IEEE 802.11g
Wireless Dual-Radio Bridge-AP

User's Guide

Version: 1.0

Last Updated: 05/07/2004

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.

Table of Contents

1. Introduction

1.1. Overview

The wireless Dual-Radio Bridge-AP (*DRBAP* for short) is a multifunction device that has two independently configurable IEEE 802.11g interfaces. Each IEEE 802.11g interface can be configured either as an AP (Access Point) interface or a LAN-to-LAN bridge interface. An AP interface enables wireless clients to associate with this device for IEEE 802.11 *infrastructure* applications and the wireless clients can be authenticated by IEEE 802.1x/RADIUS. A LAN-to-LAN bridge interface enables the device to connect to at most 6 other bridges wirelessly by the Wireless Distribution System (WDS) technology.

With the sleek and intuitive Web-based user interface and Windows-based user interface (Wireless Network Manager), an administrator can easily and clearly manage the dual-radio bridge-AP. With its maximal versatility and ease-of-management, this device can satisfy system integrators' various requirements.

In Chapter 2, we describe the steps to install and configure a newly acquired DRBAP. Following the steps, the DRBAP can be quickly set up to work. In Chapter 3, detailed explanation of each Web management page is given for you to understand how to fine-tune the settings of a DRBAP to meet his or her specific needs. In addition to using Web-based management user interface to configure a DRBAP, the Windows-based Wireless Network Manager can also be used to configure and monitor deployed DRBAPs. See the on-line help of Wireless Network Manager for more information.

1.2. Features

- **IEEE 802.11g**
    - **Dual interfaces.** Each of the two IEEE 802.11g interfaces can be configured, according to the operation mode, as an AP (Access Point) interface or a LAN-to-LAN bridge interface.
    - **Operational modes**
        - **Bridge Repeater**. In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges. It's possible to use multiple bridge repeaters between two LAN-to-LAN bridges if the distance is very long.
        - **AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface. The AP repeater is suitable for situations in which Ethernet wiring between the AP and the network backbone is impossible or costs highly.
        - **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle *twice* the number of wireless clients than a normal AP. It can be treated as "two APs in a box."
    - **AP interface**
        - **Enabling/disabling SSID broadcasts.** The administrator can enable or disable the SSID broadcasts functionality for security reasons. When the SSID broadcasts

functionality is disabled, a client computer cannot connect to the AP interface with an "any" SSID; the correct SSID has to be specified on client computers.

- **MAC-address-based access control.** Blocking unauthorized wireless client computers based on MAC (Media Access Control) addresses. The ACL (Access Control List) can be downloaded from a TFTP server.

- **WPA (Wi-Fi Protected Access).** The AP interface supports the WPA standard proposed by the Wi-Fi Alliance (http://www.wi-fi.org). Both WPA-PSK (Pre-Shared Key) mode and full WPA mode are supported. WPA is composed of TKIP (Temporal Key Integrity Protocol) and IEEE 802.1x and serves as a successor to WEP for better WLAN security.

- **IEEE 802.1x/RADIUS.** User authentication and dynamic encryption key distribution can be achieved by IEEE 802.1x *Port-Based Network Access Control* and RADIUS (*Remote Authentication Dial-In User Service*).

- **Wireless client isolation.** Wireless-to-wireless traffic among the associated wireless clients can be blocked so that the wireless clients cannot see each other. This capability can be used in hotspots applications to prevent wireless hackers from attacking other wireless users' computers.

- **AP load balancing.** Several APs can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the APs. This function is available when the AP is in AP/Bridge mode.

- **Link integrity.** If the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the AP and no wireless client can associate with it.

- **Association control.** When the AP is in AP/Bridge mode, it can be configured to deny association requests when it has served too many wireless clients or traffic load is too heavy.

- **Associated wireless clients status.** Showing the status of all wireless clients that are associated with the AP interface.

- **LAN-to-LAN bridge interface**

  - **6 Bridge links.** The bridge provides 6 bridge links based on the WDS (Wireless Distribution System) technology, so that it can wirelessly connect to at most 6 other wireless bridges, APs, or wireless routers with WDS support.

  - **Antenna alignment assistance.** The DRBAP provides a WDS link quality indicator via Wireless Network Manager to facilitate alignment of directional antennas when deploying pairs of wireless bridges.

  - **Link health monitoring.** This feature enables the administrator to see if the WDS links of the DRBAP to other peer wireless bridges are working fine.

- **RF type selection.** The RF type of each WLAN interface can be configured to work in IEEE 802.11b only, IEEE 802.11g only, or mixed mode (802.11g and 802.11b simultaneously).

- **64-bit and 128-bit WEP (Wired Equivalent Privacy).** Data transmitted over AP or bridge links can be protected by WEP encryption for better security.

  - **Transmit power control.** Transmit power of the DRBAP's RF modules can be adjusted to change RF coverage of the DRBAP.

  - **Detachable antennas.** The factory-mounted antennas can be replaced with high-gain antennas for different purposes.

- **DHCP client.** The DRBAP can automatically obtain an IP address from a DHCP server.

- **DHCP server.** The DRBAP can automatically assign IP addresses to computers or other devices by DHCP (Dynamic Host Configuration Protocol).

  - **Static DHCP mappings.** The administrator can specify static IP address to MAC address mappings so that the specified IP addresses are always assigned to the hosts with the specified MAC addresses.

  - **Showing current DHCP mappings.** Showing which IP address is assigned to which host identified by an MAC address.

