 54 Mbps, 81 Mbps, 162 Mbps, 216 Mbps, 243 Mbps, 270 Mbps
802.11b/bg/ng Operating Frequencies	2.412 ~ 2.462 GHz (US) 2.457 ~ 2.462 GHz (Spain) 2.412 ~ 2.484 GHz (Japan) 2.457 ~ 2.472 GHz (France) 2.412 ~ 2.472 GHz (Europe ETSI)
802.11 b/bg/ng Encryption	64-bits, 128- and 152-bits WEP, AES, TKIP data encryption
Network Management	Web-based configuration and status monitoring
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; maximum 64 supported.
Status LEDs	Power/Ethernet LAN/Wireless LAN/Test
Power Adapter	12V DC, 1.5 A
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

Appendix B

Command Line Reference

The MaxR-3210 Single Band Wireless-N Access Point (AP) can be configured either through the command line interface (CLI), a Web browser, or an MIB browser. The CLI allows viewing and modification of the configuration from a terminal or PC through a telnet connection.

Command Sets

keyword	Description
-backup-configuration	--backup configuration
-config>	--configuration setting
-apname	--access point name
-country	--country/region
-dhcp>	--DHCP server
-dns-server	--DNS server
-gateway	--default gateway
-ip-address	--IP range
-lease-time	--lease time
-status	--status
-subnet-mask	--subnet mask
-wins-server	--WINS server
-http-redirect	--enable HTTP redirection
-http-redirect-url	--HTTP redirection URL
-interface>	--select wireless lan interface
-wlan>	--wireless LAN interface setting
-2.4GHz>	--2.4 GHz wireless LAN interface setting
-aggregation-length	--aggregated packet size
-ampdu	--aggregated MAC Protocol Data Unit
-beacon-interval	--wireless beacon period in TU(1024 us)
-channel	--wireless channel (depends on country and wireless mode)
-channelwidth	--wireless channel width
-dtim-interval	--wireless DTIM period in beacon interval
-extension-protection-spacing	--wireless extension protection spacing
-fragmentation-length	--wireless fragmentation threshold(even only)
-guardinterval	--interval (from interference from other

```

transmissions)
| | | | |-knownap-add                --add known access point
| | | | |-knownap-del                --delete known access point
| | | | |-macacl-add                 --add wireless access control (ACL)
| | | | |-macacl-database            --delete wireless access control (ACL)
database
| | | | |-macacl-del                 --delete wireless access control (ACL)
| | | | |-mcsrate                    --transmit data rate
| | | | |-mode                       --enable wireless access control (ACL)
| | | | |-operation-mode             --wireless operation mode
| | | | |-power                      --wireless transmit power
| | | | |-preamble                   --wireless preamble (only effect on
802.11b rates)
| | | | |-radio                      --enable wireless radio
| | | | |-rate                       --wireless transmission data rate
| | | | |-rifs-transmission          --enable successive frame transmission at
different transmit powers
| | | | |-rogue-ap-detection         --enable rogue access point detection
| | | | |-rts-threshold              --wireless RTS/CTS threshold
| | | | |-security-profile>          --create security profile
| | | | | -1>                        --1st security profile
| | | | | | -authentication          --authentication type
| | | | | | -encryption              --data encryption
| | | | | | -hide-network-name       --hide network name
| | | | | | -key1                    --wireless wep key 1
| | | | | | -key2                    --wireless wep key 2
| | | | | | -key3                    --wireless wep key 3
| | | | | | -key4                    --wireless wep key 4
| | | | | | -keyno                   --key number
| | | | | | -name                    --profile name
| | | | | | -presharedkey            --pre-shared key
| | | | | | -security-separation     --disable associated wireless client
communication
| | | | | | -ssid                    --network name (1-32 chars)
| | | | | | -status                  --profile status
| | | | | | -vlan-id                 --VLAN id
| | | | | | -wep-pass-phrase         --wireless wep passphrase key
| | | | | | -wepkeytype              --wireless wep key type
| | | | | | |
| | | | | | -2>                      --2nd security profile
| | | | | | | -authentication        --authentication type
| | | | | | | -encryption            --data encryption
| | | | | | | -hide-network-name     --hide network name
| | | | | | | -key1                  --wireless wep key 1
| | | | | | | -key2                  --wireless wep key 2
| | | | | | | -key3                  --wireless wep key 3
| | | | | | | -key4                  --wireless wep key 4
| | | | | | | -keyno                 --key number

