User Guide

Ruckus Wireless
ZoneFlex 2925/2942/7942 Access Point

Legal Information

Trademarks

Ruckus Wireless ZoneFlex™ 2825/2925/2942 Access Points, BeamFlex™, MediaFlex™, MediaFlex 2900 Multimedia Access Point, MediaFlex 2501 Multimedia Wireless Adapter, 2825 Wireless Multimedia Router, 2111 Wireless Multimedia Adapter, and MM2211/MM2225 Metro Broadband Gateways are trademarks of Ruckus Wireless Web Interface

All other brands and product names are registered trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Ruckus Wireless, Inc. reserves the right to make changes to the products described in this document without notice.

Ruckus Wireless, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Information to the user

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

22 Class B (CISPR 22).(Other agency certifications go here)

Part number: USM-ZF2925-RKS1-072507-01

EDITION: July 25, 2007 -- vA

Contact Information

Headquarters — United States

Telephone

U.S.: +1 408-111-2345

Support

http://www.ruckuswireless.com

Web/email

www.ruckuswireless.com

Contents

CHAPTER 1

Are You a Wi-Fi Hotspot Operator?

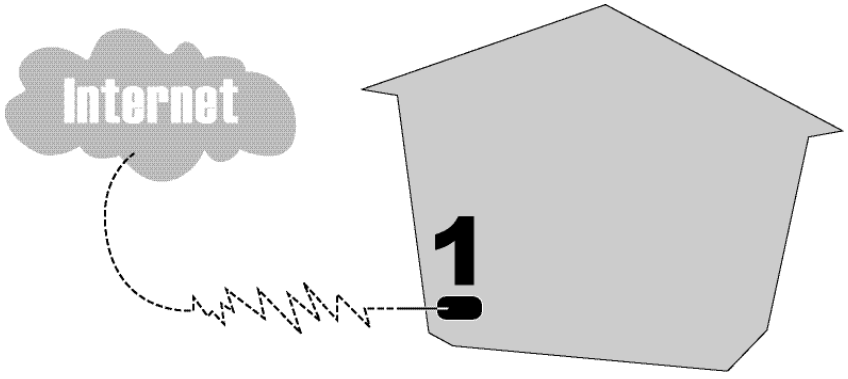
Then you'll appreciate learning about your new Ruckus Wireless hotspot access point, before you get started.

What can a Hotspot Access Point do for you?

You're occupying a large space, with lots of users, and you'd like to make it a Wi-Fi hotzone.

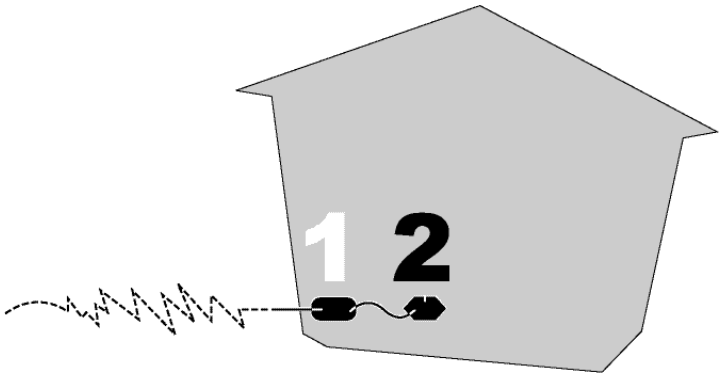
Let's make it easy for you; there's an active Internet connection from a local ISP (DSL, cable or other), and you've got a modem—as shown here.

FIGURE 1-1



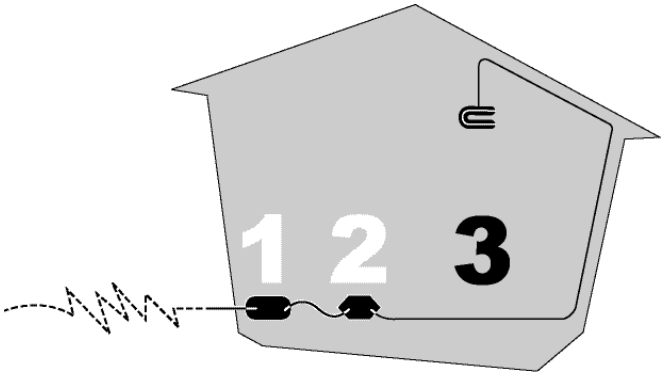
Is there a switch connected to the modem? If not, you'll need to hook one up to your modem—as shown below.

FIGURE 1-2



After preparing the Ruckus Wireless AP for network use, you can place it (as shown below) where it can broadcast the strongest signal to as many users as possible.

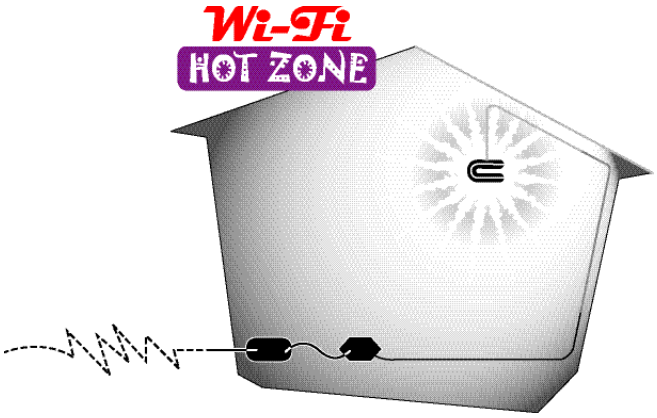
FIGURE 1-3



As the picture suggests, you should mount it high on the wall or on the ceiling.

After you mount the AP, then connect it to the switch and power it up, your hotspot/hot-zone is ready for use—as shown below.

FIGURE 1-4



Where exactly should you place the Access Point?

After you've prepared the AP for network hotspot connections, you should place it in the most strategic place in your work/business site. That means two things:

- You want the AP as "visible" as possible to as many potential users, and
- You don't want it near anything that would impede the signal

Helpful recommendations are listed in *"Placing the AP in your site"* on page14.

What you should know before starting

To install, set up and customize a new AP you must use the following:

- A desktop or laptop computer, running Microsoft Windows 2000 or XP.

You must also use one of the following Web browsers for setup:

- Internet Explorer version 6.0 and later
- Netscape version 8.1 and later
- Firefox version 1.5.0.6 and later

What's next?

Now you can get started configuring your new Ruckus Wireless AP for use, as described in the next chapter.

CHAPTER 2

Installation, Setup, and Placement of the AP

This chapter describes how to set up a Ruckus Wireless Hotspot access point for use in a Wi-Fi hotzone. This includes an important preliminary task: reconfiguring your PC/laptop to connect to the Ruckus AP through the Web User Interface. At the conclusion of setup, this chapter will guide you in resetting your PC for normal use, then guide you in placing and connecting your Wireless Hotspot AP for use.

NOTE

This chapter repeats the same information that you may already have read in the companion publication *Quick Setup Guide* (QSG). But this chapter adds a few more technical details, and is included for the benefit of any readers who don't have a copy of the QSG and who want to prepare their hotspot AP for use.

Chapter Contents

What's in the Package

When you first open the package, you should find one of each of the following:

- A Ruckus Wireless ZoneFlex 2925, 2942 or 7942 Access Point
- A 3-foot (0.9 meter) Cat5 Ethernet cable
- A power supply adapter
- A wall mounting kit, plus printed instructions

Before proceeding, review the following section to familiarize yourself with the physical features of the access point (AP).

Features of the Access Point

ZF2925 Features

The following illustration shows the front view of a ZF2925 AP, highlighting the four LED indicators that can be used to assess both device and network status.

FIGURE 2-1: Front view

[1] Power
[2] WAN Connectivity
[3] Wireless Device Association
[4] Signal Quality

For more information on what each LED's lights may indicate, see the "LED" table on the next page.

LED	If you see this...	This is happening...
	• If this LED is dark.	• No power is available, or the AP is not connected to a power source.
	• If green	• Power is available.
	• If this LED is dark.	• No link activity is detected
	• If steady yellow.	• A 10Mbps-capable device has been detected.
	• If flashing yellow.	• Data is being exchanged through the WAN port at 10Mbps.
	• If steady green.	• A 100Mbps-capable device has been detected.
	• If flashing green	• Data is being exchanged through the WAN port at 100Mbps.
	• If this LED is dark.	• No WLAN is enabled.
	• If amber	• One of the WLANs is enabled, but no wireless client has associated.
	• If green	• At least one wireless client has associated.
	• If this LED is dark.	• There is no network activity; no station detected at the WLAN port
	• If red	• There is a hardware problem affecting the WLAN port.
	• If blinking red/green alternately .	• A signal is being detected at the WLAN port, but at the lowest level.
	• If flashing green	• A moderate signal is being detected at the WLAN port.
	• If steady green.	• A strong signal is being detected at the WLAN port.

The following illustration shows the rear view of the ZF2925 AP and its major features.

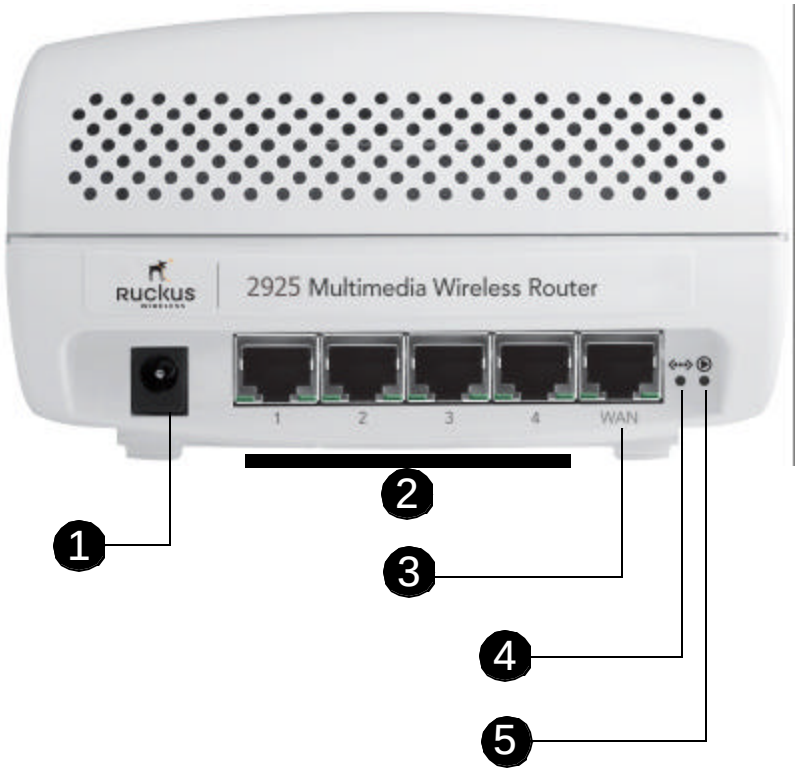


FIGURE 2-2: Rear view

[1] Power Adapter plug

Connect the power adapter to this socket. (Input 12V 1.0A DC or 5V 2.0A DC)

[2] LAN ports

Four RJ-45 ports, supporting 10/100 Mbps connections

[3] WAN Network port

One RJ-45 port, dedicated to ISP/ broadband source connection

[4] "OTA" (Over the air) button

Not active in this model at this time

[5] Reset button

[-IF NEEDED-] Use to reset AP to "factory default" state

2942/7942 Features

The following illustration shows the side view of a ZF2942/ZF7942 AP, highlighting the four LED indicators that can be used to assess both device and network status.

FIGURE 2-3: Side view

[1] OPT

[2] DIR

[3] AIR

[4] WLAN

[5] Hard Reset: Pushing this internal button and releasing quickly reboots the AP. Holding it for 6 seconds resets the AP to factory defaults.

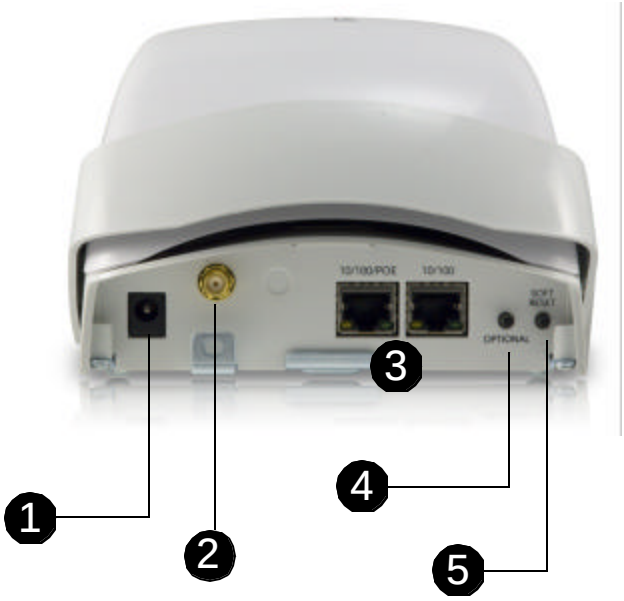
For more information on what each LED's lights may indicate, see the "LED" table below.

LED	If you see this...	This is happening...
Power	• If this LED is steady green . . . . . • If off	• Power is ON. • No power is connected.
OPT	N/A	Optional feature. Not active in this model at this time.
DIR	• If this LED is steady green . . . . . • If this LED is steady green for 2-3 seconds . . . . . . • If flashing green . . . . . . • If off	• Communication between Director and AP is up. • The AP is booting up. • Communication between Director and AP is down. • AP is not under Director control.
AIR	• If off . . . . . . • If blinking red/amber alternately . • If blinking red/green alternately . • If flashing green . . . . . . • If steady green.	• There is no station associated. • AP is booting up. • Wireless data traffic is unreachable. • Wireless data traffic is reachable. • Good air quality.

LED	If you see this...	This is happening...
WLAN	• If steady yellow. . . . . . • If steady green.	• No wireless client are associated. • At least one wireless station is associated. Also steady green during boot up.
10/100 POE	• If off . . . . . . • If steady amber. . . . . . • If flashing amber. . . . . . • If steady green. . . . . . • If flashing grren.	• Port is not connected. • Ethernet port is connected to 10Mbs Layer 2 device. • Ethernet port is passing traffic to a 10Mbs Layer 2 device.Ethernet port is connected to 100Mbs Layer 2 device. • Ethernet port is passing traffic to a 100Mbs Layer 2 device.
10/100	• If off . . . . . . • If steady amber. . . . . . • If flashing amber. . . . . . • If steady green. . . . . . • If flashing grren.	• Port is not connected. • Ethernet port is connected to 10Mbs Layer 2 device. • Ethernet port is passing traffic to a 10Mbs Layer 2 device.Ethernet port is connected to 100Mbs Layer 2 device. • Ethernet port is passing traffic to a 100Mbs Layer 2 device.

The following illustration shows the rear view of the ZF2942/ZF7942 AP and its major features.

FIGURE 2-4: Rear view



[1] Power Adapter plug

Connect the power adapter to this socket. (Input 110-240V AC, Output 12V 1.0A DC)

Power can also be supplied via 10/100 POE port.

[2] External RP-SMA connector

Optional external antenna connector.

[3] LAN ports

Two RJ-45 ports, supporting 10/100 POE (Power over Ethernet) and 10/100 Mbps connections.

[4] Optional button

Not active in this model at this time.

[5] Soft Reset button

[-IF NEEDED-] Use to reset AP. This is a normal reset and does not set AP back to factory defaults.

Preparing the Access Point for Network Use

The following sections detail how to use your PC/laptop to manually set up the AP to function as an auto-activating multimedia wireless hotspot.

What you'll be doing

- Reconfigure the local area network settings on your PC
- Power up the AP and connect it directly to the Ethernet network port on your PC
- Using a browser, log into the Ruckus Wireless Web Admin UI on the AP.
- Enter the AP setup entries and save them
- Log out, exit the browser, and disconnect/power off the AP.
- The AP is now ready for onsite placement and activation.

Requirements

Make sure you have the following before starting this process:

- A modem (DSL or cable), E1/T1 router, or other device provided by your Internet Service Provider, that brings web access to your site
- (Optional) A network switch or a DSL/Internet gateway device.
- A computer (desktop or laptop) running Windows 2000 or XP with a recent-version web browser

Note	**Important!** If the AP is deployed with a ZoneDirector, follow the ZoneDirector *Quick Setup Guide*, and connect the AP to your Ethernet network.