- **Packet Filtering.** The DRBAP provides Layer 2, Layer 3, and Layer 4 filtering capabilities.

- **Firmware Tools**

  - **Firmware upgrade.** The firmware of the DRBAP can be upgraded in the following methods:

    - **Xmodem-based.** Upgrading firmware over RS232.

    - **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).

    - **HTTP-based.** Upgrading firmware by HTTP (HeperText Transfer Protocol).

  - **Configuration backup.** The configuration settings of the DRBAP can be backed up to a file via TFTP or HTTP for later restoring.

  - **Configuration reset.** Resetting the configuration settings to factory-default values.

- **Management**

  - **Windows-based Wireless Network Manager** for configuring, monitoring, and diagnosing the local computer and neighboring APs. The management protocol is MAC-based.

  - **Web-based Network Manager** for configuring and monitoring the DRBAP via a Web browser. The management protocol is HTTP (HeperText Transfer Protocol)-based.

  - **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.11, IEEE 802.1x, and Enterprise MIB are supported.

  - **UPnP.** The DRBAP responds to UPnP discovery messages so that a Windows XP user can locate the DRBAP in My Network Places and use a Web browser to configure it.

  - **System log.** For system operational status monitoring.

    - **Local log.** System events are logged to the on-board RAM of the DRBAP and can be viewed using a Web browser.

  - **Remote log by SNMP trap.** Systems events are sent in the form of SNMP traps to a remote SNMP management server.

- **Power over Ethernet (optional).** Supplying power to a DRBAP over an Ethernet cable using PowerDsine (http://www.powerdsine.com) technology (IEEE 802.3af compliant in the future). This feature facilitates large-scale wireless LAN deployment.

- **Hardware Watchdog Timer.** If the firmware gets stuck in an invalid state, the hardware watchdog timer will detect this situation and restart the DRBAP. This way, the DRBAP can provide continuous services.

1.3. LED Definitions

There are several LED indicators on the housing of the DRBAP. They are defined as follows:

- **ALV**: *Alive*. Blinks when the DRBAP is working normally.
- **RF**: IEEE 802.11g interfaces activity
- **LAN**: Ethernet LAN interface activity
- **PWR**: Power

2. First-Time Installation and Configuration

2.1. Selecting a Power Supply Method

Optionally, the DRBAP can be powered by the supplied power adapter or POE (Power over Ethernet). The DRBAP automatically selects the suitable one depending on your decision.

To power the DRBAP by the supplied power adapter:

1. Plug the power adapter to an AC socket.

2. Plug the connector of the power adapter to the power jack of the DRBAP.

NOTE: This product is intended to be power-supplied by a Listed Power Unit, marked “Class 2” or “LPS” and output rated “5V DC, 1 A minimum” or equivalent statement.

To power the DRBAP by POE:

1. Plug one connector of an Ethernet cable to an available port of an active Ethernet switch that can supply power over Ethernet.

2. Plug the other connector of the Ethernet cable to the **LAN/Config** port of the DRBAP.

2.2. Mounting the DRBAP on a Wall

The DRBAP is wall-mountable.

1. Stick the supplied sticker for wall-mounting.

2. Use a ϕ6.5mm driller to drill a 25mm-deep hole at each of the cross marks.

3. Plug in a supplied plastic conical anchor in each hole.

4. Screw a supplied screw in each plastic conical anchor for a proper depth so that the wireless DRBAP can be hung on the screws.

5. Hang the wireless DRBAP on the screws.

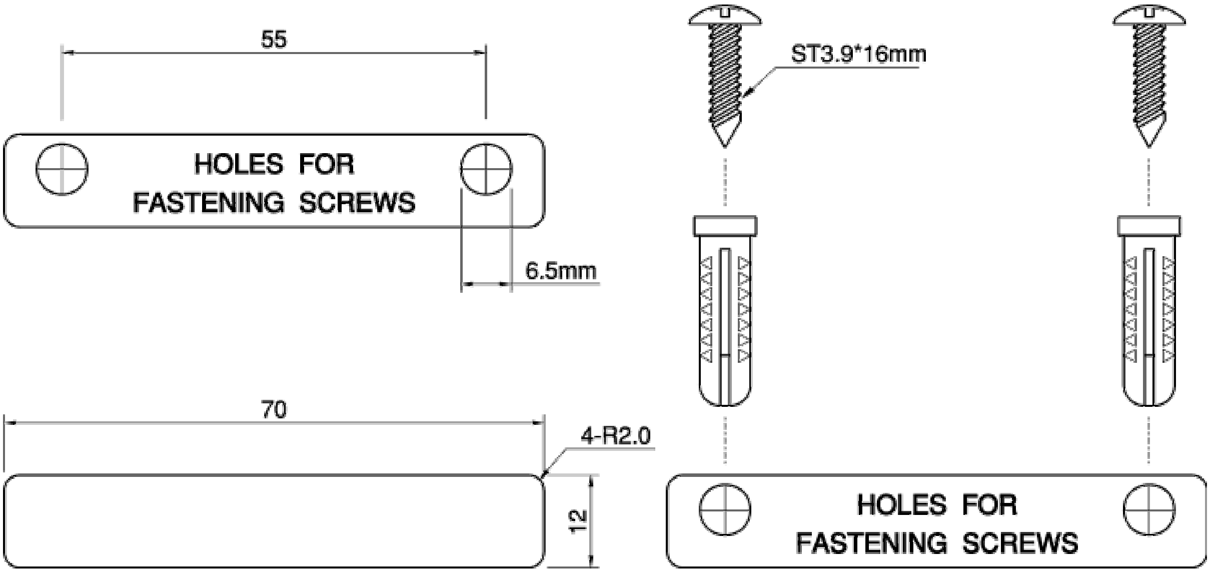


Fig. 1. Mounting the DRBAP on a wall.