```

```

| | | | | | | -name                --profile name
| | | | | | | -presharedkey          --pre-shared key
| | | | | | | -security-separation  --disable associated wireless client
communication
| | | | | | | -ssid                --network name (1-32 chars)
| | | | | | | -status                --profile status
| | | | | | | -vlan-id              --VLAN id
| | | | | | | -wep-pass-phrase       --wireless wep passphrase key
| | | | | | | -wepkeytype          --wireless wep key type
| | | | | | |
| | | | | | | -3>                --3rd security profile
| | | | | | | -authentication        --authentication type
| | | | | | | -encryption           --data encryption
| | | | | | | -hide-network-name     --hide network name
| | | | | | | -key1                --wireless wep key 1
| | | | | | | -key2                --wireless wep key 2
| | | | | | | -key3                --wireless wep key 3
| | | | | | | -key4                --wireless wep key 4
| | | | | | | -keyno              --key number
| | | | | | | -name                --profile name
| | | | | | | -presharedkey          --pre-shared key
| | | | | | | -security-separation  --disable associated wireless client
communication
| | | | | | | -ssid                --network name (1-32 chars)
| | | | | | | -status                --profile status
| | | | | | | -vlan-id              --VLAN id
| | | | | | | -wep-pass-phrase       --wireless wep passphrase key
| | | | | | | -wepkeytype          --wireless wep key type
| | | | | | |
| | | | | | | -4>                --4th security profile
| | | | | | | -authentication        --authentication type
| | | | | | | -encryption           --data encryption
| | | | | | | -hide-network-name     --hide network name
| | | | | | | -key1                --wireless wep key 1
| | | | | | | -key2                --wireless wep key 2
| | | | | | | -key3                --wireless wep key 3
| | | | | | | -key4                --wireless wep key 4
| | | | | | | -keyno              --key number
| | | | | | | -name                --profile name
| | | | | | | -presharedkey          --pre-shared key
| | | | | | | -security-separation  --disable associated wireless client
communication
| | | | | | | -ssid                --network name (1-32 chars)
| | | | | | | -status                --profile status
| | | | | | | -vlan-id              --VLAN id
| | | | | | | -wep-pass-phrase       --wireless wep passphrase key
| | | | | | | -wepkeytype          --wireless wep key type
| | | | | | |

```

```

| | | | | -5>                --5th security profile
| | | | | |-authentication  --authentication type
| | | | | |-encryption      --data encryption
| | | | | |-hide-network-name --hide network name
| | | | | |-key1            --wireless wep key 1
| | | | | |-key2            --wireless wep key 2
| | | | | |-key3            --wireless wep key 3
| | | | | |-key4            --wireless wep key 4
| | | | | |-keyno          --key number
| | | | | |-name            --profile name
| | | | | |-presharedkey    --pre-shared key
| | | | | |-security-separation --disable associated wireless client
communication
| | | | | |-ssid            --network name (1-32 chars)
| | | | | |-status          --profile status
| | | | | |-vlan-id         --VLAN id
| | | | | |-wep-pass-phrase  --wireless wep passphrase key
| | | | | |-wepkeytype       --wireless wep key type
| | | | |
| | | | | -6>                --6th security profile
| | | | | |-authentication  --authentication type
| | | | | |-encryption      --data encryption
| | | | | |-hide-network-name --hide network name
| | | | | |-key1            --wireless wep key 1
| | | | | |-key2            --wireless wep key 2
| | | | | |-key3            --wireless wep key 3
| | | | | |-key4            --wireless wep key 4
| | | | | |-keyno          --key number
| | | | | |-name            --profile name
| | | | | |-presharedkey    --pre-shared key
| | | | | |-security-separation --disable associated wireless client
communication
| | | | | |-ssid            --network name (1-32 chars)
| | | | | |-status          --profile status
| | | | | |-vlan-id         --VLAN id
| | | | | |-wep-pass-phrase  --wireless wep passphrase key
| | | | | |-wepkeytype       --wireless wep key type
| | | | |
| | | | | -7>                --7th security profile
| | | | | |-authentication  --authentication type
| | | | | |-encryption      --data encryption
| | | | | |-hide-network-name --hide network name
| | | | | |-key1            --wireless wep key 1
| | | | | |-key2            --wireless wep key 2
| | | | | |-key3            --wireless wep key 3
| | | | | |-key4            --wireless wep key 4
| | | | | |-keyno          --key number
| | | | | |-name            --profile name