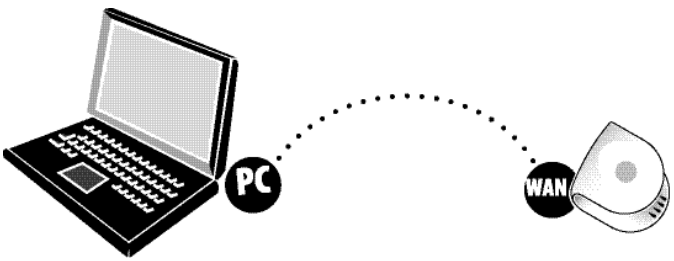
1 Connecting the AP to your PC

1 After unpacking your Ruckus Wireless access point from the package, place it next to your PC/laptop.

2 Temporarily disconnect your PC/laptop from any local wired network (if connected).

3 Using the Ethernet cable provided in the Ruckus package, connect your PC/laptop network port to one of the four LAN ports on the back of the AP.

FIGURE 2-5



- DON'T CONNECT the cable to the AP's WAN port for this task.

4 Using the AC adapter included in the package, connect the AP to a convenient (and protected) power source. After a minute, verify that the AP's Power LED is a steady green.

2 Preparing your PC for AP Setup

1 On your Windows 2000 or XP PC, open the Network Connections (or Network and Dial-up Connections) control panel according to how the Start menu is set up:

- Start-> Settings-> Network Connections
- Start-> Control Panel-> Network Connections

2 When the Network Connections window appears, right-click the icon for "Local Area Connection" and choose **Properties**.

ALERT Make sure you don't open the Properties dialog box for the wireless network.

3 When the Local Area Connection Properties dialog box appears, select **Internet Protocol (TCP/IP)** from the scrolling list, and click **Properties**.

The TCP/IP Properties dialog box appears.

NOTE **IMPORTANT!**—Write down all of the currently active settings so you can restore your computer to its current configuration when this process is complete.

4 Select **Use the following IP address** (if it's not already active) and make the following entries:

IP Address	192.168.0.22 (or any address in the 192.168.0.x network—with the exception of 192.168.0.1, which is already used by the AP)
Subnet mask	255.255.255.0
Default gateway	192.168.0.1
Preferred DNS server	192.168.0.1

- You can leave the **Alternate DNS server** field empty.

5 Click **OK** to save your changes and exit first the TCP/IP Properties dialog box, then the Local Area Connection Properties dialog box.

Your changes are put into effect immediately.

3 Logging into the AP

As specified earlier, the AP should be directly connected to your PC/laptop (through one of the LAN ports), and have been powered up, ready for setup.

1 Verify that the AP's Power LED is a steady green.

2 On the PC, open a web browser window.

3 In the browser, type the following IP address to connect to the AP:

https://192.168.0.1

4 Press **Enter** to initiate the connection.

5 When a security alert dialog box appears, click **OK/Yes** to proceed.

6 When the Ruckus Wireless Admin login page appears, enter the following:

Username super

Password sp-admin

7 Click **Login**.

The *Ruckus ZoneFlex AP* management interface (the *Web User Interface*) appears in the browser window.

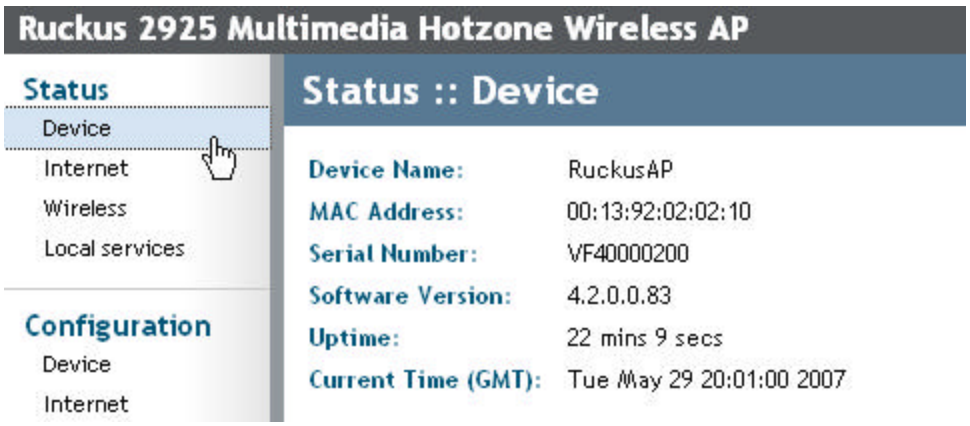


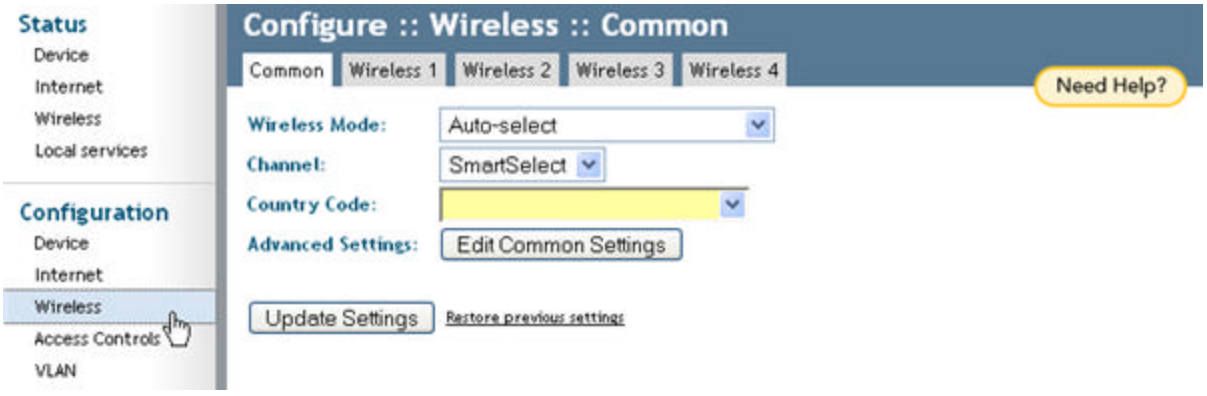
FIGURE 2-6

The "Status::Device" workspace is active—as shown above.

4 Customizing the Wireless Settings on the AP

1 In the left-hand menu bar of the Web User Interface, choose **Wireless** (under *Configuration*).

The Configure::Wireless::Common options appear.



2 Verify that the following "Common" settings are active:

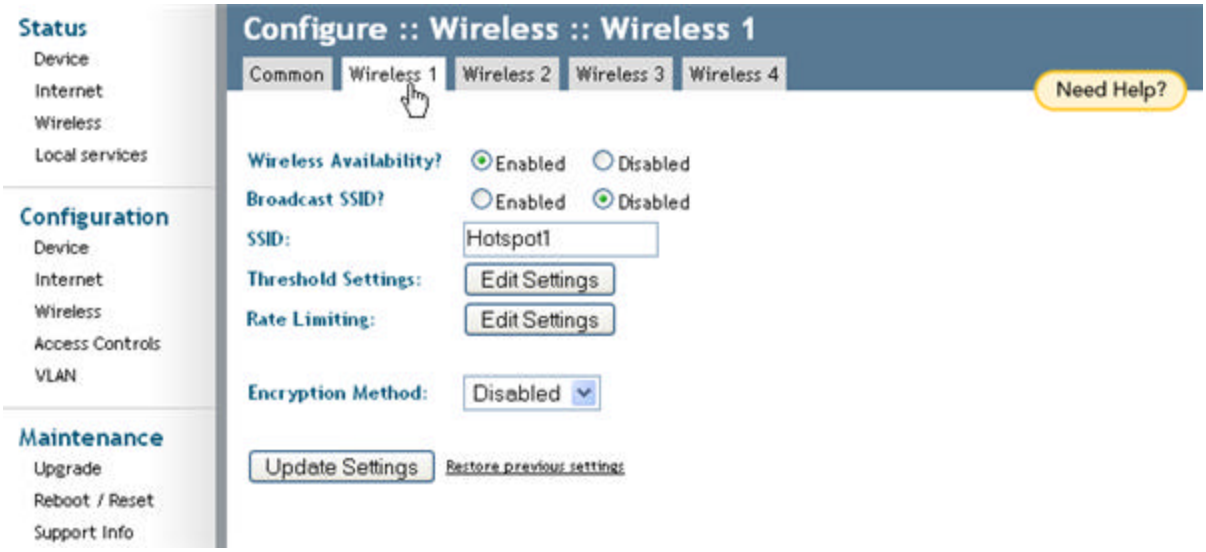
Wireless Mode "Auto-select" should be selected

Channel	"SmartSelect" should be selected
Country Code	If you are not in the United States, open this menu and choose the country.

3 Click **Update Settings** if you made any changes.

4 Click any of the four "Wireless" tabs.

The Configure::Wireless::Wireless [#] options appear.



5 Delete the text in the **SSID** field and type the name of your network.

(If your network doesn't have a "name", type a short name that relates to your site, plus a number. This will help your users identify the Wi-Fi network in their wireless network connection application.)

Each WLAN (e.g., Wireless 1, Wireless 2, etc.) should have its own unique SSID.

6 Click **Update Settings**.

7 Repeat the preceding steps with each Wireless tab.

Important!

If you anticipate logging into the AP to regularly perform monitoring or maintenance (once it is in place), you may want to consider assigning a static IP address to the AP. This would simplify connections made to the AP for all post-installation maintenance.

In a default configuration, the AP uses a DHCP-assigned IP address. Any post-installation connections require (1) a reverse ARP lookup or (2) logging into the DHCP server, to determine which IP address is in effect in the AP. If the AP is not assigned an IP address by a DHCP server, it will automatically revert to an IP address of 192.168.0.1.

8 [-*Steps 8-12 Optional*-] To switch from DHCP (the default) to Static IP, choose **Internet** (under *Configuration*).

The Configure::Internet options appear.

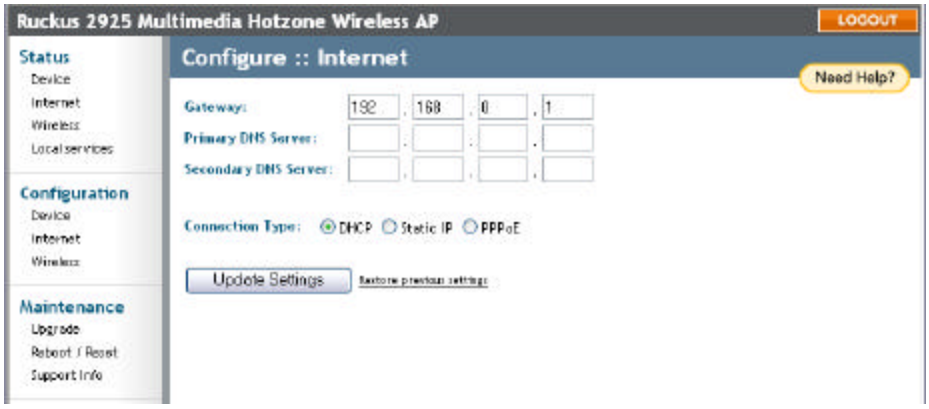


FIGURE 2-7

9 Click the button by **Static IP**.

10 Fill in the **IP Address** and **Mask** fields that appear.

Make sure you use a unique IP address that is not already taken by another device on your network. (For example, try pinging the IP address from your PC before assigning that address to the AP.)

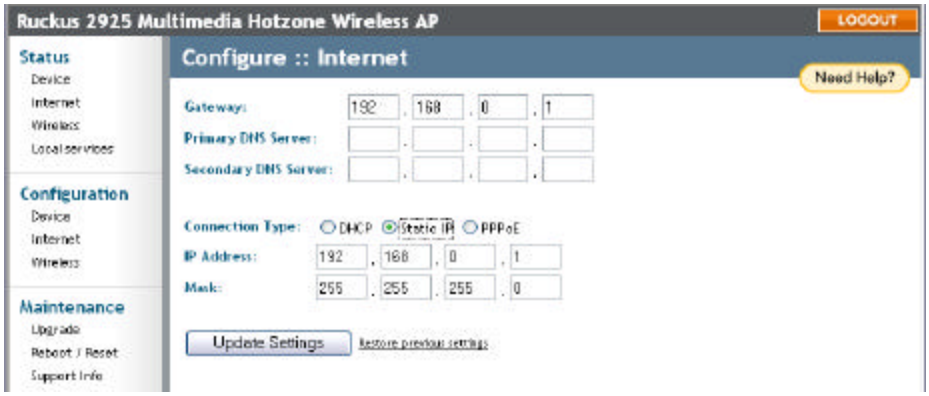


FIGURE 2-8

11 Click **Update Settings**.

12 Click **Logout** to exit the Web User Interface.

13 When the Web Admin login page reappears, you can exit your browser.

Disconnect the AP from the PC and from the current power source, and restore your PC to the normal network connections—as detailed in the next section.

5 Restoring your PC's network settings

To restore the network settings for your PC/laptop, do one of the following first steps, according to which OS your PC/laptop is using:

1 Click **Start** and choose Settings-> Network Connections.

- (If Windows 2000, click Start and choose Settings->Network and Dial-up Connections.)

2 When the Network Connections window appears, right-click the icon for the "Local Area Connection" designated for your home network and choose **Properties**.

3 When the Local Area Connection Properties dialog box appears, select **Internet Protocol (TCP/IP)** from the scrolling list, and click **Properties**.

The TCP/IP Properties dialog box appears.

4 Restore the entries from your standard network configuration.

5 Click **OK** to save your settings and exit first the TCP/IP Properties dialog box, then the Local Area Connection Properties dialog box.

Your PC/laptop is now ready for normal network use.

Extra: Default Network Configuration

FOR YOUR REFERENCE— When you first take the AP out of the box, these network settings are in effect:

Network names - SSIDs	Wireless1–Wireless4
Security (encryption)	Disabled for each WLAN
Default management IP	192.168.0.1

6 Placing the AP in your site

1 Disconnect the AP's power adapter from the power outlet.

2 Move the AP to its permanent location (accessible to both AC power and ISP connections). **TIP:** Use the wall-mount bracket to help secure the AP in an advantageous location on the wall or ceiling.

3 Follow these placement guidelines:

- Place the AP as close to the center of the space you want to cover, and away from any physical obstructions.
- Place the AP on a wall mount, on a shelf or other elevated location (ceiling) where the potential user's wireless networking devices are in line-of-sight access.
- Avoid any sources of electromagnetic interference.
- Avoid placing the AP near large metal or glass surfaces.

4 Use an Ethernet cable to connect the WAN port of the AP to the appropriate device:

- The ISP's modem or gateway device
- The Ethernet switch that is connected to the ISP's device

FIGURE 2-9

5 Connect the AP power adapter to the AP, then to a convenient power source.

6 Verify that the WAN port LED is lit, along with the activity LEDs on the front of the AP.

7 After a short pause to re-establish the Internet connection, you can test the AP.

7 Testing the newly placed AP

1 Using any wireless-enabled computer or mobile device, search for and select the wireless network you've previously configured.

2 Open a browser and link to any public Web site.

Congratulations! Your wireless network is active and ready for use.

Troubleshooting the Initial Setup Connection

If the startup sequence doesn't work, verify that the network name (SSID) and security settings on the AP match your wireless network.

- Disconnect the AP from the power source, wait 5 seconds, then reconnect it—and wait 60 seconds before attempting a reconnection.
- Disconnect and reconnect the AP and the PC.
- Replace the Ethernet cable with a new one if the relevant LAN port LED is not illuminated. (LEDs in each port light up during a successful connection.)

If all else fails, you can reset the AP to the factory defaults (and start over).

1 Insert a straightened-out paper clip into the reset button hole (located on the back of the AP.)

2 Press and hold the Reset button for at least eight (8) seconds.

3 You can now reconnect your PC directly to the AP (as described on *"Connecting the AP to your PC"* on page9) and start over with installation, using the default network settings.

What's Next?