2.3. Preparing for Configuration

For you to configure a DRBAP, a *managing computer* with a Web browser is needed. For first-time configuration of a DRBAP, an Ethernet network interface card (NIC) should have been installed in the managing computer. For maintenance-configuration of a deployed DRBAP, either a wireless computer (if the DRBAP is configured to act as an **AP Repeater** or **Dual AP**) or a wired computer can be employed as the managing computer.

NOTE: If you are using the browser, *Opera*, to configure a DRBAP, click the menu item **File**, click **Preferences...**, click **File types**, and edit the MIME type, **text/html**, to add a file extension ".sht" so that Opera can work properly with the Web management pages of the DRBAP.

Since the configuration/management protocol is HTTP-based, we have to make sure that **the IP address of the managing computer and the IP address of the *managed DRBAP* are in the same IP subnet** (the default IP address of a DRBAP is **192.168.0.1** and the default subnet mask is **255.255.255.0**.)

2.3.1. Connecting the Managing Computer and the DRBAP

To connect the Ethernet managing computer and the managed DRBAP for first-time configuration, you have two choices as illustrated in Fig. 2.

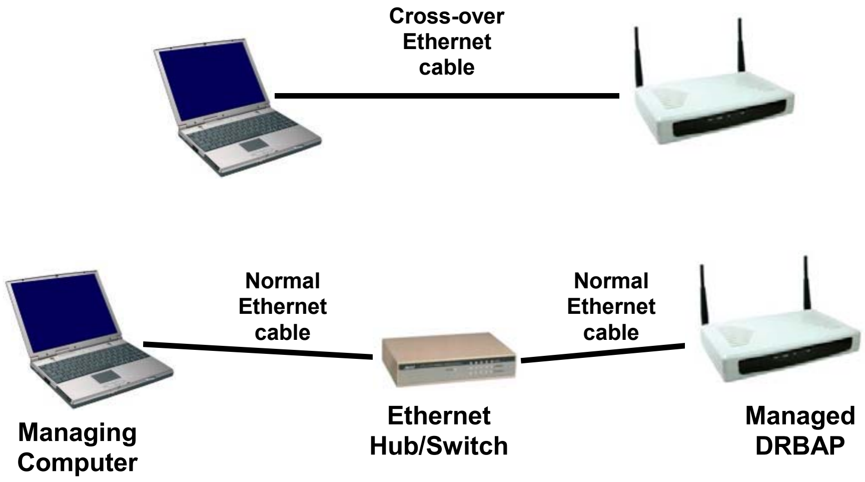


Fig. 2. Connecting a managing computer and a DRBAP via Ethernet.

You can use either a *cross-over* Ethernet cable (included in the package) or a switch/hub with 2 normal Ethernet cables.

NOTE: One connector of the Ethernet cable must be plugged into the **LAN/CONFIG** Ethernet jack of the DRBAP for configuration.

2.3.2. Changing the TCP/IP Settings of the Managing Computer

Use the **Windows Network Control Panel Applet** to change the TCP/IP settings of the managing computer, so that the IP address of the computer and the IP address of the DRBAP are in the same IP subnet. Set the IP address of the computer to **192.168.0.xxx** (the default IP address of a DRBAP is **192.168.0.1**) and the subnet mask to **255.255.255.0**.

NOTE: For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

TIP: After you have connected the managing computer and the DRBAP via Ethernet, you can install Wireless Network Manager on the managing computer and use it to configure the DRBAP without being concerned about the TCP/IP settings of the managing computer. Refer to the on-line help of Wireless Network Manager for more information.

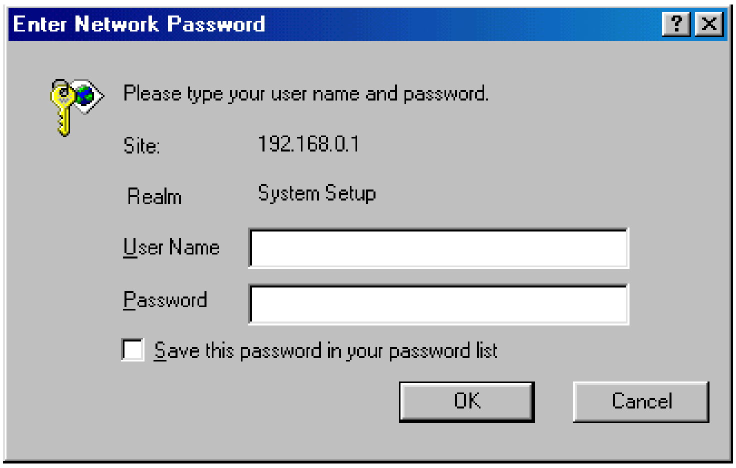
2.4. Configuring the DRBAP

After the IP addressing issue is resolved, launch a Web browser on the managing computer. Then, go to "**http://192.168.0.1**" to access the *Web-based Network Manager* start page.

TIP: For maintenance configuration of a DRBAP, the DRBAP can be reached by its *host name* using a Web browser. For example, if the DRBAP is named "DRBAP", you can use the URL "http://DRBAP" to access the Web-based Network Manager of the DRBAP.