```

```

| | | | | | | -presharedkey      --pre-shared key
| | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | | -ssid              --network name (1-32 chars)
| | | | | | | -status            --profile status
| | | | | | | -vlan-id           --VLAN id
| | | | | | | -wep-pass-phrase  --wireless wep passphrase key
| | | | | | | -wepkeytype       --wireless wep key type
| | | | | | |
| | | | | | | -8>                --8th security profile
| | | | | | | -authentication  --authentication type
| | | | | | | -encryption       --data encryption
| | | | | | | -hide-network-name --hide network name
| | | | | | | -key1             --wireless wep key 1
| | | | | | | -key2             --wireless wep key 2
| | | | | | | -key3             --wireless wep key 3
| | | | | | | -key4             --wireless wep key 4
| | | | | | | -keyno           --key number
| | | | | | | -name            --profile name
| | | | | | | -presharedkey    --pre-shared key
| | | | | | | -security-separation --disable associated wireless client
communication
| | | | | | | -ssid              --network name (1-32 chars)
| | | | | | | -status            --profile status
| | | | | | | -vlan-id           --VLAN id
| | | | | | | -wep-pass-phrase  --wireless wep passphrase key
| | | | | | | -wepkeytype       --wireless wep key type
| | | | | | |
| | | | | | | -wireless-bridge>    --wireless bridge setting
| | | | | | | -security-profile> --create security profile
| | | | | | | -1>                --1st security profile
| | | | | | | | -authentication --authentication type
| | | | | | | | -encryption   --data encryption
| | | | | | | | -name         --profile name
| | | | | | | | -presharedkey --preshared key
| | | | | | | | -remote-mac  --remote MAC
| | | | | | | | -status       --profile status
| | | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | | -wepkey       --wireless wep key
| | | | | | | | -wepkeytype  --wireless wep key type
| | | | | | |
| | | | | | | -2>                --2nd security profile
| | | | | | | | -authentication --authentication type
| | | | | | | | -encryption   --data encryption
| | | | | | | | -name         --profile name
| | | | | | | | -presharedkey --preshared key
| | | | | | | | -remote-mac  --remote MAC