Your Ruckus Wireless hotspot access point is now in place, serving your wi-fi network users. But there are additional settings you might want to adjust, to fine-tune and improve the performance of your AP and the whole wi-fi network. The next chapter will guide you through all of these options.

CHAPTER 3

After the Installation (Post-Installation Setup)

Browse this chapter for any relevant post-installation options you might wish to customize for your wi-fi network site. When you are finished, be sure to browse the following two chapters for specific guidance on monitoring and management tasks you can perform on your Ruckus Wireless AP and your wi-fi hotspot.

ALERT	Many of the following tasks should be undertaken only if you are an experienced network administrator or are under the guidance of your ISP or an IT/support professional.

Chapter Contents

Opening the Web User Interface

If you need to manage your AP, you do it with the features of the Ruckus Wireless Web User interface (which you already used to set up the AP for use).

ALERT	The following procedure assumes that you know the static IP address of the AP (now in use), or you have some means of determining the dynamic IP address in use by the AP. The PC you use for AP administration should be on the MGMT VLAN.

To open the Web User interface:

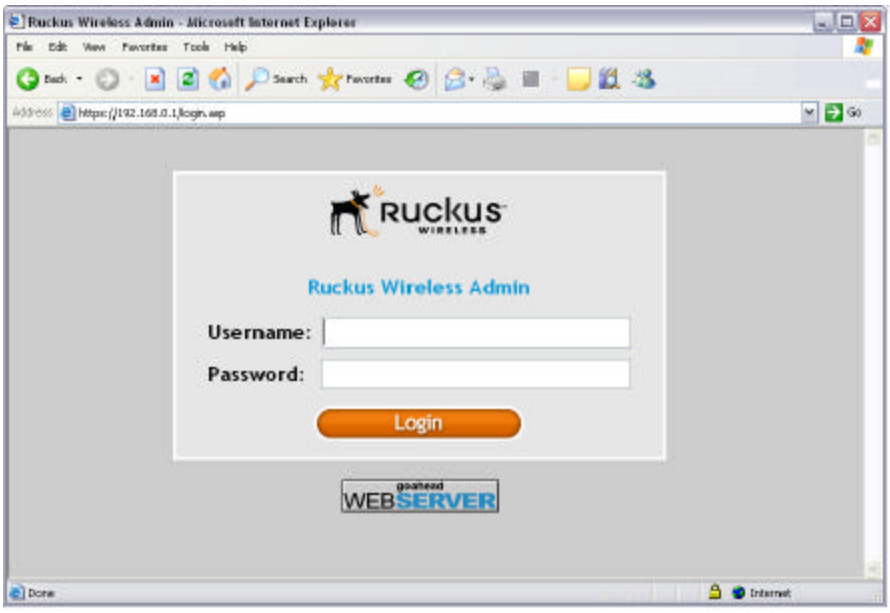
1 On the PC, open a web browser window.

2 Type the IP address of the AP in the browser window, then press Enter to initiate the connection.

- Be sure to enter it in this format: **https://<ip_address>**

3 If a Windows security alert dialog box appears, click **OK/Yes** to proceed.

The Ruckus Wireless Admin login page appears.



4 If you represent a “hotspot operator”, enter the following:

Username super

Password sp-admin

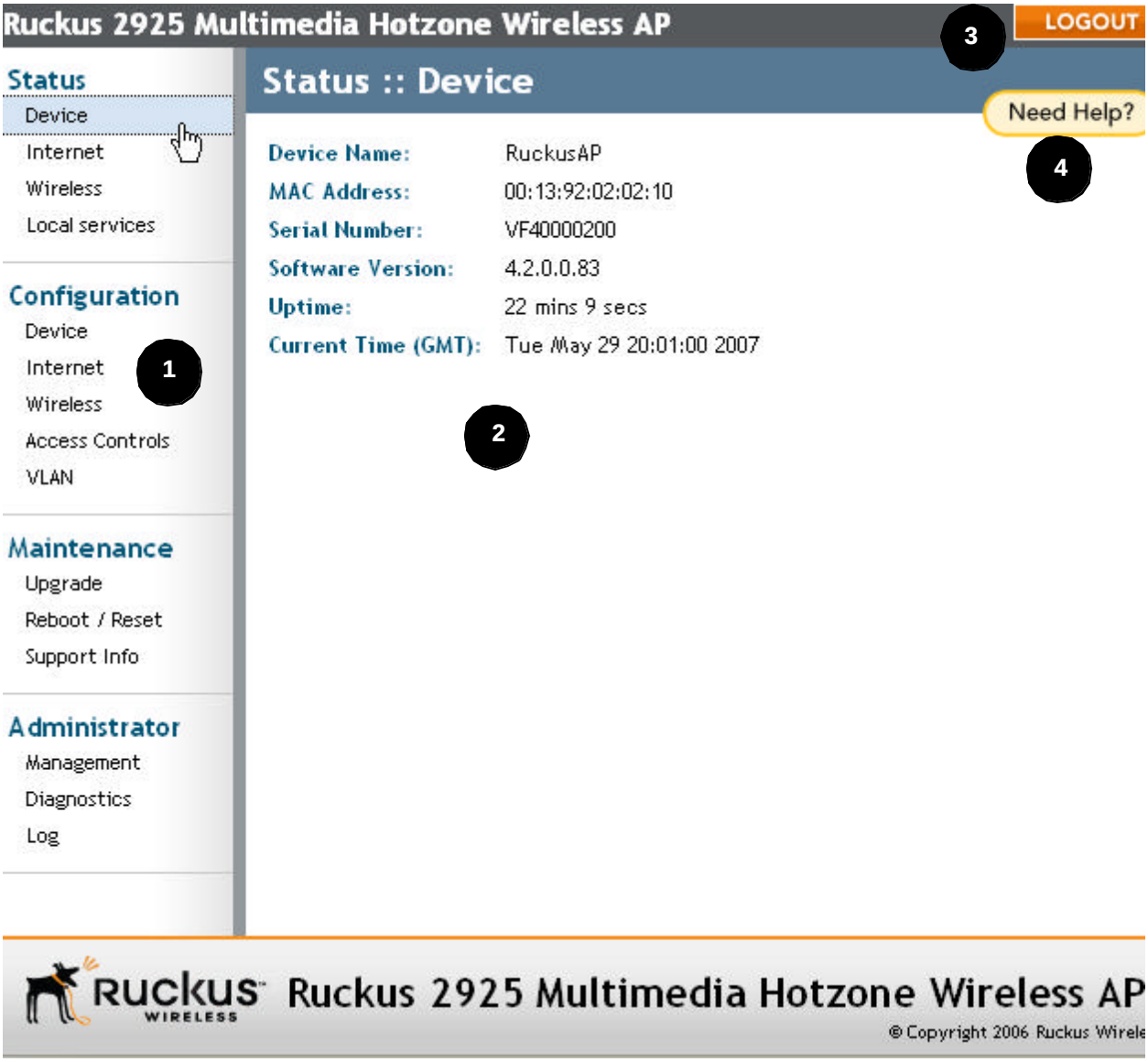
ALERT	The login information will change, once you complete the process detailed in *“Changing the Administrator Login Settings”* on page20

5 Click **Login**.

The Web User interface appears.

Key features of the Web User interface

The Wireless Web User interface has been organized into the following collections of features.



Menu bar [1] Under each category (*Status*, *Configuration*, etc.) are options that, when clicked, open related workspaces in the area to the right.

Workspace [2] This large area displays features, options and indicators relevant to your menu bar choices.

Logout [3] Click this button to log out of the AP.

Need help? [4] Click this button to open a help window with information related specifically to the options currently displayed in the workspace.

Changing the Administrator Login Settings

To replace the current Hotspot Operator login settings, follow these steps:

1 After logging in to the Web User interface, click **Device** under Configuration.

The Configure::Device workspace appears.

2 Review the options. If, you log in as an Operator or Service Provider user, you'll see two sets—*Home* and *Service Provider* login fields.

- The Service Provider user login settings (which you use as "Operator") initially have "super" as the username, and "sp-admin" as the password.
- You can safely ignore the Home settings.

3 Change the Service Provider user name and password (either or both) in the appropriate text fields.

- User names and Passwords must be between 6 and 32 characters in length, and be comprised of letters and numbers only.
- Both user name and password entries are case-sensitive.
- Do not use word spaces.

4 Be sure to write down the new user name or password if you make changes.

5 When you're finished, click **Update Settings**.

A confirmation message appears at the top of the workspace.

Activating other Administrator Access Options

ALERT Do not undertake the customizing of these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

In addition to using the Web User interface to connect to the AP for management and monitoring purposes, you can also take advantage of these network access options:

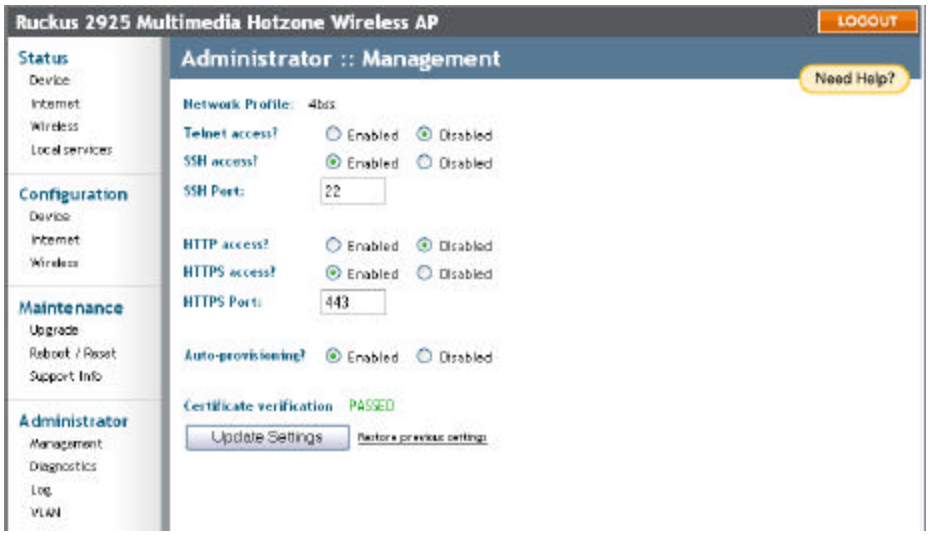
- Telnet access
- Secure shell (SSH) access

This section shows you how to configure Telnet or SSH access, as well as how to direct your web browser to the AP through an HTTP or HTTPS connection.

To take advantage of these options, follow these steps.

1 After logging into the Web User interface, click **Management** under Administrator.

The Administrator::Management workspace appears.



2 Review the options and make changes as needed

Telnet access	By default, this option is disabled (inactive).
Telnet port	This field lists the default Telnet port of 23—only if Telnet is active. You can manually change this port number if required.
SSH access	By default, this option is enabled (active).
SSH port	This field lists the default SSH port of 22—only if SSH is active. You can manually change this port number if required.
HTTP access	This option is disabled by default.

HTTP port	This field lists the default HTTP port of 80, if HTTP has been activated. You can manually change this port number if required.
HTTPS access	By default this option is enabled. This connection mode requires a security certificate, a copy of which has been preinstalled in the device.
HTTPS port	This field lists the default HTTPS port of 443—only if HTTPS has been activated. You can manually change this port number if required.
Certification Verification	This notes whether the security certificate linked to the HTTPS settings has been passed or not.

3 Click **Update Settings** to save your changes.

A confirmation message appears at the top of the workspace.

Changing the IP Address

ALERT Perform this task only in consultation with your Internet Service Provider.

There are at least two instances when you would change the IP address of the AP:

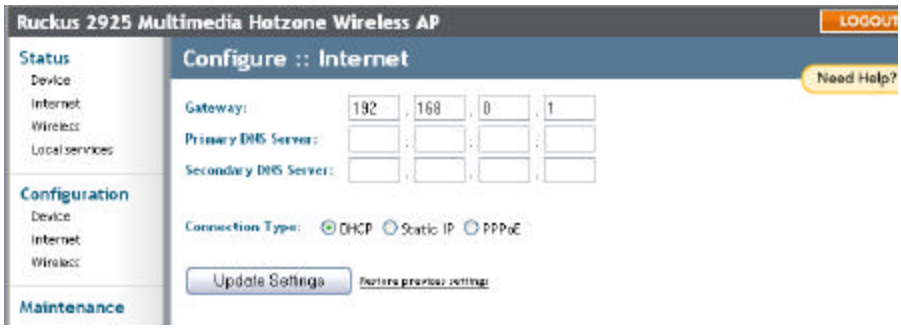
- If the current AP IP address consistently conflicts with that of any other device in your network
- If you want to switch to a static IP address from DHCP, for use in managing or maintaining the AP

Unless you are able to determine the IP address assigned by the DHCP server to the AP, it may prove helpful for anyone needing administrative access to assign a static IP address to the AP.

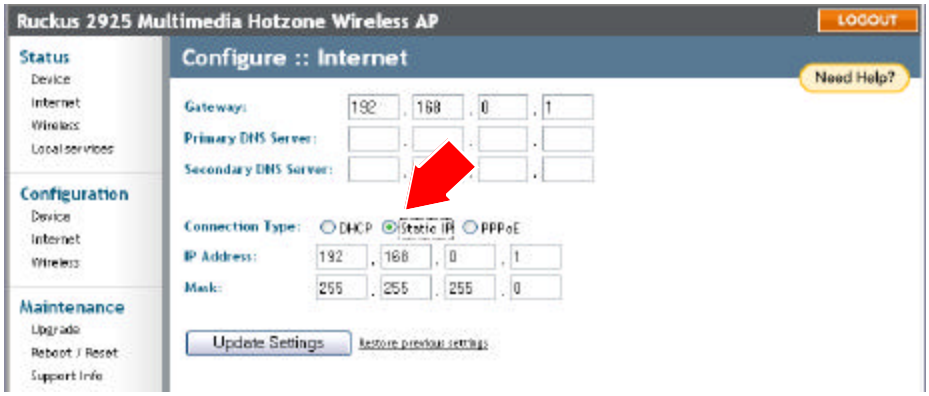
To review and modify the network configuration, follow these steps:

1 After logging into the Web User interface, click **Internet** under Configuration.

The Configure::Internet options appear.



2 Verify that the **Connection Type** is "Static IP".



3 When the Static IP options appear, you can make the following changes:

Gateway	This is the gateway IP address of the Internet interface.
Primary DNS Server	This is the primary Domain Name System (DNS) server IP address.
Secondary DNS Server	This is the secondary Domain Name System (DNS) server IP address.

4 Click **Update Settings** to save and apply the changes.

Changing the Connection Type

ALERT

Perform this task only with guidance from your ISP. The required entries for static IP or PPPoE should be available, if your AP connection type is changed to either of those types.

To change the connection type (DHCP, PPPoE or Static IP), follow these steps:

1 After logging into the Web User interface, click **Internet** under Configuration.

2 When the Configure::Internet options appear (as shown previously), click the button by the **Connection Type** to be applied to this AP.

Typically, connection options relate to your ISP's delivery method:

- in certain uncommon instances, a static IP address is provided
- for cable modem access, **DHCP** is used
- For DSL access, **PPPoE** is used

3 If you need to change to PPPoE or Static IP (from DHCP), fill in the related fields according to your ISP-provided information.