2.4.1. Entering the User Name and Password

Before the start page is shown, you will be prompted to enter the user name and password to gain the right to access the Web-based Network Manager. For first-time configuration, use the default user name "**root**" and default password "**root**", respectively.



Please type your user name and password.

Site: 192.168.0.1

Realm System Setup

User Name

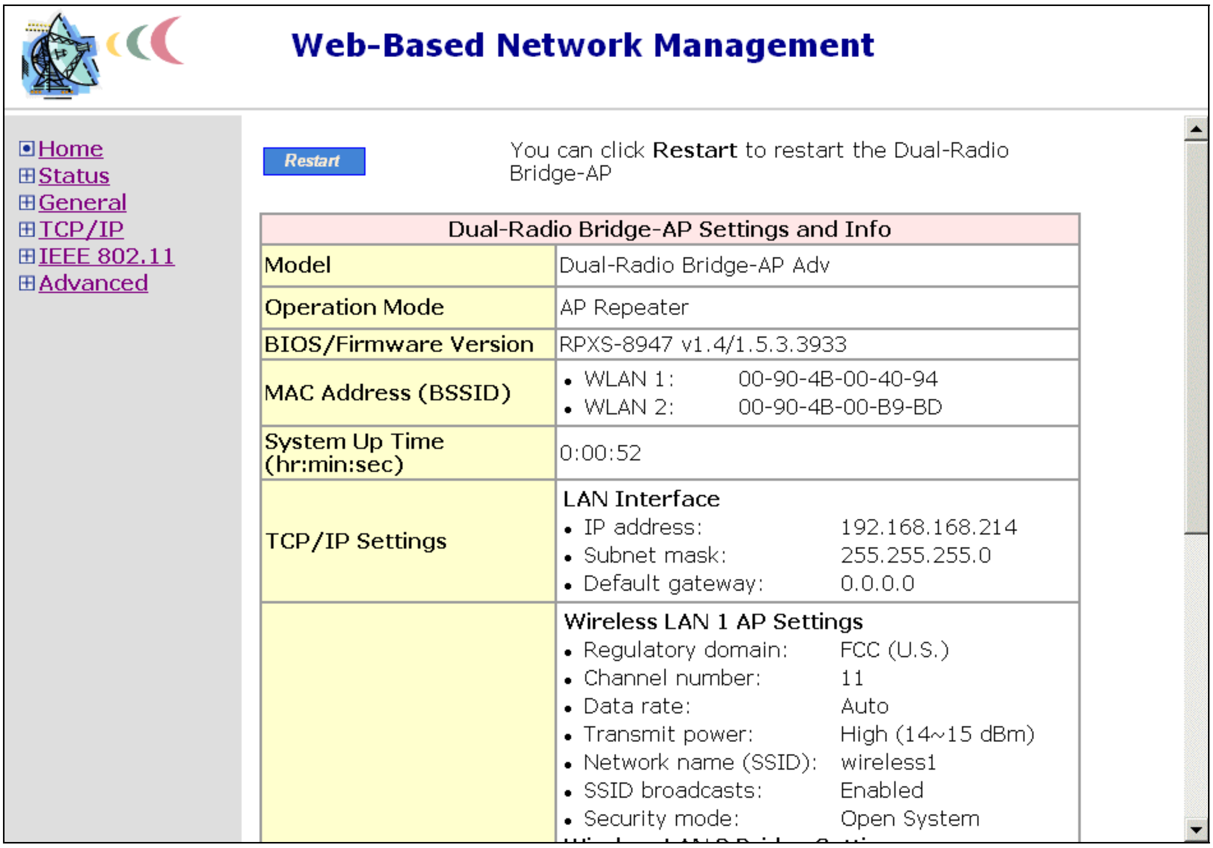
Password

□ Save this password in your password list

Fig. 3. Entering the user name and password.

NOTE: It is strongly recommended that the password be changed to other value for security reasons. On the start page, click the **General, Password** link to change the value of the password (see Section 3.3.1 for more information).

TIP: Since the start page shows the current settings and status of the DRBAP, it can be saved or printed within the Web browser for future reference.