```

```

| | | | | | -status          --profile status
| | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | -wepkey          --wireless wep key
| | | | | | -wepkeytype      --wireless wep key type
| | | | | |
| | | | | | -3>          --3rd security profile
| | | | | | | -authentication --authentication type
| | | | | | | -encryption      --data encryption
| | | | | | | -name          --profile name
| | | | | | | -presharedkey  --preshared key
| | | | | | | -remote-mac    --remote MAC
| | | | | | | -status        --profile status
| | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | -wepkey        --wireless wep key
| | | | | | | -wepkeytype    --wireless wep key type
| | | | | |
| | | | | | -4>          --4th security profile
| | | | | | | -authentication --authentication type
| | | | | | | -encryption      --data encryption
| | | | | | | -name          --profile name
| | | | | | | -presharedkey  --preshared key
| | | | | | | -remote-mac    --remote MAC
| | | | | | | -status        --profile status
| | | | | | | -wep-pass-phrase --wireless wep passphrase key
| | | | | | | -wepkey        --wireless wep key
| | | | | | | -wepkeytype    --wireless wep key type
| | | | | |
| | | | | | -wmm>          --wmm settings
| | | | | | | -ap-data0-best-effort --access point best effort voice data
| | | | | | | -ap-data1-background --access point low-priority data
| | | | | | | -ap-data2-video    --access point video data
| | | | | | | -ap-data3-voice    --access point voice data
| | | | | | | -station-data0-best-effort --station best effort voice data
| | | | | | | -station-data1-background --station low-priority data
| | | | | | | -station-data2-video    --station video data
| | | | | | | -station-data3-voice    --station voice data
| | | | | | | -support          --support
| | | | | |
| | | | | | -ip>          --set host IP
| | | | | | | -address        --host IP address
| | | | | | | -default-gateway --IP address of default gateway
| | | | | | | -dhcp-client    --enable dhcp client
| | | | | | | -dns-server     --IP address of DNS server
| | | | | |
| | | | | | -log>          --syslog setting

```



```

| | | -syslog                --enable syslog client
| | | -syslog-server-ip      --syslog server IP address
| | | -syslog-server-port   --syslog server port number
| |
| | | -radius>
| | | | -accounting-server-primary          --primary accounting server
| | | | -accounting-server-primary-port    --primary accounting server port
| | | | -accounting-server-primary-sharedsecret --primary accounting server shared
secret
| | | | -accounting-server-secondary        --secondary accounting server
| | | | -accounting-server-secondary-port  --secondary accounting server port
| | | | -accounting-server-secondary-sharedsecret --secondary accounting server
shared secret
| | | | -authentication-server-primary      --primary authentication server
| | | | -authentication-server-primary-port --primary system accounting
server shared secret
| | | | -authentication-server-primary-sharedsecret --primary authentication
server shared secret
| | | | -authentication-server-secondary    --secondary authentication server
| | | | -authentication-server-secondary-port --secondary authentication server
port
| | | | -authentication-server-secondary-sharedsecret --secondary authentication
server shared secret
| |
| | | -remote>                --enable remote access via SSH
| | | | -ssh-port              --SSH port
| | | | -sshd                  --SSH daemon
| | | | -telnet                --enable remote access via Telnet
| |
| | | -snmp>                  --SNMP setting
| | | | -description           --SNMP system description
| | | | -read-community         --SNMP ReadCommunity
| | | | -snmp-status           --SNMP status
| | | | -trap-community        --SNMP ReadCommunity
| | | | -trap-server           --SNMP TrapServer IP address
| | | | -write-community       --SNMP WriteCommunity
| |
| | | -spanning-tree          --enable spanning tree protocol
| | | -time>                 --time Setting
| | | | -custom-ntp-server     --custom NTP server host name
| | | | -daylightsaving        --daylight saving
| | | | -ntp-client            --NTP client host name
| | | | -ntp-server            --NTP server host name
| | | | -time-zone            --time zone
| |
| | | -vlan>                  --vlan settings
| | | | -management-vlan      --vlan management id
| | | | -untagged-vlan        --untagged vlan id

```

```
| | | -untagged-vlan-status          --untagged vlan status
| |
| -exit                             --logout from CLI
| -file                             --
| -firmware-upgrade                 --upload new system firmware file
| -password                         --system password
| -restore-configuration             --restore system configuration
| -restore-default-password         --restore default system password
| -show>                             --show system settings
| | -configuration                  --show system configuration
| | -interface>                     --show wireless lan interface
| | | -eth>                         --ethernet interface
| | | | -statistics                 --show ethernet statistics
| | |
| | | -wlan>                         --wlan interface settings
| | | | -2.4GHz>                   --2.4GHz wlan interface settings
| | | | | -configuration            --interface configuration
| | | | | -knownaplist              --known access point list
| | | | | -stationlist              --station list
| | | | | -statistics                --interface statistics
| | | | | -trusted-stationlist      --trusted station list
| | | | | -unknownaplist            --unknown access point list
| | | |
| | |
| |
| | -log                             --system log
| | -system                          --system setting
```