4 Click **Update Settings** to save and apply the changes.

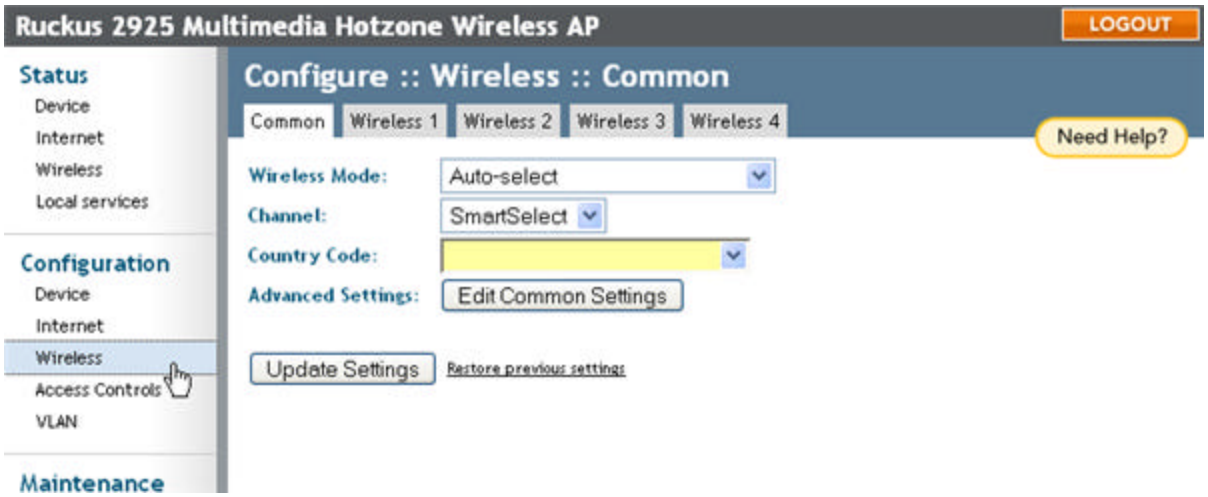
Customizing Common Wireless Configuration

ALERT Do not undertake the customizing of these options unless you are an experienced network administrator or are under the guidance of your ISP or an IT/support professional.

To configure the wireless settings common to all hotspots, follow these three steps:

1 Open the Web User interface, and click **Wireless** under Configuration.

The Configure::Wireless::Common workspace appears.



2 Make changes to the following options (if necessary):

Wireless mode The wireless mode options include the following:

Auto-Select:	Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting.
2.4GHz 54 Mbps	(For faster 802.11g devices only): Allows only 802.11g-compliant devices to join the network.
2.4GHz 11Mbps	(For slower 802.11b devices only): Allows only 802.11b-compliant devices to join the network.

Channel This menu lets you select the channel used by the network. You can choose **SmartSelect**, or choose one of a specific number of channels. If you choose SmartSelect, the AP selects the best channel (encountering the least interference) to transmit the signal.

Country Code This menu, if active, lets you pick your country or region code.

Advanced Settings See *"Reviewing the Advanced::Common Options"* on page25.

WARNING—Selecting the incorrect country or region may result in violation of applicable law.

ALERT If your AP was shipped in the United States, the country code was pre-defined for "United States" and cannot be modified.

3 [-Optional-] Click **Update Settings** before reviewing the "common" advanced options.

Reviewing the Advanced::Common Options

This workspace permits access to advanced wireless functions. These settings should only be changed by an experienced administrator. Incorrect settings can severely impact wireless performance. It is recommended that the default settings be retained for best performance.

1 In the Configure::Wireless::Common workspace, click **Edit Common Settings**.

The Configure::Wireless::Advanced::Common workspace appears.

2 Make the following entries, as needed:

Data Rate (The default value is **Best**.) Select the preferred rate of data transmission from the drop-down menu. Selecting Best allows the AP to adapt data transmission to the best rate available. The efficacy of rates listed in the Data Rate drop-down menu is dependent on the Wireless Mode previously specified.

WARNING—In order to fully benefit from the Ruckus AP's capabilities, it is advisable not to change this value unless absolutely necessary.

Transmit Power (The default is **Full**.) Select the level of transmit power from the drop-down menu. This option sets the maximum transmit power level relative to the pre-defined power (this value differs according to the current country code).

Beacon Interval (The default value is **100**.) A beacon is a broadcast packet regularly sent out by the AP to continually synchronize wireless network communication. The Beacon Interval value determine the frequency, measured in milliseconds.

Protection Mode (**Inactive** by default.) If you activate protection, you control how 802.11 devices know when they should communicate to another device. This is important in a mixed environment of both 802.11b and 802.11g clients. WARNING: Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g devices *but will severely decrease performance*.

CTS-only Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated.

RTS/CTS Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.

For information on "Protection Mode"-specific Threshold options and how they can be customized on an individual hotspot basis, see the following section, *"Setting Threshold Options"*.

3 Click **Update Settings** to save and apply the changes.

Setting Threshold Options

ALERT

Do not undertake the customizing of these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

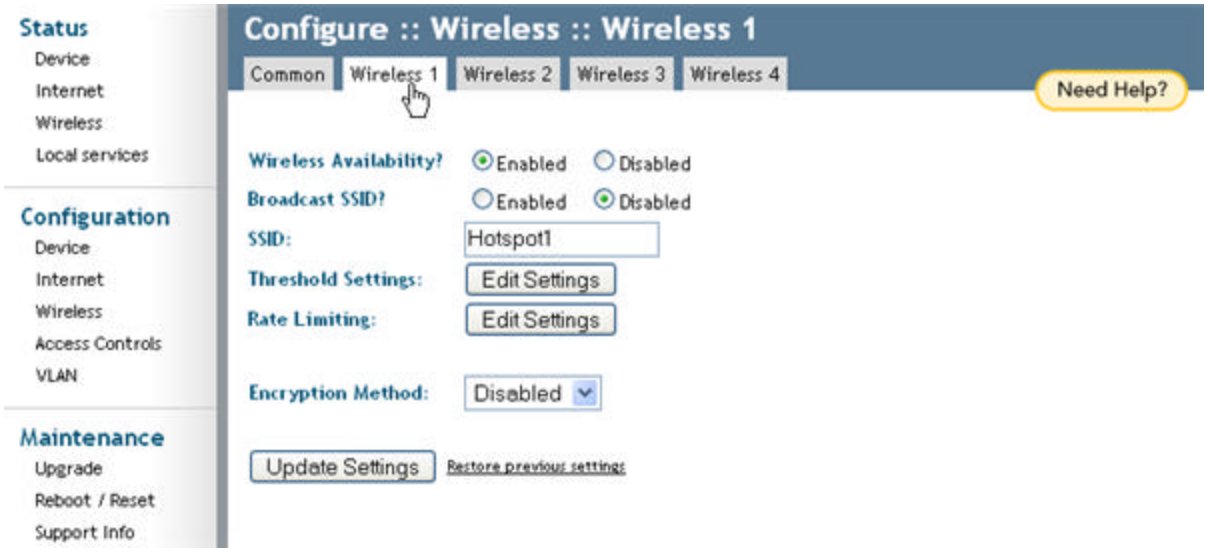
The following options allow you to fine-tune the "Protection Mode" behavior, set previously in the Wireless::Common workspace. After activating a Protection Mode, you can open each Wireless tab and customize the threshold settings, that determine what is put in effect and when.

To customize Protection Mode (Threshold) settings, follow these steps:

1 Open the Web User interface, and click **Wireless** under Configuration.

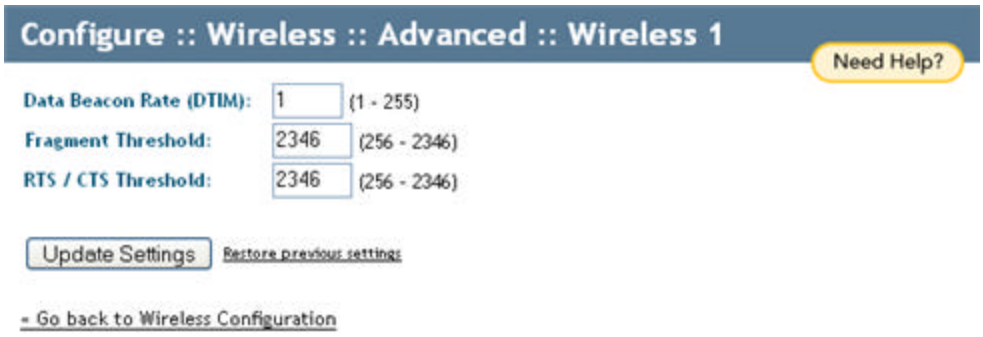
2 When the Configure::Wireless::Common workspace appears, click a hotspot-specific tab.

The Configure::Wireless::Wireless [#] workspace appears.



3 Look for Threshold Settings and click **Edit Settings**.

The Configure::Wireless::Advanced::Wireless [#] workspace appears.



4 Review the following options and make any needed changes:

Data Beacon Rate (The default value is **10**.) The value indicates the interval of the Delivery Traffic Indication Message (DTIM). This is a countdown field that the device uses to inform its clients of the next window for listening to broadcast or multicast messages.

Fragment Threshold (The default value is **2346**.) This option sets the maximum length of a packet before data is fragmented into multiple packets. In a good wireless environment, the larger the fragment, the more efficient the network operates. In a noisy environment, the threshold should be adjusted to a smaller size to minimize retransmission and increase the reliability of the transmission.

RTS/CTS Threshold (The default value is **2346**.) This option determines at what packet length the RTS/CTS function is triggered. A lower threshold may be necessary in environment with excessive signal noise or hidden nodes; but may result in some performance degradation.

5 Click **Update Settings** to save and apply the changes.

A confirmation message appears at the top of this workspace.

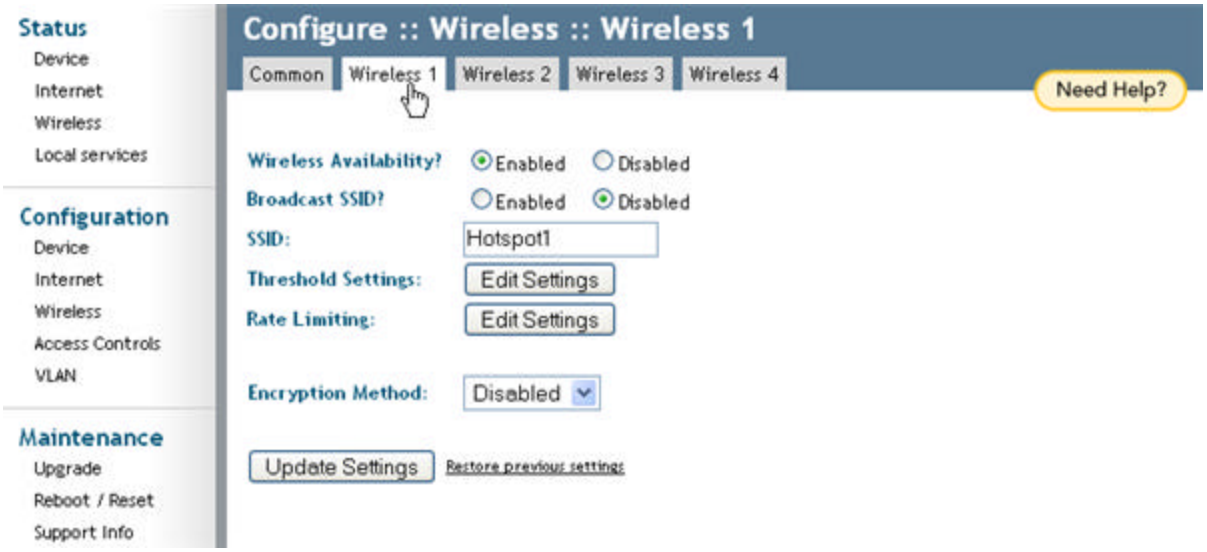
6 Click **Go back to Wireless Configuration** to reopen the previous workspace.

Customizing Wireless Hotspot Settings

1 After opening the Web User interface, click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click one of the four **Wireless (#)** tabs.

The Configure::Wireless::Wireless (#) workspace appears.



3 Make the following entries:

Wireless Availability This option controls whether or not the wireless network is available to users (Off or On).

Broadcast SSID This option controls whether or not the hotspot SSID is visible to anyone looking for wireless networks. Disabling (hiding) the SSID requires the user must be told the correct SSID before they can connect to your network.

SSID This is the publicly-broadcast "name" of your wireless network. A default SSID is present (which you ideally replaced in the installation process). If the default SSID is still active, it is strongly recommended that you change it. An effective SSID somehow indicates your location or group name. The "name" can be up to 32 characters in length, containing letters and numbers, and is case-sensitive.

Threshold Settings This button opens a workspace where you can configure the Protection Mode you activated in the Wireless::Common workspace. If Protection Mode is not active, ignore this option.

For more information, see *"Setting Threshold Options"* on page26.

Encryption Method By default, all data exchanges in your wireless network are not encrypted, but you can pick an encryption method in this option, and use the extra workspace features that appear to fine-tune the encryption.

For more information, see either *"Customizing Wireless WEP Encryption"* on page29 or *"Customizing Wireless WPA Encryption"* on page 30.

4 When you are finished, click **Update Settings** to save and apply the changes.

A confirmation message appears at the top of this workspace.

5 Click **Go back to Wireless Configuration** to reopen the previous workspace.

Customizing Wireless WEP Encryption

ALERT Do not undertake the customizing of these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

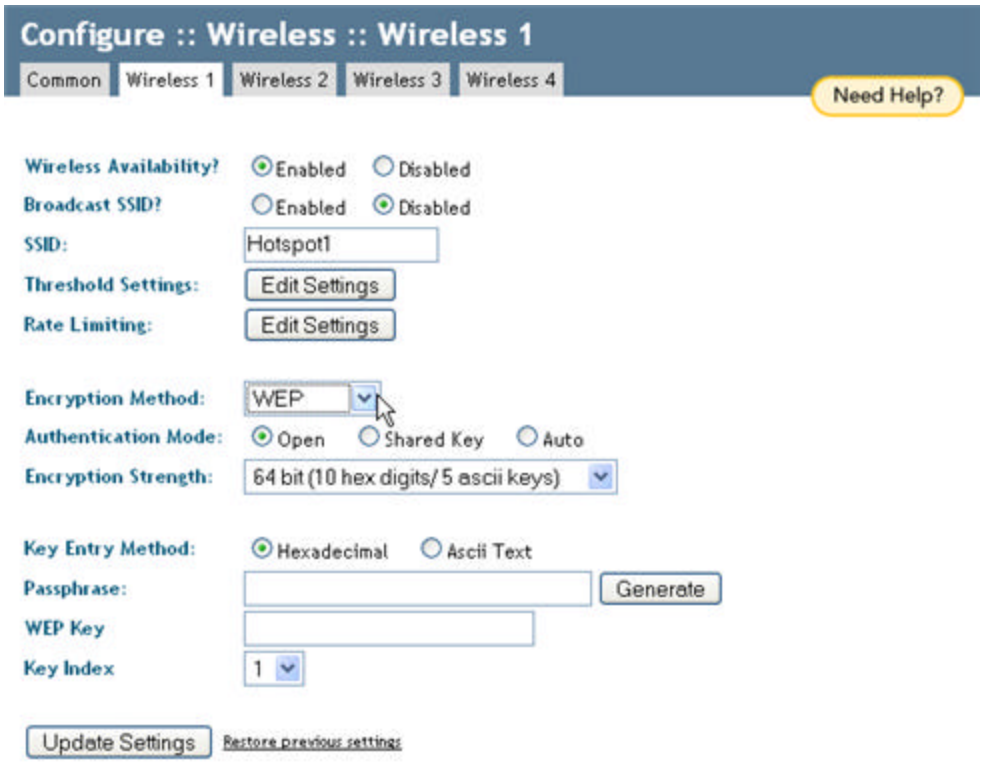
To configure hotspot-specific WEP encryption settings, follow these steps:

1 Open the Web User interface, and click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click a hotspot-specific tab.

3 When the Configure::Wireless::Wireless [#] workspace appears, open the **Encryption Method** menu and choose **WEP**.

An additional set of WEP-specific encryption options appear in this workspace.



4 You can make the following changes:

Authentication Mode Your options include —

Open: No security measure is enforced.

Shared Key: The selected Default Shared Key is used.

Auto: Automatically-selected authentication mode.

Encryption Strength	64 bit: Specify the key with 10 hexadecimal digits or 5 ASCII characters. 128 bit: Specify the key with 26 hexadecimal digits or 13 ASCII characters. The 128-bit cryptography is stronger privacy protection for your network and is recommended if you use WEP.
Key Entry Method	Hexadecimal: The encryption key only accepts hexadecimal characters (0-9, A-F). ASCII Text: The encryption key accepts ASCII characters.
Passphrase	This assists in automatic key generation. Enter some text and click the Generate button. The system will generate the WEP key automatically. You may specify a passphrase up to 32 characters. Please note that the algorithm used for key generation may vary from system to system. Checking the WEP keys used between wireless stations and the AP is recommended.
WEP Key	Enter the key manually according to the Key Entry Method and Encryption Strength settings.
Key Index	Choose the index, from "1" to "4", that the WEP key is to be stored in.