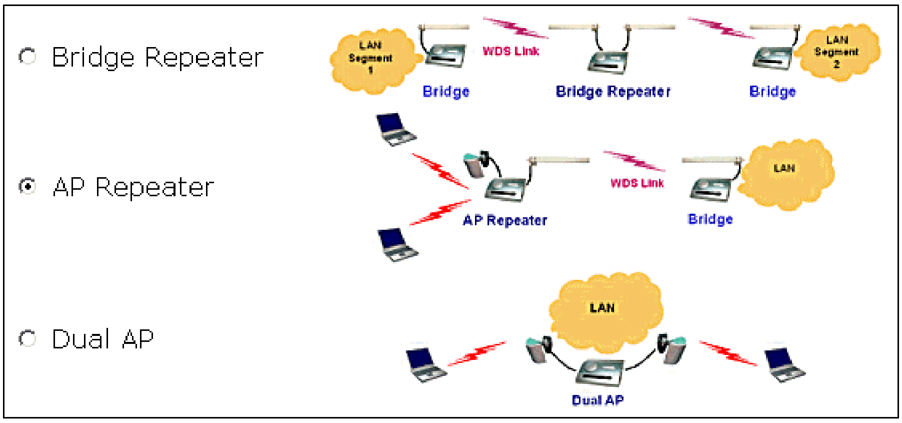


You can click **Restart** to restart the Dual-Radio Bridge-AP

Dual-Radio Bridge-AP Settings and Info	
Model	Dual-Radio Bridge-AP Adv
Operation Mode	AP Repeater
BIOS/Firmware Version	RPXS-8947 v1.4/1.5.3.3933
MAC Address (BSSID)	• WLAN 1: 00-90-4B-00-40-94 • WLAN 2: 00-90-4B-00-B9-BD
System Up Time (hr:min:sec)	0:00:52
TCP/IP Settings	LAN Interface • IP address: 192.168.168.214 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
	Wireless LAN 1 AP Settings • Regulatory domain: FCC (U.S.) • Channel number: 11 • Data rate: Auto • Transmit power: High (14~15 dBm) • Network name (SSID): wireless1 • SSID broadcasts: Enabled • Security mode: Open System

Fig. 4. The Start page.

2.4.2. Step 1: Selecting an Operational Mode



○ Bridge Repeater

● AP Repeater

○ Dual AP

Fig. 5. Operational modes.

Go to the **General, Operational Mode** section to select an operational mode for the DRBAP. There are 3 operational modes—*Bridge Repeater*, *AP Repeater*, and *Dual AP*.

- **Bridge Repeater**. In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges. It's possible to use multiple bridge repeaters between two LAN-to-LAN bridges if the distance is very long.

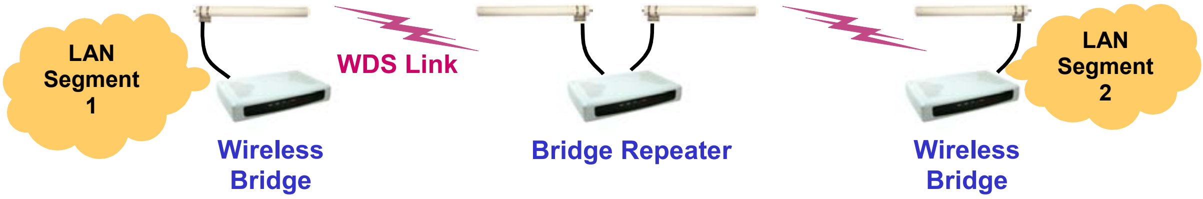


Fig. 6. **Bridge Repeater** mode.

- **AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface. The AP repeater is suitable for situations in which Ethernet wiring between the AP and the network backbone is impossible or costs highly.

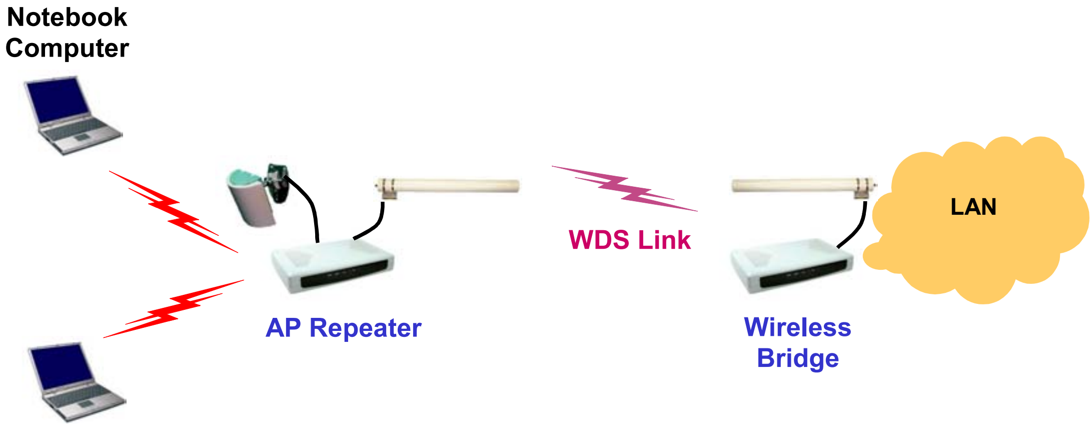


Fig. 7. **AP Repeater** mode.

- **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle *twice* the number of wireless clients than a normal AP. It can be treated as “two APs in a box.”

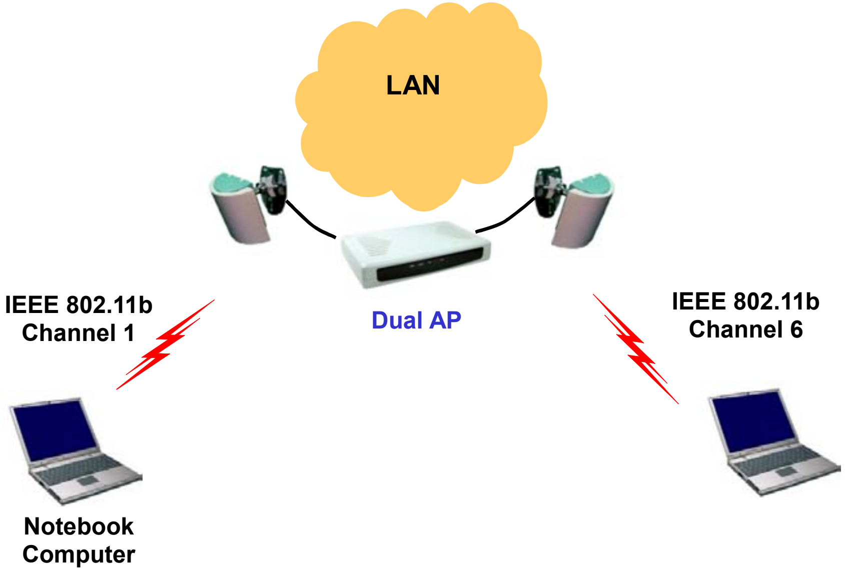
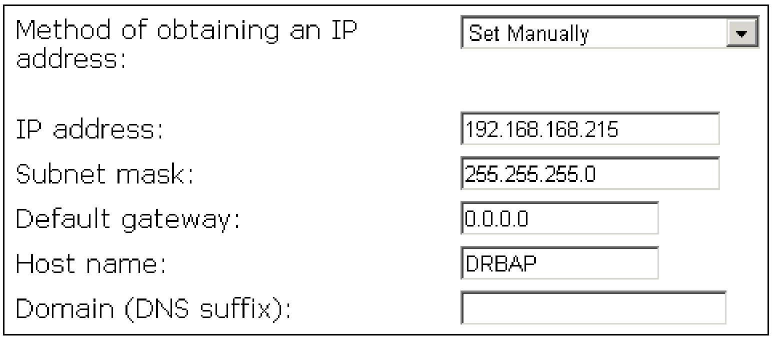