Numerics

- 20 MHz *2-15*
- 20/40 MHz *2-15*
- 40 MHz *2-15*
- 802.11b/g/n *1-4, 2-13*
 - default SSID *2-10*
 - standards compliance *1-2*
- 802.11e *1-3, 2-16, 4-6*
- 802.11n
 - data encryption option, recommendation *2-3*
- 802.1Q *2-27*
- 802.1Q VLAN, support *1-2*
- 802.1x *2-20*
- 802.3af *1-3*

A

- access control
 - MAC address filtering *1-3*
 - MAC authentication *2-38*
 - trusted wireless stations *1-3*
- access control list
 - MAC authentication *2-38*
- access point mode
 - security options *2-20*
- access point name *2-5*
- access point, more than one *2-15*
- ACK *1-4*
- activity log *3-12*
- AES
 - 802.11n, recommended for *2-3*
 - with WPA2, with RADIUS *2-32*
 - with WPA2-PSK *2-36*
- aggregation length *4-6*

- aggregation, support for *1-4*
- AID see association ID
- A-MPDU (Aggregation of MAC Protocol Data Units) *4-6*
- antenna *4-6*
 - 2.4 GHz *1-5*
 - position *2-2, 2-9*
- associated stations
 - present in AWSL, only *3-16*
- association ID
- authentication server settings
 - IP address *2-24*
 - port number *2-24*
 - shared secret *2-24, 2-25*
- auto or long preamble, support for *1-4*
- Auto UplinkTM *1-4*
- autosensing ethernet, support for *1-3*
- autosensing, LAN interface *1-4*
- available wireless station list (AWSL) *3-16*
- available wireless stations list *2-39*
- AWSL table fields
 - channel *3-16*
 - MAC address *3-16*
 - mode *3-16*
 - rate *3-16*
 - SSID *3-16*
 - state *3-16*
 - status *3-16*
 - type *3-16*
 - wireless network name (SSID) *3-16*

B

- back off *1-4*
- Basic Service Set (BSS) *1-2*
- Basic Service Set Identifier (BSSID) *1-2*

- beacon generation, support for *1-4*
- beacon interval *4-5*
- bridge
 - network authentication *2-20*
- bridge mode wireless station
 - wireless point to point bridge *4-8*
 - wireless point-to-multi-point bridge *4-8*
- BSSID *3-16*

C

- Category 5 Ethernet cable *1-5*
- change password *3-10*
- channel auto
 - testing connectivity *2-17*
- channel auto selection *2-17*
- channel interference *2-17*
- channel spacing *2-3*
- channel spacing, recommended *2-15*
- channel, auto
 - configuring channel/frequency *2-14*
- channel, default *2-14*
- CLI
 - command set *3-4*
- command line interface (CLI) *3-3*
- configuration file *3-6*
 - backup or restore *3-7*
- conventions, typographical *1-i*
- coverage *2-2*
- coverage area *1-1, 2-9*
- CSMA/CA *4-5*
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection) *4-5*
- CTS (Clear to Send) *4-5*

D

- data encryption settings
 - 128 bits WEP *2-21*
 - 152 bits WEP *2-21*
 - 64 bits WEP *2-21*
 - AES *2-21*