5 Click **Update Settings** to save and apply the changes.

A confirmation message appears at the top of this workspace.

6 Click **Go back to Wireless Configuration** to reopen the previous workspace.

Customizing Wireless WPA Encryption

ALERT Do not undertake the customizing of these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

Use of WPA PSK allows automatic key generation based on a single passphrase. WPA-PSK provides very strong security, but may not be supported on older wireless devices. In some cases, the older devices can be upgraded with adapters to take advantage of WPA-PSK.

If you configure the hotspot AP with WPA-PSK, some network users will not be able to connect to your hotspot WLAN unless their devices are manually set to WPA-PSK and configured with the same passphrase.

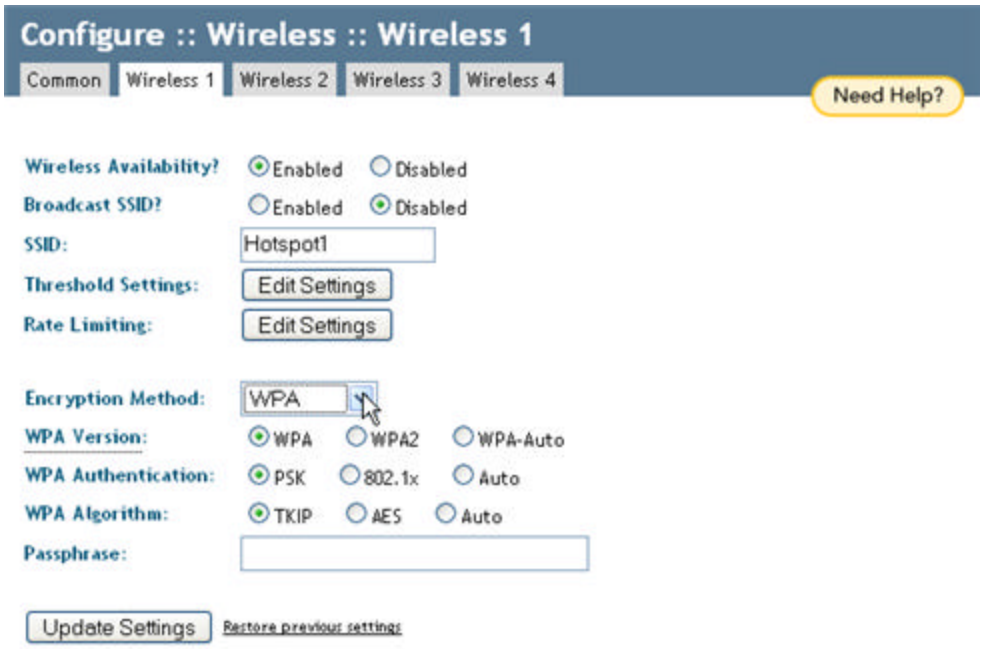
To configure hotspot-specific WPA encryption settings, follow these steps:

1 Open the Web User interface, and click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click a hotspot-specific tab.

3 When the Configure::Wireless::Wireless[#] workspace appears, open the **Encryption Method** menu and choose **WPA**.

An additional set of WPA-specific encryption options appear in this workspace.



4 You can make the following changes:

WPA Version Your options are WPA, WPA2 or WPA Auto.

When WPA-Auto is selected, the wireless client decides the version of WPA will be used. WPA is the recommended default for best compatibility. Wi-Fi WPA-capable PDAs and other gadgets are usually limited to WPA + TKIP.

WPA2 is an advanced option. WPA2 support on Windows requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later.

WPA-Auto is an advanced option. Only the best WPA 802.11i-conforming/Wi-Fi WPA-certified client devices can operate in this mode.

WPA Authentication PSK mode is suitable for home or personal use. 802.1x mode uses a networked RADIUS server to verify user identity. The auto mode offers both options for the wireless client to pick.

WPA Algorithm When Auto is selected, the wireless client decides whether TKIP or AES will be used. AES is the strongest encryption and requires additional hardware support on wireless devices.You should consult the documentation of your wireless client devices. Auto is an advanced option and some wireless clients may fail to associate.

Passphrase Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters (letters, numbers, hyphens and underscores).

5 Click **Update Settings** to save and apply the changes.

A confirmation message appears at the top of this workspace.

6 Click **Go back to Wireless Configuration** to reopen the previous workspace.

Customizing 802.1x (Settings)

ALERT Do not undertake the customizing of these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

If you choose "WPA" as the encryption method, you have the option to set up the AP to act as an 802.1x proxy, utilizing external authentication sources such as a RADIUS server. This provides a higher level of security, when compared to the static security process in a WEP configuration.)

Using 802.1x lets a device complete authentication prior to the exchange of data, as in a DHCP environment. Another benefit: each BSSID can be individually configured to forward all authentication requests to its own server.

To configure hotspot-specific 802.1x authentication settings, follow these steps:

1 Open the Web User interface, and click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click a hotspot-specific tab.

3 When the Configure::Wireless::Wireless[#] workspace appears, open the **Encryption Method** menu and choose **WPA**.

The basic set of WPA-specific encryption options appear in this workspace.

4 Select **802.1x** as the WPA Authentication mode.

5 Additional options appear, that you can use to customize your 802.1x authentication.

RADIUS NAS-ID Enter the network ID assigned to your RADIUS server.

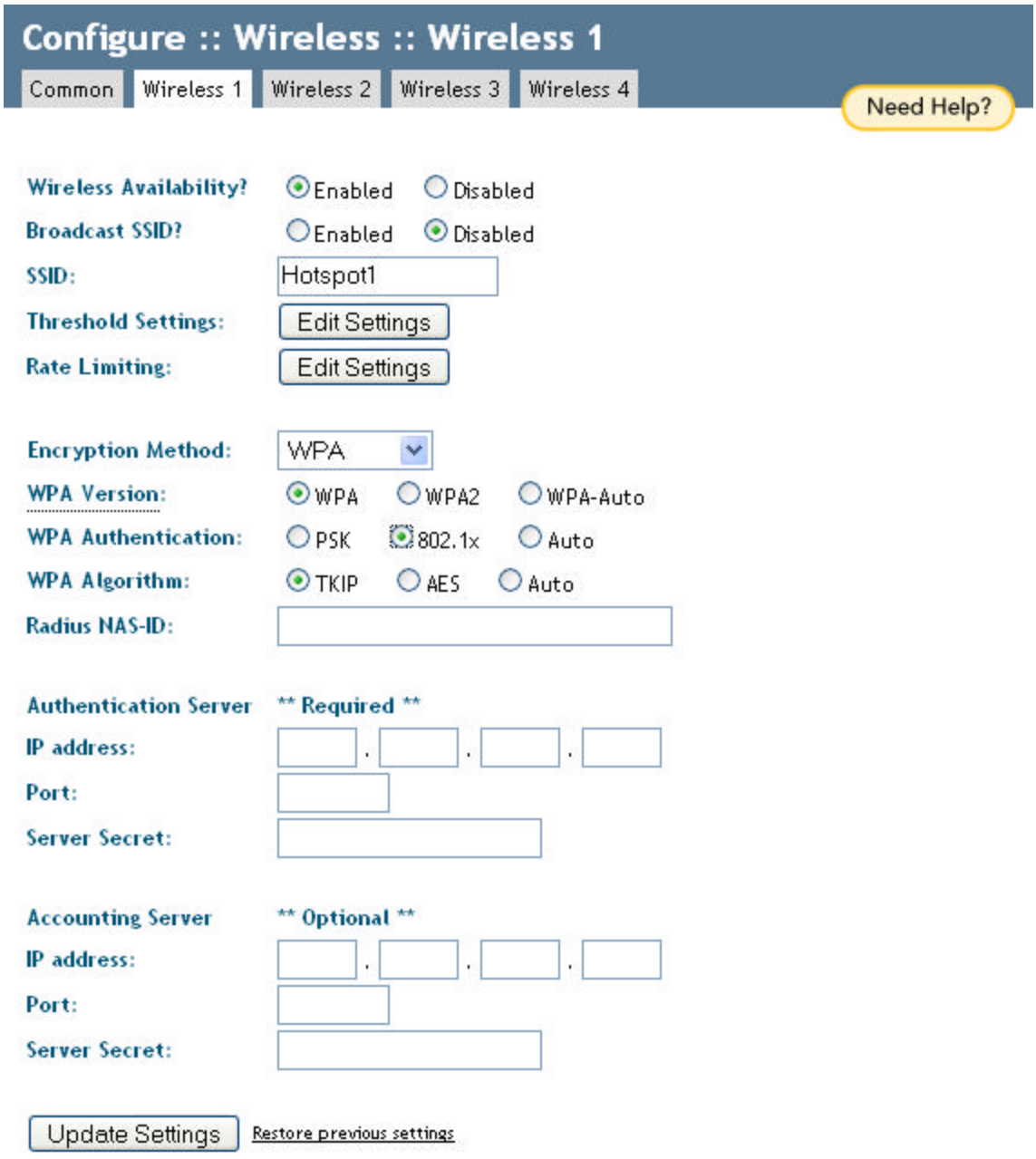
Authentication Server [-Required-] Enter the information needed to establish a connection between the AP and the RADIUS server.

Accounting Server [-Optional-] Enter the information needed to establish this connection.

6 Click **Update Settings** to save and apply the changes.

A confirmation message appears at the top of this workspace.

7 Click **Go back to Wireless Configuration** to reopen the previous workspace.


Configure :: Wireless :: Wireless 1
Common
Wireless 1
Wireless 2
Wireless 3
Wireless 4
Need Help?
Wireless Availability?
Enabled
Disabled
Broadcast SSID?
Enabled
Disabled
SSID:
Hotspot1
Threshold Settings:
Edit Settings
Rate Limiting:
Edit Settings
Encryption Method:
WPA
WPA Version:
WPA
WPA2
WPA-Auto
WPA Authentication:
PSK
802.1x
Auto
WPA Algorithm:
TKIP
AES
Auto
Radius NAS-ID:
Authentication Server
** Required **
IP address:
Port:
Server Secret:
Accounting Server
** Optional **
IP address:
Port:
Server Secret:
Update Settings
Restore previous settings

Reviewing Current VLAN IDs

ALERT	Do not make any changes to these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

1 After logging into the Web User interface, click **VLAN** under Configuration.

The Configuration::VLAN workspace appears.

2 Review the current IDs.

3 Make any changes, if needed.

4 Click **Update Settings (test)**.

For more on VLAN configuration, see *"VLANs"* on page46.

CHAPTER 4

Managing the Access Point

This chapter covers the tasks you might consider in the course of regular maintenance of a Ruckus Wireless AP (and its network services). These range from renaming the AP to fine-tuning wireless configurations, to upgrading the internal firmware of an AP.

Be sure to browse the topical subheads in the first section, *"Maintaining your HotSpot AP"*.

You will also learn how to restore the AP to a "factory default" state, but this should be done only if the AP is inoperable, and Ruckus support staff have recommended this action. Doing this will force you to restart the entire AP "installation", as detailed in the Quick Setup Guide and in this chapter—*"Installation, Setup, and Placement of the AP"* on page4

Chapter Contents

Maintaining your HotSpot AP

This section highlights a collection of individual, context-free tasks culled from the Web User interface (and detailed here for your convenience).

Maintenance topics covered in this section

Changing the Device Name

1 After opening the Web User interface, click **Device** under Configuration.

2 Make any changes in the **Device Name** field in the Configure::Device workspace.

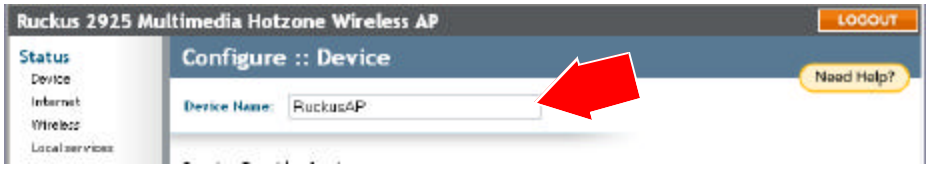


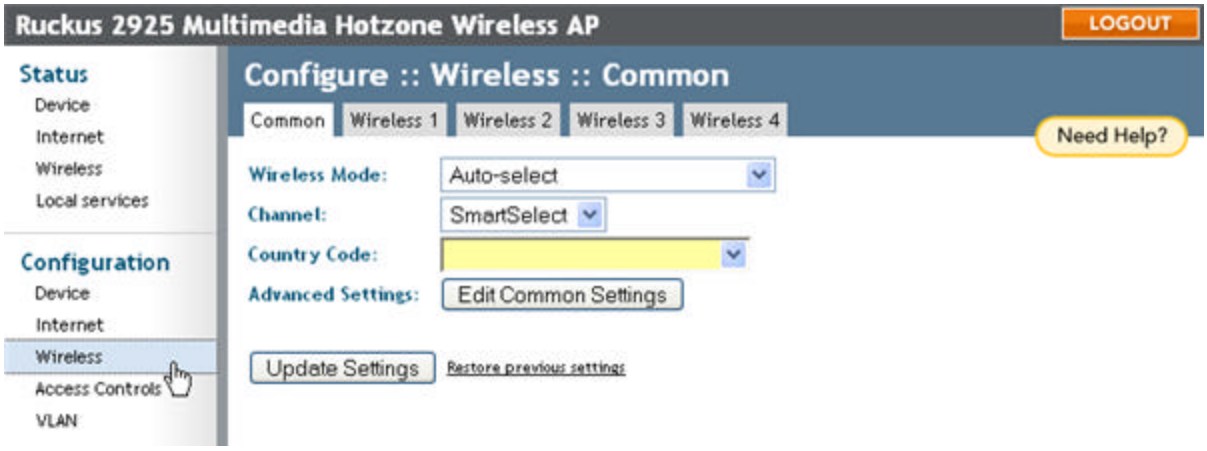
FIGURE 4-1:

3 Click **Update Settings** to save and apply the changes.

Changing the Wireless Mode

1 After opening the Web User interface, click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, review the choices.



3 Select any of the following modes from **Wireless Mode**:

Auto-Select: Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting.

2.4GHz 54 Mbps (For faster 802.11g devices only): Allows only 802.11g-compliant devices to join the network.

2.4GHz 11Mbps (For slower 802.11b devices only): Allows only 802.11b-compliant devices to join the network.

4 For information about the remaining common wireless configuration options, see *"Customizing Common Wireless Configuration"* on page24.

5 Click **Update Settings** to save and apply the changes.

Changing the Wireless Channel

1 After opening the Web User interface, click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, review the options.

3 Open the **Channel** menu and select the channel used by the network.

- You can choose **SmartSelect**, or choose one of a specific number of channels. If you choose SmartSelect, the AP selects the best channel (encountering the least interference) to transmit the signal.

4 Click **Update Settings** to save and apply the changes.

Changing the Wireless Data Rate

1 After opening the Web User interface, click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click **Edit Common Settings**.

3 When the Configure::Wireless::Advanced::Common workspace appears, review the options.

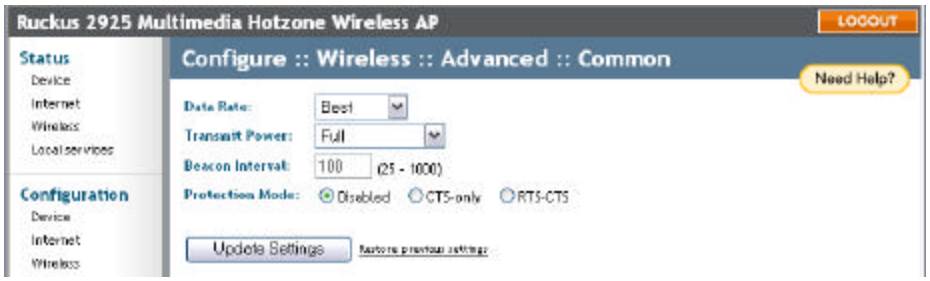


FIGURE 4-2:

4 Open the **Data Rate** menu and make a selection. (The default value is **Best**.)

5 Select the preferred rate of data transmission from the drop-down menu.

- Selecting **Best** allows the AP to adapt data transmission to the best rate available.
- Note: the efficacy of rates listed in the Data Rate drop-down menu is dependent on the Wireless Mode previously specified.