Fig. 8. **Dual AP** mode.

The following table shows the type of each WLAN interface for each operational mode.

	WLAN 1 Interface Type	WLAN 2 Interface Type
Bridge Repeater	LAN-to-LAN Bridge	LAN-to-LAN Bridge
AP Repeater	AP	LAN-to-LAN Bridge
Dual AP	AP	AP

2.4.3. Step 2: Configuring TCP/IP Settings



Method of obtaining an IP address:	Set Manually
IP address:	192.168.168.215
Subnet mask:	255.255.255.0
Default gateway:	0.0.0.0
Host name:	DRBAP
Domain (DNS suffix):	

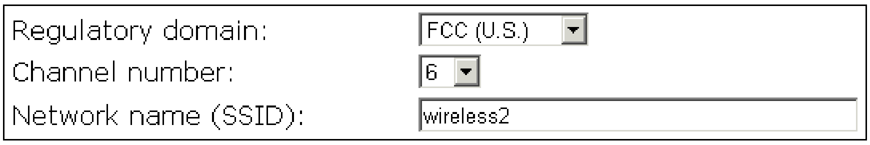
Fig. 9. TCP/IP settings.

Go to the **TCP/IP, Addressing** section to configure IP address settings. The IP address can be manually set or automatically assigned by a DHCP server on the LAN. If you are manually setting the **IP Address**, **Subnet Mask**, and **Default Gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host Name** and **Domain** (DNS suffix) of the DRBAP. When you are finished, click **Save** at the bottom of this page, and then you are brought back to the start page.

2.4.4. Step 3: Configuring IEEE 802.11 Settings

Go to the **IEEE 802.11, Communication** section to configure IEEE 802.11g-related communication settings, including *Regulatory Domain*, *Channel Number*, *Network Name (SSID)*, and *Bridge Links*, for both WLAN interfaces, depending on their interface types. No matter the type of a WLAN interface is AP or LAN-to-LAN bridge, Regulatory Domain, Channel Number, and Network Name have to be configured.

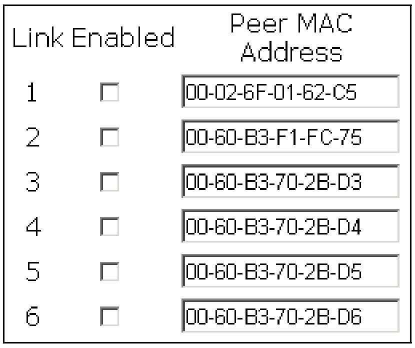
The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. **For two wireless devices to communicate with each other, they must be set to identical SSID (Service Set IDentifier).**



Regulatory domain: FCC (U.S.)
Channel number: 6
Network name (SSID): wireless2

Fig. 10. Basic IEEE 802.11g communication settings.

For a LAN-to-LAN bridge interface, also set the MAC address of each peer bridge according to your planned network topology. Specify an MAC address, and then select its corresponding checkbox.



Link	Enabled	Peer MAC Address
1	□	00-02-6F-01-62-C5
2	□	00-60-B3-F1-FC-75
3	□	00-60-B3-70-2B-D3
4	□	00-60-B3-70-2B-D4
5	□	00-60-B3-70-2B-D5
6	□	00-60-B3-70-2B-D6

Fig. 11. Bridge links settings.

When you are finished, click **Save** at the bottom of this page, and then you are brought back to the start page.

TIP: Plan your wireless network and draw a diagram, so that you know how a DRBAP is connected to other peer bridges and can therefore set the bridge links settings correctly.

TIP: Plan your wireless network and draw a diagram, so that you know how a bridge is connected to other peer bridges by WDS. See the following figure for an example network-planning diagram.