- none *2-21*
- TKIP *2-21*
- TKIP + AES *2-21*
- data rates 802.11bgn *2-15*
- default access point name *2-6*
- default channel *2-14, 2-17*
- default gateway, configure *2-12*
- default IP address *2-4, 2-12*
- default password *2-4*
- default reset button *3-9*
- default SSID *2-10*
- default user name *2-4*
- default wireless access point name *2-10*
- DHCP
 - point-to-multi-point bridging *4-14*
- DHCP client
 - default setting *2-10*
- DHCP client, configure *2-12*
- DHCP client/server
 - support *1-2*
- DHCP server
 - configure *4-1*
 - on LAN *2-12*
 - on LAN, assigns IP address *2-10*
- distributed coordinated function, support for *1-4*
- documentation *2-5*
- DTIM (Delivery Traffic Indication Message) interval *4-6*
- dynamic encryption key generation, support *1-2*
- dynamic IP address, configure *2-10*
- dynamic per frame rekeying *2-3*

E

- EDCA (Enhanced Distributed Channel Access) *4-7*
- Ethernet
 - RJ-45 port *1-6*
- ethernet cable, connect *2-10*

F

- factory default settings *3-6*

- reset button *1-6, 5-4*
- resetting *5-4*
- restore *3-8*
- table *A-1*

- firmware
 - upgrade *3-6*

- FLASH *3-5*

- formats, document *1-i*

- fragmentation *4-5*

- fragmentation threshold *4-5*

- full-duplex *1-4*

H

- half-duplex *1-4*

- hidden mode, support for *1-3*

- hotspot

- server settings *4-3*
 - support for *1-3*
 - wireless client security separation *2-28*
 - wireless client security separation *2-30, 2-32, 2-33, 2-35, 2-36, 2-37*

- HTTP redirect

- hotspot settings *4-3*

I

- interference, channel settings *2-14*

- interference, least *2-14*

- interference, reduce *2-3, 2-15*

- interference, sources *2-2*

- IP address

- configure *2-7, 2-12*

- IP settings, configure *2-11*

K

- keys, use with WEP *2-21*

L

- LAN IP address

- default *5-3*

- latency *2-2*

- legacy rates *2-3*

- line of sight *2-9*

- location *2-2, 2-9*

- log in *2-11*

- logs *3-11, 3-12*

M

- MAC address

- access control list *2-38*
 - bridge mode wireless station *4-8*
 - wireless point-to-multi-point bridge *4-8*

- MAC authentication

- available wireless stations list *2-39*
 - MAC address database, local *2-39*
 - MAC address database, RADIUS *2-39*
 - trusted wireless stations *2-39*
 - turn access control on *2-39*

- Management Information Base (MIB) management *1-2*

- max users *1-1*

- maximum packet size *4-5*

- multiple access points

- placement of *2-3*

- multiple BSSIDs, support for *1-2*

- multiple input, multiple output (MIMO), support for *1-4*

- multi-point bridging

- extend *4-14*

N

- NetBIOS name *2-6*

- network authentication, types of

- legacy 802.1x *2-20*
 - open system *2-20*
 - shared key *2-20*
 - WPA and WPA2 with RADIUS *2-20*
 - WPA with RADIUS *2-20*
 - WPA2 with RADIUS *2-20*
 - WPA2-PSK *2-20*
 - WPA-PSK *2-20*
 - WPA-PSK and WPA2-PSK *2-20*

- network key

- with WPA-PSK and WPA2-PSK 2-37
- WPA-PSK 2-35

- network statistics 3-14
 - fields 3-15

- NTP client, configure 2-8

- NTP server, configure 2-8

O

- operating frequency 1-2

- operating modes, supported
 - point-to-multi-point bridge 1-3
 - point-to-point bridge 1-3
 - wireless access point 1-2

P

- package contents 1-5

- packet fragmentation, support for 1-4

- packet size 4-5

- passphrase, use with WEP 2-21, 2-28

- password
 - change 3-10

- performance degradation
 - causes of 2-2

- placement 2-2

- point-to-multi-point bridge 4-8
 - configure 4-13

- point-to-point bridge 4-8
 - configure 4-12

- point-to-point bridge mode
 - wireless point-to-multi-point bridge 4-8

- power adapter 1-6

- power consumption 2-2

- Power over Ethernet (PoE), support for 1-3

- preamble type 4-6

- preshared key passphrase
 - WPA-PSK 2-35

- primary DNS server, configure 2-12

- profile name
 - bridge mode wireless station 4-8
 - wireless point-to-multi-point bridge 4-9