6 Click **Update Settings** to save and apply the changes.

Changing the Transmit Power Setting

1 After opening the Web User interface, click **Wireless** under Configuration.

2 When the Configuration::Wireless::Common workspace appears, click **Edit Common Settings**.

3 When the Configure::Wireless::Advanced::Common workspace appears, review the available options.

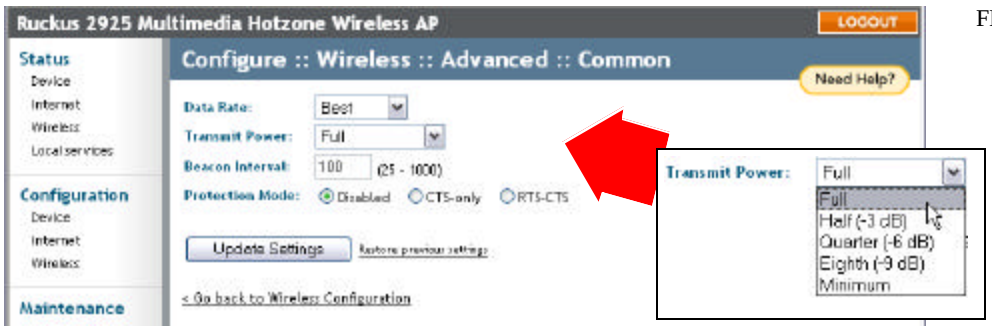


FIGURE 4-3:

4 Open the **Transmit Power** menu and make a selection. (The default is **Full**.)

5 Select the level of transmit power from the drop-down menu. This option sets the maximum transmit power level relative to the calibrated power.

6 Click **Update Settings** to save and apply the changes.

Changing the Beacon Interval

1 After opening the Web User interface, click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click **Edit Common Settings**.

3 When the Configure::Wireless::Advanced::Common workspace appears, review the options.

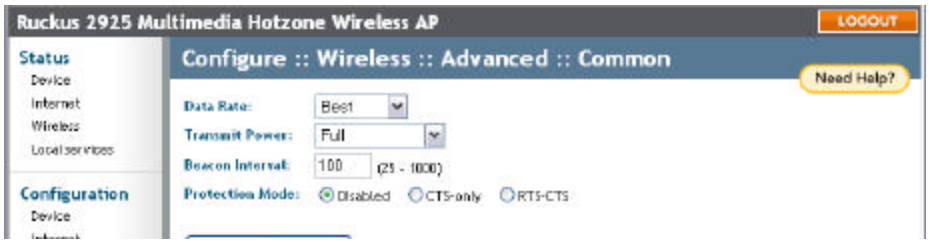


FIGURE 4-4:

4 Delete the text (if you choose) in the **Beacon Interval** field and type the preferred number.(The default value is **100**.)

- A beacon is a broadcast packet regularly sent out by the AP to continually synchronize wireless network communication. The Beacon Interval value determine the frequency, measured in milliseconds.

5 Click **Update Settings** to save and apply the changes.

Changing the Protection Mode

1 After opening the Web User interface, click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click **Edit Common Settings**.

3 When the Configure::Wireless::Advanced::Common workspace appears, review the options.

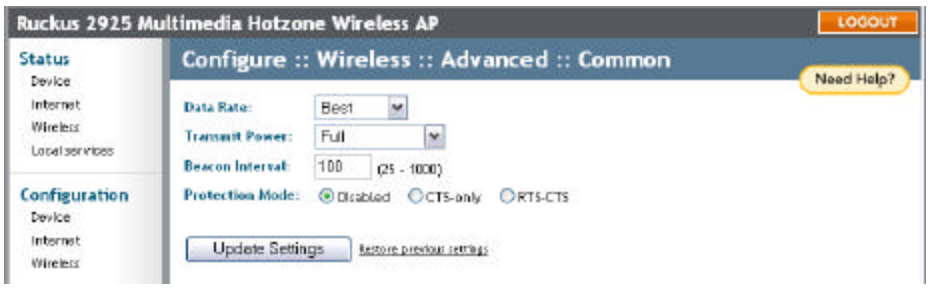


FIGURE 4-5:

4 Click the radio button by your preferred **Protection Mode**—if any. (**Disabled** by default.)

If you activate protection, you control how 802.11 devices know when they should communicate to another device. This is important in a mixed environment of both 802.11b and 802.11g clients. Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g devices but will severely decrease performance.

CTS-only Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated.

RTS/CTS Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.

For information on "Protection Mode"-specific Threshold options and how they can be customized on an individual hotspot basis, see *"Setting Threshold Options"* on page 26.

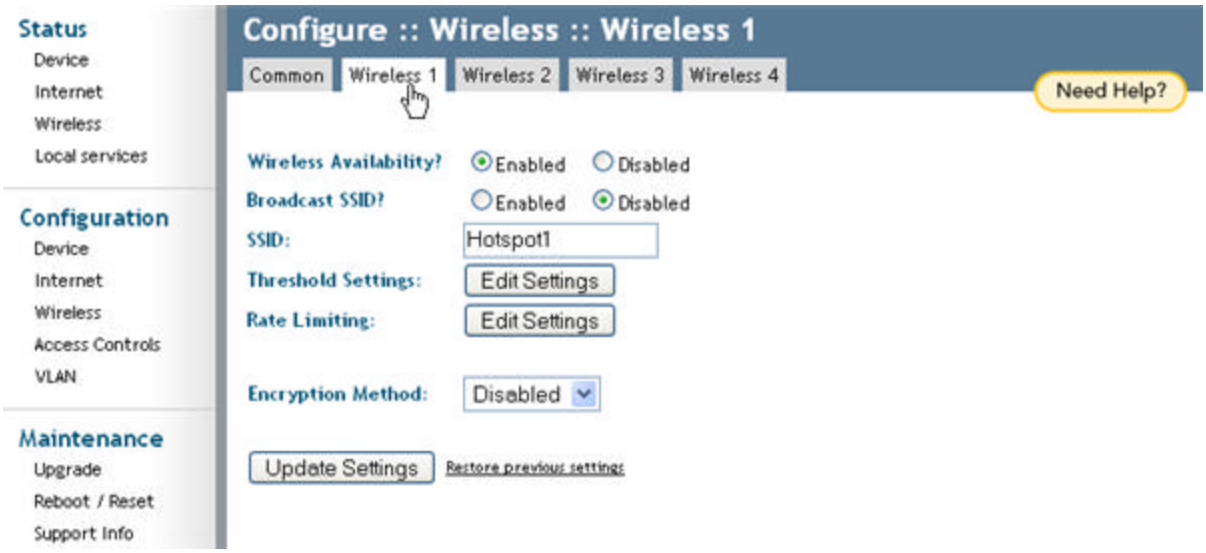
5 Click **Update Settings** to save and apply the changes.

Changing the Wireless Availability Setting

This controls whether or not a hotspot is active. To deactivate a hotspot, use this feature.

1 Open the Web User interface, and click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click the relevant hotspot-specific tab.



3 When the Configure::Wireless::Wireless [#] workspace appears, click one of two **Wireless Availability** options for this hotspot.

4 Repeat the previous step with the remaining hotspot tabs, as needed.

5 Click **Update Settings** to save and apply the changes.

Changing the Broadcast SSID setting

This controls whether or not a hotspot sends out an SSID to any nearby wireless devices. If you deactivate it, you control access to a hotspot to those people who "know the hotspot name".

1 Open the Web User interface, and click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click a hotspot-specific tab.

3 When the Configure::Wireless::Wireless [#] workspace appears, click one of two **Broadcast SSID** options for this hotspot.

4 Repeat the previous step with the remaining hotspot tabs.

5 Click **Update Settings** to save and apply the changes.

Changing a Hotspot-specific SSID

This affects how a specific wi-fi hotspot is "identified" in a user's wireless device.

1 Open the Web User interface, and click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click a hotspot-specific tab.

3 When the Configure::Wireless::Wireless [#] workspace appears, delete the text in the **SSID** field that represents this hotspot.

4 Type a new SSID.

5 Repeat the previous two steps with the remaining hotspot tabs.

6 Click **Update Settings** to save and apply the changes.

Rate Limiting HotSpots

Rate limiting controls fair access to the network. When enabled, the network traffic throughput of each network device is limited to the rate specified in the traffic policy, and that policy can be applied on either the uplink or downlink. Rate limiting is restricted to Super User access only.

Rate limiting topics covered in this section

- *"Enabling rate limiting"* on page 41
- *"Rate Limiting fields and headings"* on page43

Enabling rate limiting

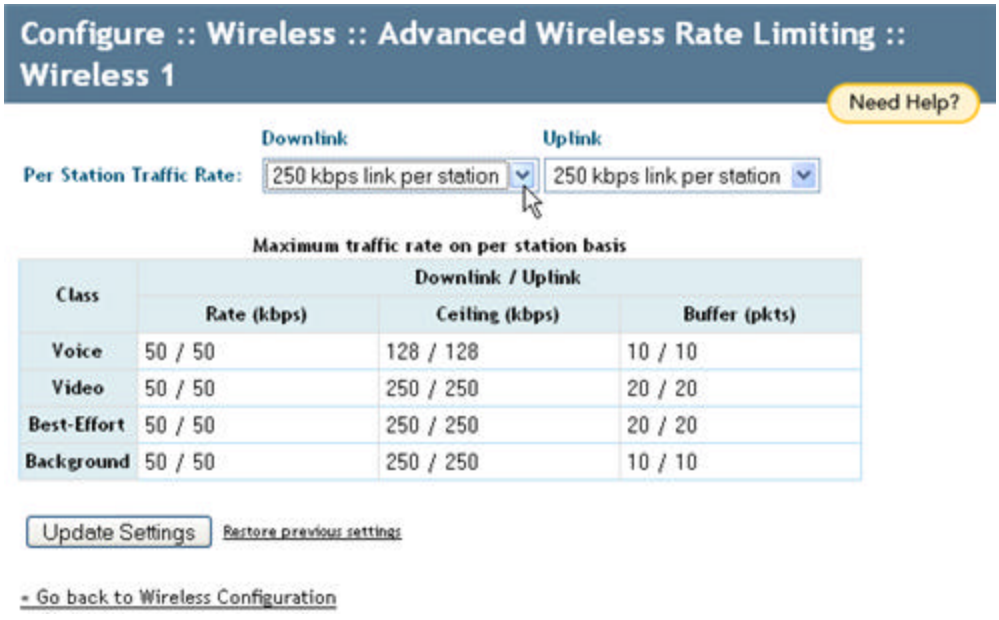
1 Open the Web User interface, and click **Wireless** under Configuration.

2 When the Configure::Wireless::Common workspace appears, click a hotspot-specific tab, such as Wireless 1.

3 When the Configure::Wireless::Wireless [#] workspace appears, click the **Edit Settings** button next to "Rate Limiting".

4 Toggle the **Downlink** drop-down menu and select the downlink rate limit for each station.

5 Toggle the **Uplink** drop-down menu and select the uplink rate limit for each station.



6 Click the **Update Settings** button to save your changes.

Rate Limiting fields and headings

- **Per Station Traffic Rate**: Each station on the WLAN will be limited to this data rate. Depending on conditions such as "air quality" (ability for transmit and receive radio signals by each station), the number of stations with data and how much data they have to send, the actual transmission rate may be less. Traffic policy is applied equally to each connected device.
- **Downlink**: The "downlink policy" applies to traffic going to any station.
- **Uplink**: The "uplink policy" applies to traffic being sent from a wireless station. The downlink policy is also applicable to traffic going to another station on the same WLAN, such as a printer, wi-fi music player, etc.
- **Class**: All network traffic is classified into voice, video, data (best-effort), or background. Classification determines priority.
- **Voice**: Voice requires the highest priority so that conversations can be readily understood.
- **Video**: The second-highest priority class, video data also requires prompt delivery but is less sensitive to delay compared to voice.
- **Best-Effort**: Traffic that is not video, voice or background.
- **Background**: The category for everything else: traffic used by network devices to provide basic network presence, aliveness, and so on. This category is the least sensitive to transit delay variations, and is given the lowest priority.
- **Rate**: This is the nominal data rate. Assuming available bandwidth, traffic may exceed this rate but cannot exceed the ceiling.
- **Ceiling**: This is the absolute limit, subject to lowered actual rates if either the existing "air quality" is low, or traffic from higher-priority classes prevents reaching the "ceiling" value, or some combination of these.
- **Buffer**: This is the number of packets that can be queued waiting for their turn to be sent. This allows limited ability to handle traffic bursts but prevents exceeding the permitted rate, i.e., excessive traffic will be dropped.

Access Controls

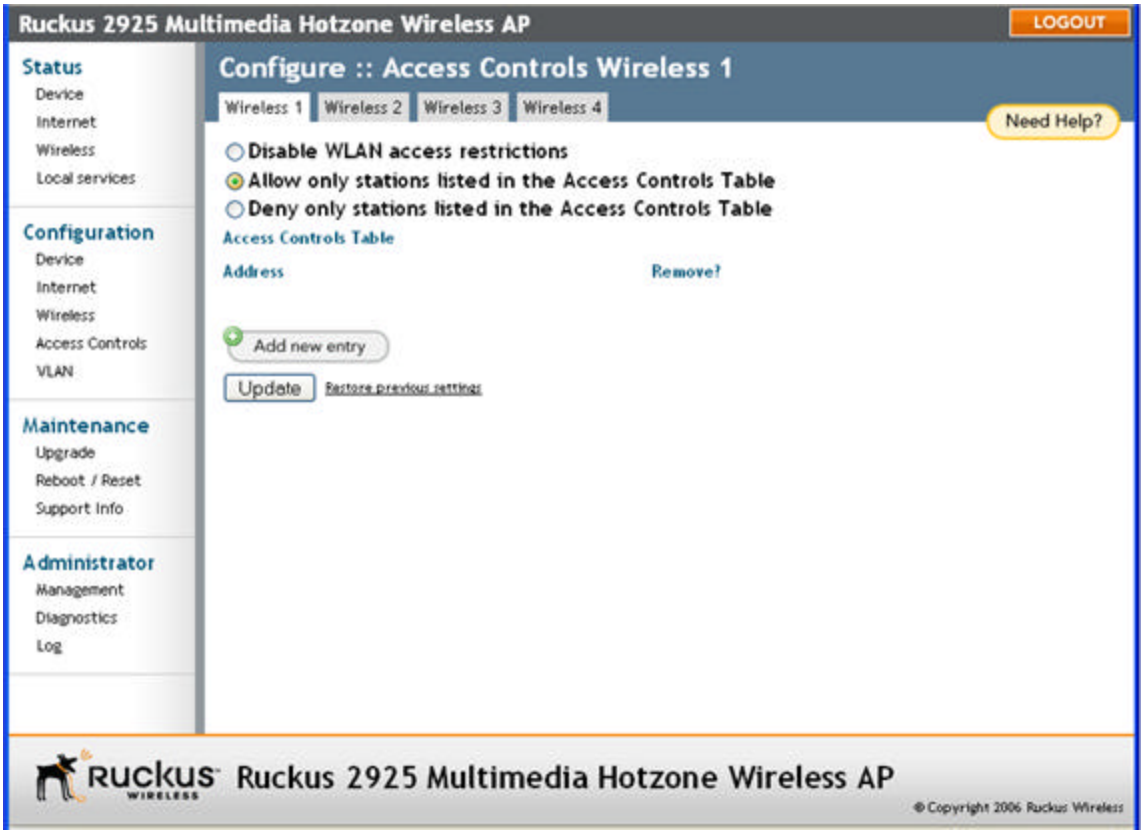
Access Controls give you control over which stations are allowed to join (associate with) your WLAN networks. There are "tab" entries for each available WLAN.