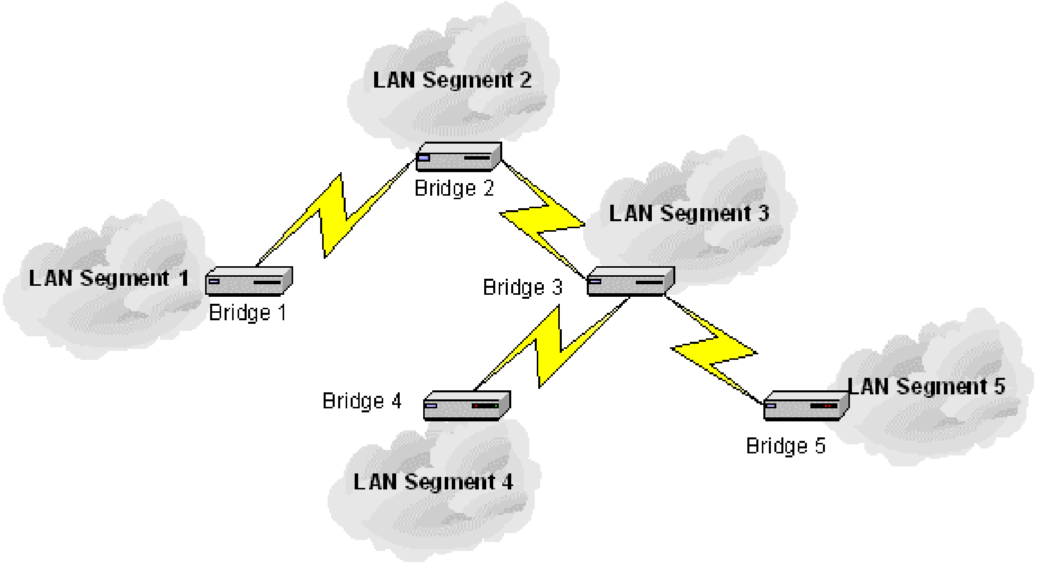


Fig. 12. Sample wireless bridge network topology.

WARNING: Don’t let your network topology consisting of wireless DRBAPs, wireless bridges, Ethernet switches, Ethernet links, and WDS links contains *loops*. If any loops exist, packets will circle around the loops and network performance will be seriously degraded.

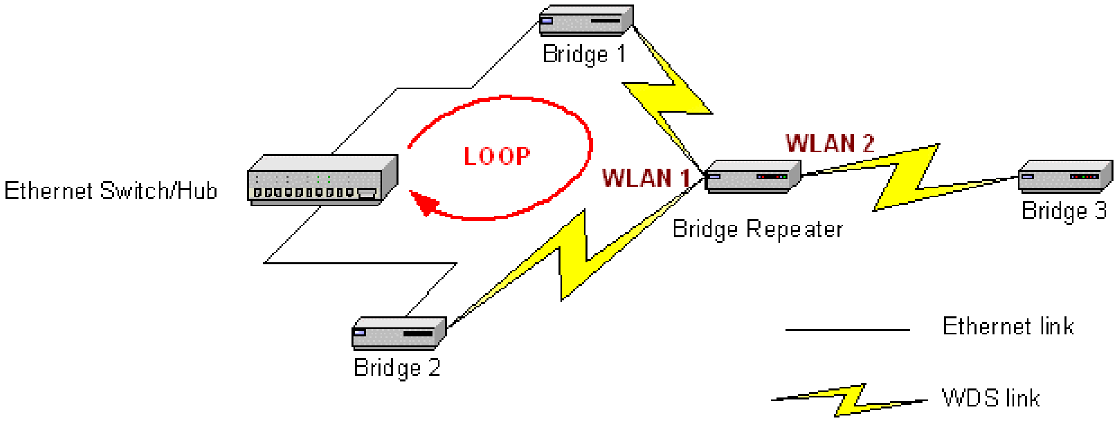
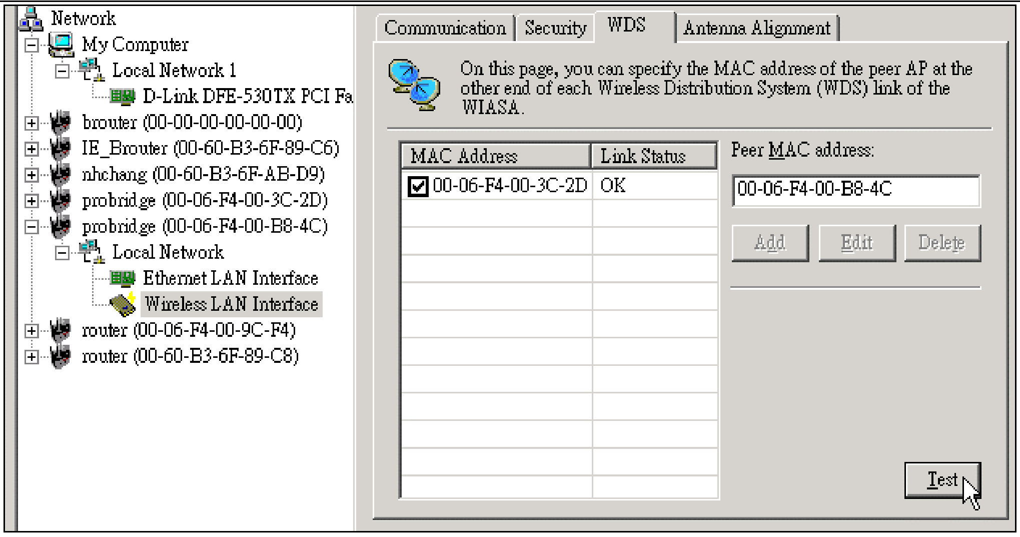


Fig. 13. Network topology containing a loop.

TIP: You can check whether the WDS links of the DRBAP are functioning by using Wireless Network Manager.