Q

- QoS queues 4-7

- QoS settings 2-16

- QoS settings, advanced
 - AP EDCA parameters 4-7
 - station EDCA parameters 4-7

R

- RADIUS and certificate authentication, support 1-2

- RADIUS server, configure 2-23
 - accounting server 2-24
 - authentication server 2-24

- RADIUS server, configure first 2-18, 2-25

- range 1-1
 - guidelines 2-2

- rear panel 1-5

- reboot 3-9
 - reset button, using 5-4

- rebooting
 - losing previous state 3-17

- reception 2-2

- redirect HTTP 4-3

- redirect URL
 - hotspot settings 4-4

- reduced inter frame spacing, support for 1-4

- remote console
 - secure shell (SSH) 3-3
 - Telnet 3-3

- request to send threshold 4-5

- reset button 3-9

- reset to factory defaults 3-9

- retransmission 1-4

- RIFS
 - wireless settings 4-6

- roaming
 - multiple wireless access points 3-16

- roaming on same subnet, support for 1-4

- rogue AP detection
 - configure 3-17
 - import rogue AP list from file 3-18

- support for 1-3
- unknown AP list 3-18
- rogue AP list 3-19
 - unknown AP list 3-19, 3-21
- RTS 4-5
- RTS/CTS handshake, support for 1-4

S

- secure Telnet CLI, support for 1-3
- secure Telnet client 3-3
- secure Telnet interface, using 3-3
- security profile
 - VLAN ID 1-4, 2-27
- security profile definition
 - authentication settings 2-20
 - broadcast wireless network name (SSID) 2-19
 - data encryption 2-21
 - security profile name 2-19
 - VLAN ID 2-21
 - wireless client security separation 2-21
 - wireless network name (SSID) 2-19
- security profile, support for 1-3
- security profiles
 - about 2-18
- security profiles, setting up 2-25
- security profilee
 - wireless client security separation 2-27
- serial console port, connectors 1-6
- Service Set Identifier (SSID)
 - max per radio mode 1-2
- setup form 2-22
- SNMP
 - enable SNMP 3-2
 - read-only community name 3-2
 - read-write community name 3-2
 - receive traps IP address 3-2
 - remote management 3-1
 - trap community name 3-2
 - trap port 3-2
- SNMP (Simple Network Management Protocol), support 1-2
- software upgrade 3-5

- SSID 2-14
 - hidden mode 1-3
- SSID broadcast, disable 2-19
- SSID match
 - verify connectivity 2-10
- SSID, wireless network name 2-19
- standards, supported 1-2
- static IP address 5-3
 - default 2-4
- statistics 3-14
- subnet mask
 - default 5-3
- support documentation 2-5
- syslog server
 - setup 3-11
- system information 3-12
 - fields 3-13
- system requirements 1-4

T

- technical specifications A-3
- Telnet client
 - recommendations 3-3
- Telnet options 3-3
- terminal-emulation program, configure 3-4
- throughput performance 2-2
- timezone, configure 2-6, 2-8
- timezone, default 2-8
- TKIP
 - data rates, provided by 2-3
 - with WPA, with RADIUS 2-30
 - with WPA-PSK 2-35
- TKIP+AES
 - with WPA and WPA2, with RADIUS 2-33
 - with WPA-PSK + WPA2-PSK 2-37
- transmit power 2-15
- Trap 3-2
- troubleshooting 5-1
 - access point, connecting to 5-3
 - configuring, 5-3

- LAN activity 5-2
- power connection 5-1
- timeout error 5-3
- wireless Internet connection 5-2
- wireless LAN activity 15-2

trusted wireless stations list

- MAC authentication 2-39

U

- unauthorized access, secure from 2-1
- upgradeable firmware, support for 1-3

V

- VLAN (802.1Q) 2-27
- VLAN ID
 - DHCP server 4-2
- VLAN security profiles (VLAN ID), support for 1-4
- Voice-over-IP (VoIP) 4-6