Access control topics covered in this section

Changing the access controls for a WLAN

1. Open the Web User interface, and click **Access Controls** under Configuration.
2. When the Configuration::Access Controls workspace appears, click a hotspot-specific tab; by default, Wireless 1 appears.
3. Click on the tab for the WLAN you want to configure.
4. Select the radio button for the desired access control. (For a description of the options, see *"Access control options"* on page45.) The Access Controls Table appears.
5. Click the **Add new entry** button to add a MAC address to the table.
6. Type the MAC address in the spaces provided.
7. Click the **Update** button to save your changes. Assuming all parameters you entered are acceptable, that row will be added to the table.

8 If you have additional MAC addresses you want included, click **Add new entry** and repeat these steps until you've entered all the stations you want. There is a limit of 128 rows.



Removing MAC addresses from a list

Simply check the box under the Remove column for the MAC address entry(ies) you want to remove from the table and click **Update**.

Access control options

Disabling WLAN access restrictions

If you select "Disable WLAN access restrictions", then MAC-address-based restrictions on which stations can join the WLAN are disabled; thus, any station can join. If the WLAN uses encryption, then the station must still supply the correct encryption pass-phrase.

The Access Controls table is hidden if the current mode is "Disable WLAN access restrictions".

Allowing only stations explicitly listed in the Access Controls Table

If you select "Allow only stations listed in the Access Controls Table", then stations entered into the access-controls table are allowed but all others are disallowed. To add MACaddresses, see *"Changing the access controls for a WLAN"* on page44.

Denying only stations explicitly listed in the Access Controls Table

If you select "Deny only stations listed in the Access Controls Table", then stations entered into the access-controls table are disallowed but all others are allowed. To add MACaddresses, see *"Changing the access controls for a WLAN"* on page44.

Access Control Table columns

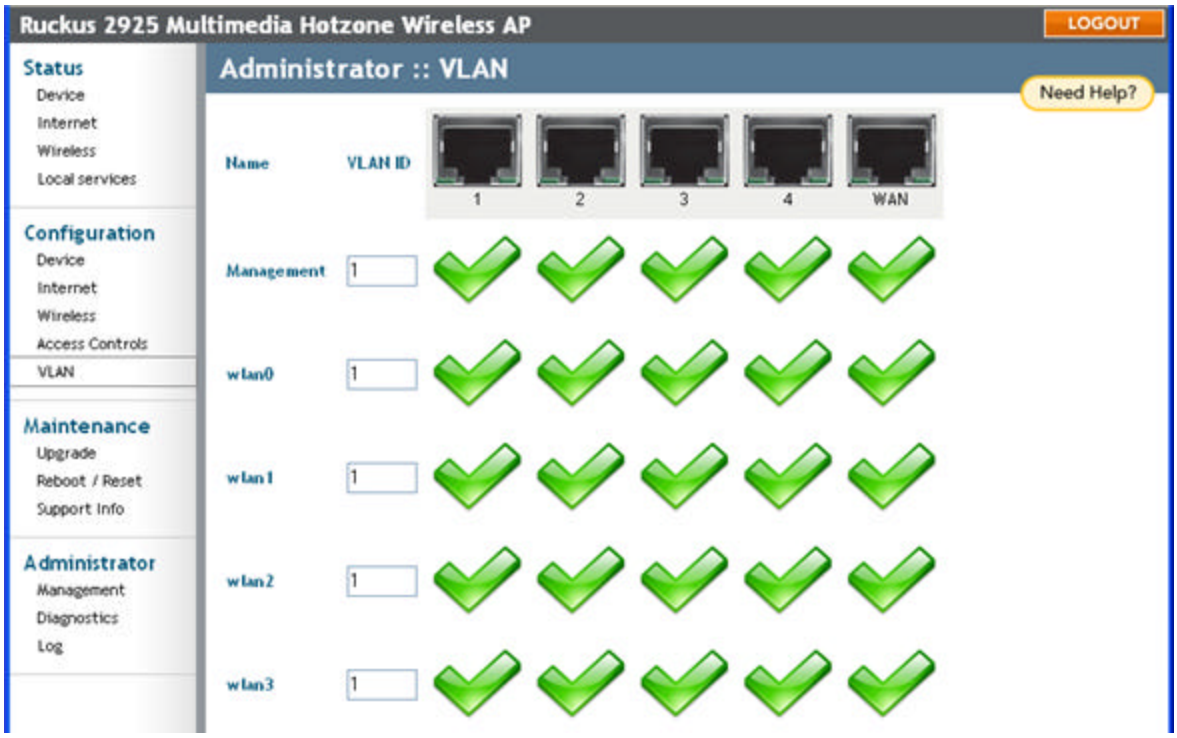
The Access Control Table contains the following columns:

- **Address**: six text boxes appear in which you enter the desired MAC address, in hexadecimal digit form, two characters in each box. You can specify a full 12-hex-digit MAC address or enter "wildcard" characters for "don't care" digits. Allowable hex-digit characters are 0-9, a-f, and A-F. Most address-tags and software where you find MAC addresses listed include colons or dashes to separate the address-pairs; that is provided for you on the web page, so do not enter the colons or dashes. The wildcard characters are "x", "X" and blank (space character). Wildcards are useful when you want to specify all MAC addresses from a given manufacturer. Thus for example, by specifying only the Organizationally Unique Identifier (the first six hexadecimal digits of any MAC address from that manufacturer is its OUI) saves you having to enter all 24 million of them (the table size is limited in the AP/Router to 128 entries). Some manufacturers produce devices using more than one OUI, in which case you may need to enter each applicable one.
- **Name**: You may optionally assign a name to a given MAC address. This helps you recognize known equipment. Names are not used by the router/AP device, they are merely an aid for recognizing equipment on your network. Names need not be specified and do not need to be unique. Names are accessible by Service Provider Technical Support personnel, so if privacy is a concern, you may wish to use generic-sounding names, such as "Room 1 TV", or not use names at all.
- **Remove**: Check the 'Remove' box for any row(s) you no longer want used.

VLANs

The VLAN page is used to configure the virtual LAN (VLAN) parameters of the AP. Traffic never uses VLAN tags over wireless links, but traffic originating on or destined for wireless-LAN stations can be differentiated by a VLAN identifier as it travels over other links, such as Ethernet, DSL or cable-Internet, etc., thus given the appropriate priority as it traverses the Internet.

VLAN topics covered in this section

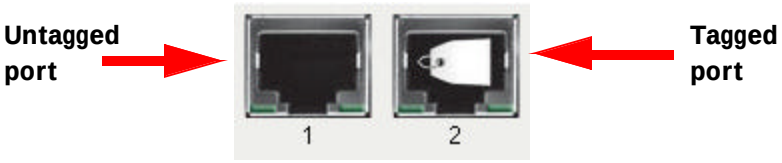


Navigating the VLAN page

- **Name**: The name appearing in the first cell of each column identifies each "network". Here the term refers to a single broadcast-domain. There is also a "Management" network, referring to communications directly to the AP/Router.
- **VLAN ID**: If the VLAN ID field is blank or empty, no VLAN tagging will occur for that network. The state is shown by one of three images, explained below in "VLAN port state icons."

Note	If two rows (two networks) are assigned the same VLAN ID, then they are considered to be the same network.

- VLAN tagging: Each RJ45 port can be configured to use VLAN tagging. By default, no RJ45 port is tagged. When the icon contains a white "tag", that port is tagged; otherwise it is un-tagged. Clicking on the icon switches between tagged and un-tagged modes.
    - **RJ45 port state images**: The AP/Router may be connected to the same or different service-provider "uplinks" using the RJ45-type connectors on the back of the AP/Router. The images of RJ45 connectors represent those RJ45 connectors on the AP. Each image includes the label of the RJ45 port which it represents. Clicking on an icon switches between "tagged" and "un-tagged" modes. When the icon contains a white "tag", that port is tagged; otherwise it is un-tagged. If desired, traffic can be distinguished with different VLAN IDs, which you configure using this page.



- **VLAN port state icons**: "Member VLAN ports" allow the network's traffic to flow through it's associated RJ45 connector. If that port is configured for VLAN-tagging, then the "tagged member VLAN port" icon will be displayed. A "non-member VLAN port" does not allow network traffic to flow through the RJ45 connector.

  Clicking an icon toggles that VLAN port between "member" and "non-member" status. The port may automatically be marked as "tagged" where appropriate.

- **Show me an example**: Clicking on the button labeled **Show me an example** opens a few sample configurations, with an explanation of what each shows. See *"VLAN configuration examples"* on page48.
- **Update Settings (test)**: When you click **Update Settings (test)**, if any configuration settings changed, a connectivity-test will be run; this lasts approximately 30 seconds. If the browser and the AP/Router can communicate with the new VLAN settings, then they will remain set. If connectivity fails, then the device will revert to the previous VLAN settings. A pop-up message will tell you whether the test passed or failed and VLAN values were reverted.
- **Update Settings (no testing, override)**: When you click **Update Settings (no testing, override)**, you are saving configuration changes without a connectivity test.

VLAN configuration examples

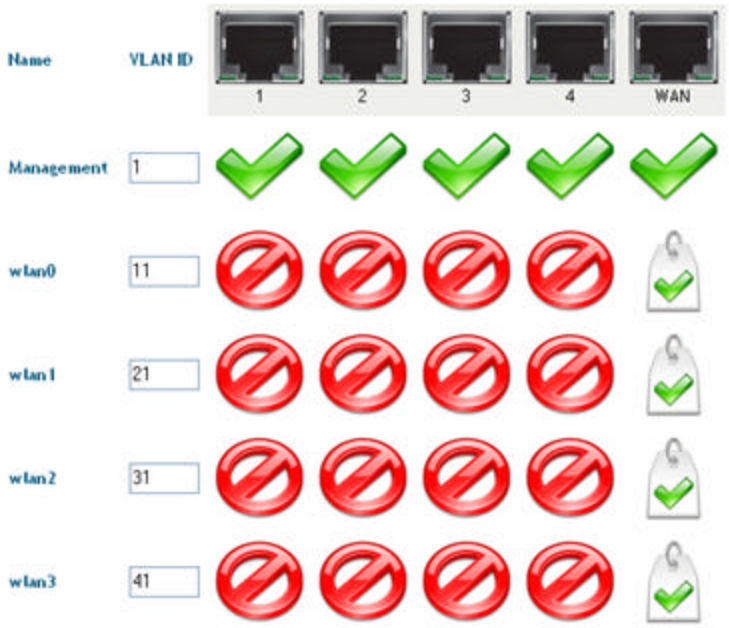
Default Configuration

By default, the Management network and all WLANs are mapped to the same VLAN and are available untagged on all ports.

VLAN Separation

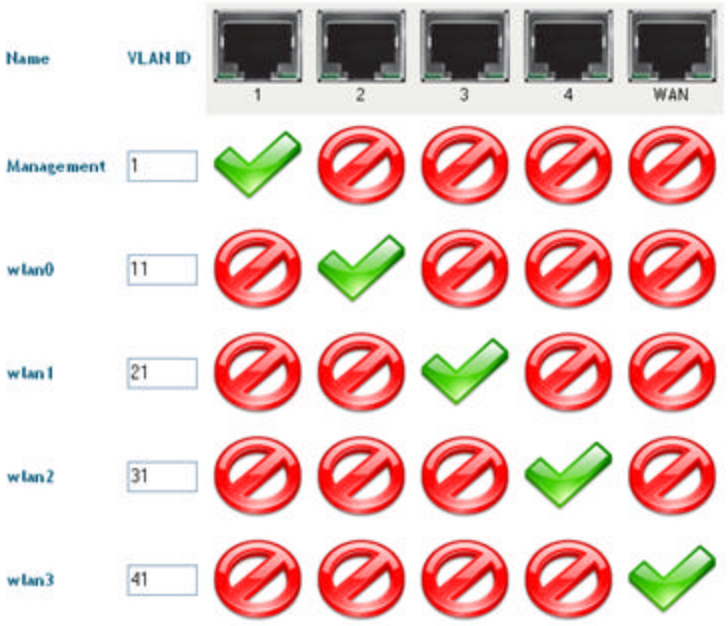
In this example, each wireless LAN (wlan#) is mapped to a different VLAN (e.g., wlan0 is mapped into VLAN 11). All of these WLANs are available on the WAN port where the Management network is untagged and the rest of the VLANs are tagged.

The Management network is available untagged on all ports.



Physical Port Separation

In this example, each WLAN is mapped to a physical port. None of the networks is tagged.



Changing a VLAN ID

This task should be performed by an experienced network administrator or are under the guidance of an IT/support professional.

1 After logging into the Web User interface, click **VLAN** under Administrator.

The Administrator::VLAN workspace appears.

2 Clear the value in the VLAN ID column, and type the new value.

3 Click **Update Settings (test)** to verify connectivity prior to saving changes. This prevents you from being locked out in the event you were to change the Management interface VLAN ID.

ALERT This works best in conjunction with *"Changing the port state for a VLAN"* and *"Changing an RJ45 port's VLAN tagged state"* for individual state changes.

Changing the port state for a VLAN

This task should be performed by an experienced network administrator or are under the guidance of an IT/support professional.

1 After logging into the Web User interface, click **VLAN** under Administrator.

The Administrator::VLAN workspace appears.

2 Click a green check mark to change the state between member, non-member, or tagged member.

3 Click **Update Settings (test)** to verify connectivity prior to saving changes. This prevents you from being locked out in the event you were to change the Management interface VLAN ID.

ALERT This works best in conjunction with *"Changing a VLAN ID"* and *"Changing an RJ45 port's VLAN tagged state"* for individual state changes.

Changing an RJ45 port's VLAN tagged state

This task should be performed by an experienced network administrator or are under the guidance of an IT/support professional.

1 After logging into the Web User interface, click **VLAN** under Administrator.

The Administrator::VLAN workspace appears.

2 Click an RJ-45 port icon to change the state from untagged to tagged.

3 Click **Update Settings (test)** to verify connectivity prior to saving changes. This prevents you from being locked out in the event you were to change the Management interface VLAN ID.

ALERT This works best in conjunction with *"Changing a VLAN ID"* and *"Changing the port state for a VLAN"* for individualized state changes.

Renewing or Releasing DHCP

This task should be performed only with guidance from your ISP. It serves as a troubleshooting technique when DHCP addresses to one or more networked devices prove to be unusable or in conflict with others.

1 After logging in to the Web User interface, click **Internet** under Status.

2 Review the current settings.

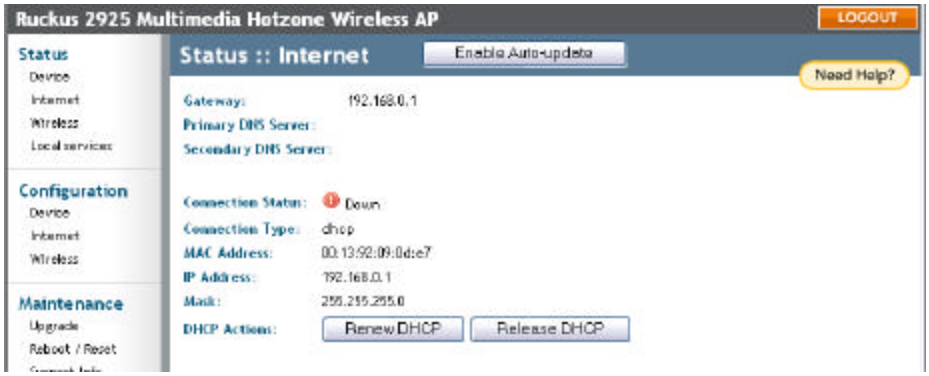


FIGURE 4-6

3 If the current **Connection Type** is DHCP, you will be able to see the currently-assigned IP address and subnet mask listed below.

- To force the DHCP server to assign a new IP address to this AP, click **Renew DHCP**. This will cause a slight interruption in network service until the new IP address has been put in use.
- To force the DHCP server to assign new IP addresses to all networked devices at the same time (including this AP), click **Release DHCP**. This will cause a temporary interruption in overall network service.

Upgrading the AP Firmware

You can use the Web User interface to check for software updates/upgrades for the firmware built into the AP. You can then apply these updates to the device in one of two ways: [1] manual updating on an as-needed basis or [2] automating a regularly scheduled update.

Before starting, decide which option you want to take:

- Automate a regularly scheduled update
- Run a one-time manual update right now.

By default, the automatic upgrade option is active, and will check the Ruckus Wireless update server every 12 hours.

1 After logging into the Web User interface, click **Upgrade** under Maintenance.

The Maintenance::Upgrade options appear.

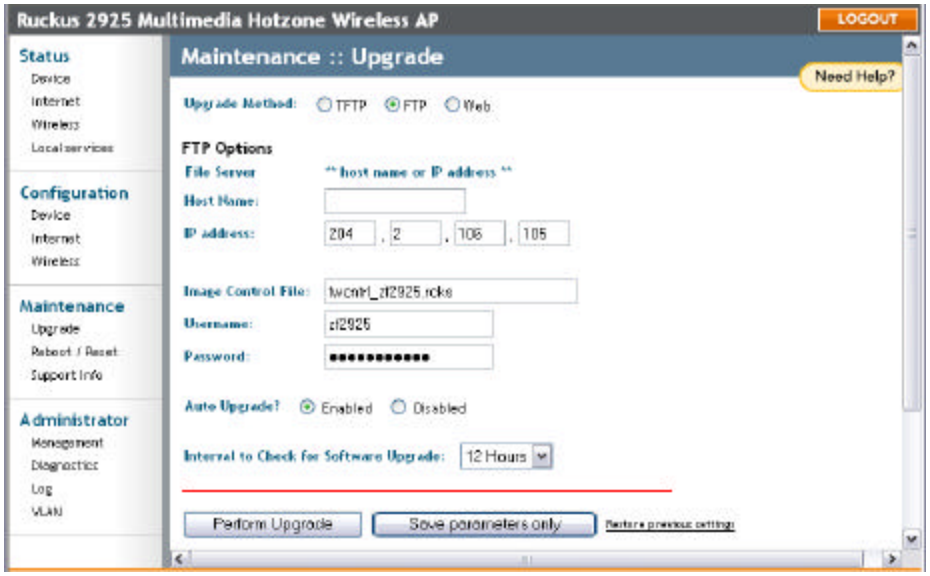


FIGURE 4-7:

2 Each of the three upgrade options listed in this workspace are described in separate sections following.

[-1-] Running a manual upgrade through the Web

1 In the Upgrade Method options, click **Web**.

2 Click in the Web Options **URL** field and type the URL of the download web site.

- Remember to start the URL with http://

3 You can change the **Image control file** filename extension as noted here:

- Replace any file names ending in .rcks with the .html extension
- Replace any file names ending in .fI7 with the .html extension

4 **Do not change** the **Username** or **Password** entries.

5 Click **Perform Upgrade.**

A status bar appears during the upgrade process.

6 When the upgrade is complete, you must manually reboot the AP.

[-2-] Running a manual upgrade through an FTP/TFTP server

1 In the Upgrade Method options, click **FTP** or **TFTP**.

2 Click on the host name field and type the URL of the server, or click on the IP address field and type the IP address of the server. (Remember to start the URL with FTP://)

3 Do not change any of the **Image control file**, **Username**, or **Password** entries.

4 Click **Perform Upgrade**.

A status bar appears during the upgrade process.

5 When the upgrade is complete, you must manually reboot the AP.

[-3-] Scheduling an automatic upgrade

1 In the Upgrade Method options, click the button by your preferred choice.

2 Enter the appropriate information in the **Host name** field or **IP address** field.

3 Do not change any of the **Image control file**, **Username**, or **Password** entries.

4 Make sure that the **Auto upgrade enables** option is checked (active).

5 Open the **Interval to check** menu and select your preferred interval.

6 You have two options at this point:

- Click **Perform Upgrade**, which will start the process and the clock. The next upgrade will occur at the selected interval.
- Click **Save parameters only.** The clock starts right away, and the actual upgrade will occur at the first effective interval.

A status bar appears during the upgrade process.

When the upgrade is complete, the AP will reboot automatically.

Rebooting the AP

You can use the Web User interface to prompt the AP to reboot, which simply restarts the AP without changing any of the current settings. Please note that this will disrupt network communications in any currently active hotspots.

1 After logging into the Web User interface, click **Reboot/Reset** under Maintenance

The Maintenance::Reboot/Reset workspace appears.

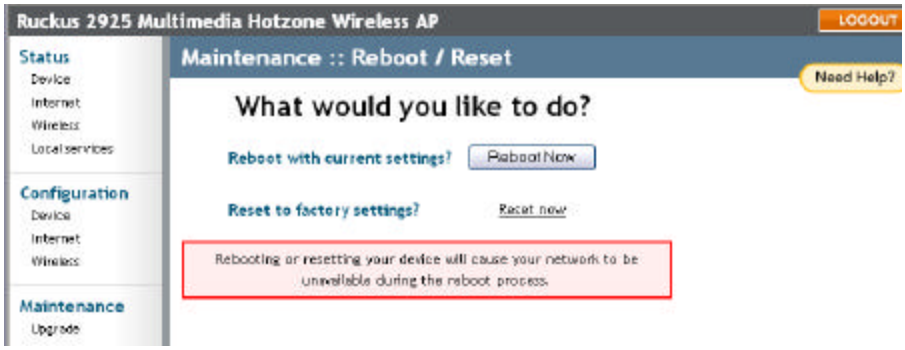


FIGURE 4-8:

2 Review the options.

3 Click **Reboot now**.

After a brief pause, you will be automatically logged out of the AP.

4 After a minute or so, you should be able to log back into the AP—which verifies that the reboot was successful. (Viewing the activity lights on the front of the AP also verifies the current status of the device

Restoring the AP to Factory Default Settings

ALERT!	DO NOT DO THE FOLLOWING unless you are directed to do so by Ruckus Wireless support staff or by a network administrator. Do this only if you are able to immediately reconnect the restored AP to your computer, to reconfigure it for wi-fi network use—as detailed in *"Installation, Setup, and Placementof the AP"* on page4.

You can use the Web User interface to restore an inoperative AP to its factory default settings, which will completely erase the configuration currently active in the device. Note, too, that this will disrupt all wi-fi network communications through this device.

After restoring the factory default state, you can reset the AP to match your preferences, as detailed in *"Installation, Setup, and Placementof the AP"* on page4.

1 After logging into the Web User interface, click **Reboot/Reset** under Maintenance

The Maintenance::Reboot/Reset workspace appears.

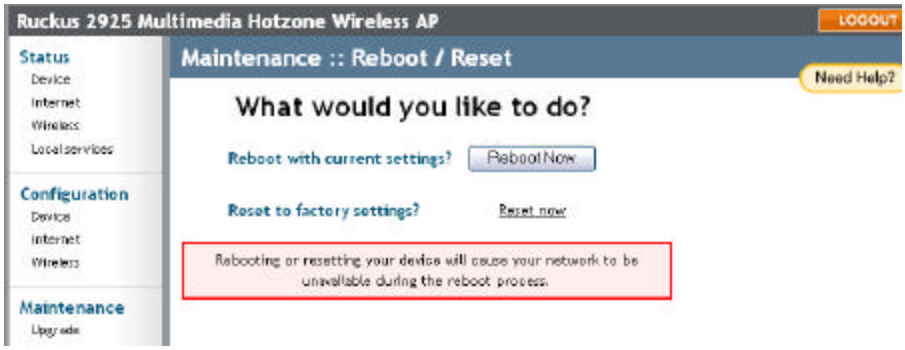


FIGURE 4-9:

2 Review the options.

3 Click **Reset now** (by *Restore to factory settings*).

After a brief pause, you will be automatically logged out of the AP.

You must now disconnect the AP from the switch (and the network) and re-connect it to your computer, as described in *"Installation, Setup, and Placementof the AP"* on page 4. At this time, you can restore the network settings, then replace it in your site for full network use.

CHAPTER 5

Monitoring Activity in the Access Point

This chapter provides information on how you can use the *Web User Interface* to monitor the activity and status of your Ruckus Wireless AP, its network, and (in a limited way) who is connected to your wi-fi hotzone.

Chapter Contents

Monitoring WLAN Use

A limited usage-monitoring capability has been built into the AP, that aids you in efficiently tracking and blocking rogue Access Points that are in use.

1 After opening the Web User interface, click **Wireless** under Status.

2 When the Status::Wireless workspace appears, click any of the hotspot tabs..

3 Look at the list of **Connected Devices**.

A table lists all currently active access points—authorized and rogue—associated with this particular hotspot.

4 Repeat this procedure on all other hotspot-specific tabs to gain an overall view of devices in your network.

5 For a more detailed view of AP activity, click the **MAC address** link in the Connected Devices table.

Monitoring Local Services

1 After opening the Web User interface, click **Local Services** under Status.

2 The Status::Local Services workspace appears, displaying a list of devices (computers, printers, access points) that are currently connected to the local network.

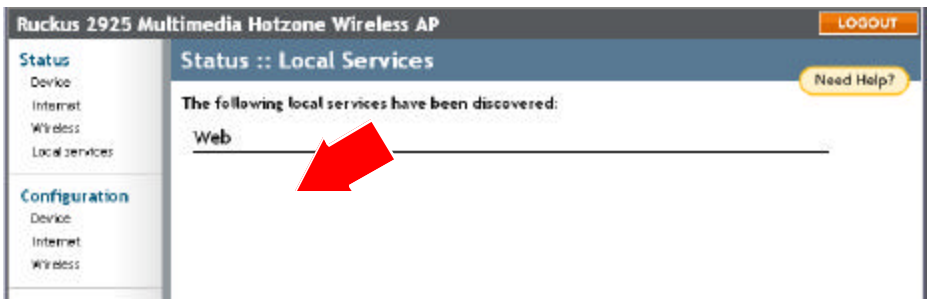


FIGURE 5-1

Activating the AP Log and Sending the Log to a Syslog Server

1 After logging in to the Web User interface, click **Log** under Administrator.

The Administrator::Log workspace appears.

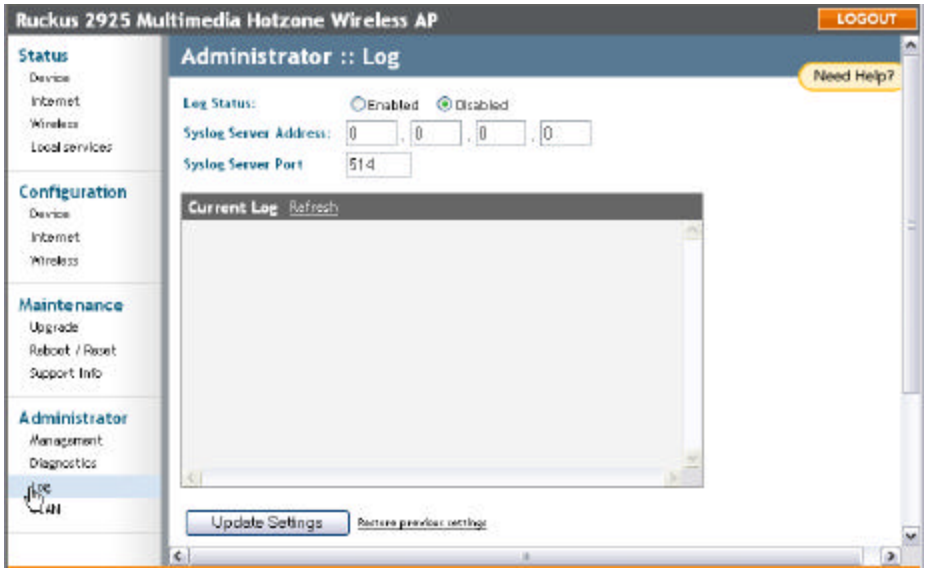


FIGURE 5-2

2 Look for **Log status** and click **Enabled**. (By default the log is disabled.)

3 After enabling the log, you can make the following changes:

Syslog server address	[Optional] To enable the AP to send messages to a syslog server as they appear, enter the IP address for the server in this field.
Syslog server port	By default the port number is 514. If the syslog server watches a different port, enter that port number in this field.

4 Click **Update Settings** to save and apply your changes.

Reviewing the Latest Log File Entries

The Log screen shows the log messages kept by the Ruckus Wireless Router since it was rebooted. The log has limited size: the oldest messages are replaced as new messages arrive.

1 After logging into the Web User interface, click **Log** under Administrator.

The Administrator::Log workspace appears.

ALERT	if you have not previously activated the AP log function, you will need to do so now as there will be no entries in the log file. For more information see the previous section.

The current log contents are displayed in a frame inside the workspace. The most recent entries are shown in chronological order, with the most recent entries being at the top of the log frame.

2 After reviewing the log file contents, you can save a copy of the log file to your local PC, if needed. For more information, see the following section.

Sending a Copy of the Log File to Support Staff

The Support Info log consists of the configuration and run-time status of the Ruckus Wireless AP and can be useful for troubleshooting.

You have three options for sending a copy of the Current Log file to support staff:

- Save a copy to your local PC, then attach it to an e-mail message and send it to support
- Set up a connection to an FTP site
- Set up a connection to a TFTP site

To take advantage of these options, follow these steps

1 After logging into the Web User interface, click **Support Info** under Maintenance

2 When the Maintenance::Support info workspace appears, review the Upload Method options.

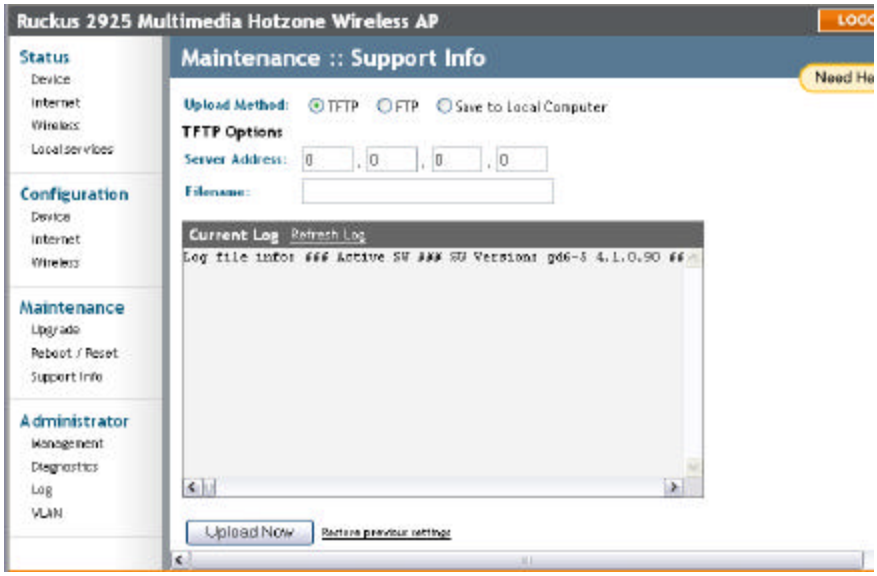


FIGURE 5-3

3 To upload a copy of the support info file to an FTP or TFTP server, click the appropriate button by **TFTP** or **FTP**. Selecting FTP prompts you to enter a User ID and Password.

4 Enter the Server IP address in the **Server Address** field.

5 Enter a name for this file in the **Filename** field.

ALERT	Remember to add a .TXT file extension to the file name, especially if you are using Internet Explorer as your Web Admin "host".

6 When you're ready, click **Upload Now**.

Saving a copy of the Log to your computer

You can manually send a copy of the Current Log to your own computer, if needed.

1 After logging into the Web User interface, click **Support Info** under Maintenance

The Maintenance::Support Info workspace appears.

2 Review the **Upload Method** options

3 Click the button by **Save to local computer**.

4 Click **Upload Now**.

5 When the "Save as..." dialog appears, change the destination directory and change the file name if you prefer.

ALERT	Remember to add a .TXT file extension to the file name, especially if you are using Internet Explorer as your Web Admin "host".

6 Click **Save** to save the file to your computer.

Running Diagnostics on Network Connections

Two network connection tests have been built into the AP that you can take advantage of in the Web User interface: ping and traceroute.

To run diagnostics for network troubleshooting, follow these steps:

1 After logging in to the Web User interface, click **Diagnostics** under Administrator.

The Administrator::Diagnostics workspace appears.

FIGURE 5-4

Two options are available:

- **Ping**
- **Traceroute**

2 Click in the text field by the option you want to activate, and type the network address of a site you wish to connect to.

3 Click **Run Test**.

The results appear in the text field below each option.