W

- WEP
 - data rates, provided by 2-3
- WEP, configure
 - data encryption keys 2-28
 - data encryption strength 2-28
 - network authentication type 2-27
 - wireless client security separation 2-28
- Wi-Fi Multimedia (WMM) 4-6
- Wi-Fi Protected Access (WPA) 2-3
- wired equivalent privacy (WEP) 2-3
- wireless access point
 - software 3-5
- wireless access point name 2-10
- wireless adapter
 - verifying connectivity 2-10
- wireless adapter, settings 2-18
- wireless adapters
 - WPA support, restriction 2-29
 - WPA2 support, restriction 2-31
- wireless bridging and repeating 4-8

- wireless channel
 - changing 2-14, 2-17
- wireless client
 - point-to-point bridge communication 4-8
- wireless client security separation
 - hotspot setting 2-28
- wireless computer, configuring from 2-29
- wireless connection
 - losing 2-38
- wireless connection, losing 2-18
- wireless connectivity, testing 2-17
- Wireless Multimedia (WMM) 2-16
- Wireless Multimedia (WMM), support for 1-3
- Wireless Multimedia Extension (WME) 4-6
- wireless network name (SSID) 2-26
- wireless point-to-multi-point bridge 4-8
- wireless point-to-point bridge 4-8
- wireless security options
 - restrict access based on MAC address. 2-3
 - turn off broadcast of wireless network name (SSID) 2-3
 - WEP, use 2-3
 - WPA or WPA-PSK, use 2-3
- wireless settings 802.11b/bg/ng, advanced
 - aggregation length 4-6
 - A-MPDU 4-6
 - antenna 4-6
 - beacon interval 4-5
 - DTIM interval 4-6
 - fragmentation length 4-5
 - preamble type 4-6
 - RIFS transmission 4-6
 - RTS threshold 4-5
- wireless settings 802.11bgn
 - broadcast wireless network name (SSID) 2-14
 - channel width 2-15
 - channel/frequency 2-14
 - guard interval 2-15
 - MCS index/data rate 2-15
 - output power 2-15
 - turn radio on 2-14
 - wireless mode 2-14
 - wireless network name (SSID) 2-14

- wireless settings, basic 2-9
- wireless sniffer 2-3
- WPA and WPA2 with RADIUS
 - restriction with WPA and WPA2 2-32
- WPA and WPA2 with RADIUS, configure 2-33
 - data encryption 2-33
 - network authentication type 2-33
 - wireless client security separation 2-33
- WPA preshared key passphrase, use with WPA-PSK 2-21
- WPA with RADIUS, configure 2-29
 - data encryption default 2-30
 - network authentication type 2-30
 - wireless client security separation 2-30
 - WPA with RADIUS, restrictions 2-29
- WPA/WPA2
 - use restrictions 2-20
- WPA/WPA2, support for 1-2
- WPA2 with RADIUS, configure 2-31
 - data encryption default 2-32
 - network authentication type 2-32
 - wireless client security separation 2-32
- WPA2-PSK, configure
 - data encryption 2-36
 - network authentication type 2-36
 - preshared key passphrase 2-36
 - restrictions using WPA2 2-35
 - wireless client security separation 2-36
- WPA-PSK and WPA2-PSK preshared key authentication, support 1-2
- WPA-PSK and WPA2-PSK, configure
 - data encryption 2-37
 - network authentication setting 2-37
 - restrictions using WPA/WPA2 2-36
 - wireless client security separation 2-37
 - WPA passphrase (network key) 2-37
- WPA-PSK, configure
 - data encryption 2-35
 - network authentication type 2-35
 - preshared key passphrase 2-35
 - restrictions for WPA 2-34
 - wireless client security separation 2-35