Network
My Computer
Local Network 1
D-Link DFE-530TX PCI Fa
brouter (00-00-00-00-00-00)
IE_Brouter (00-60-B3-6F-89-C6)
nhchang (00-60-B3-6F-AB-D9)
probridge (00-06-F4-00-3C-2D)
probridge (00-06-F4-00-B8-4C)
Local Network
Ethernet LAN Interface
Wireless LAN Interface
router (00-06-F4-00-9C-F4)
router (00-60-B3-6F-89-C8)
Communication
Security
WDS
Antenna Alignment
Add
Edit
Delete
Test

On this page, you can specify the MAC address of the peer AP at the other end of each Wireless Distribution System (WDS) link of the WIASA.

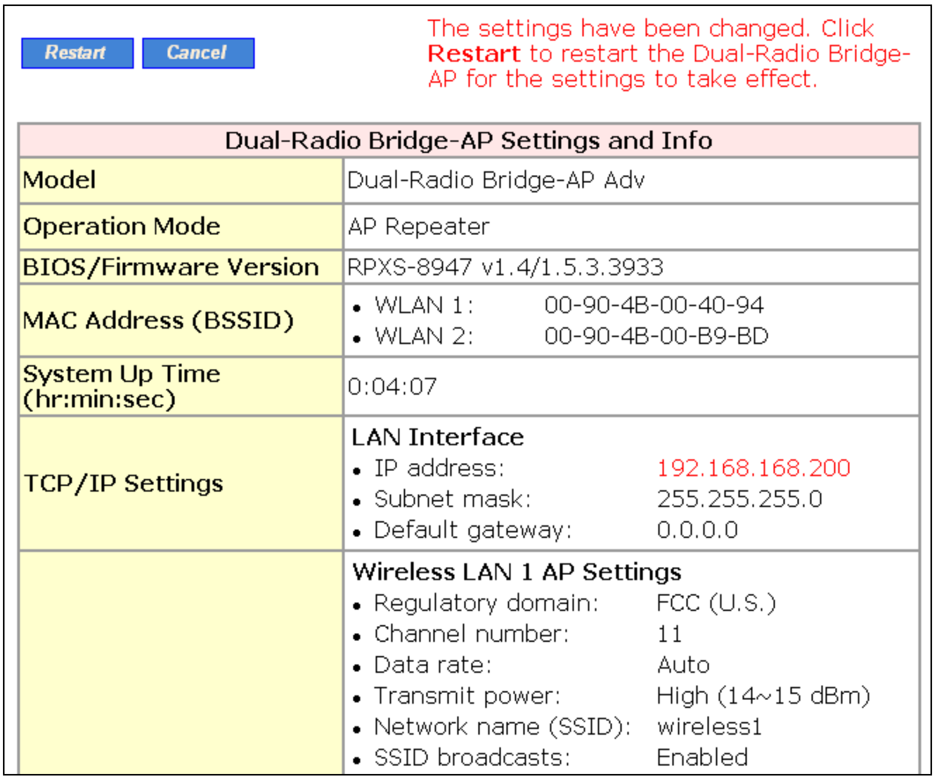
MAC Address	Link Status
☑ 00-06-F4-00-3C-2D	OK

Peer MAC address: 00-06-F4-00-B8-4C

Fig. 14. Link health monitoring.

Run Wireless Network Manager on a computer and locate the DRBAP you want to manage. Go to the WDS tab, and then click **Test**. The test results (*OK* or *Broken*) will be shown in the **Link Status** column of the WDS links table.

2.4.5. Step 4: Reviewing and Applying Settings



The settings have been changed. Click **Restart** to restart the Dual-Radio Bridge-AP for the settings to take effect.

Dual-Radio Bridge-AP Settings and Info	
Model	Dual-Radio Bridge-AP Adv
Operation Mode	AP Repeater
BIOS/Firmware Version	RPXS-8947 v1.4/1.5.3.3933
MAC Address (BSSID)	• WLAN 1: 00-90-4B-00-40-94 • WLAN 2: 00-90-4B-00-B9-BD
System Up Time (hr:min:sec)	0:04:07
TCP/IP Settings	LAN Interface • IP address: 192.168.168.200 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
	Wireless LAN 1 AP Settings • Regulatory domain: FCC (U.S.) • Channel number: 11 • Data rate: Auto • Transmit power: High (14~15 dBm) • Network name (SSID): wireless1 • SSID broadcasts: Enabled

Fig. 15. Settings changes are highlighted in red.

On the start page, you can review all the settings you have made. Changes are highlighted in red. If they are OK, click **Restart** to restart the DRBAP for the new settings to take effect.

NOTE: About *7* seconds are needed for the DRBAP to complete its restart process.

2.5. Deploying the DRBAP

After the settings have been configured, deploy the DRBAP to the field application environment. Connect the DRBAP to a LAN segment through an Ethernet switch/hub.

If external high-gain *directional* antennas are used for LAN-to-LAN bridge interfaces, it's difficult to adjust alignments of the antennas when distance between the DRBAP and its peer bridge is long.

To adjust the alignments of directional antennas:

1. Connect each device to a computer via Ethernet.

2. Configure the date rate of each bridge to the lowest value, 1Mbps.

3. Fix the alignment of the antenna on one side.

4. Adjust the alignment of the other side by using response time information obtained from PINGing (run PING.exe) the "fixed-side" computer.

5. Fine-tune the alignment of the antenna until you get a best response time.

6. Increase the data rate of each bridge simultaneously until a maximal workable data rate is reached. You may not be able to use the highest data rate, 54Mbps, because of the distance and the gain of the antennas.

Fig. 16 illustrates the idea.

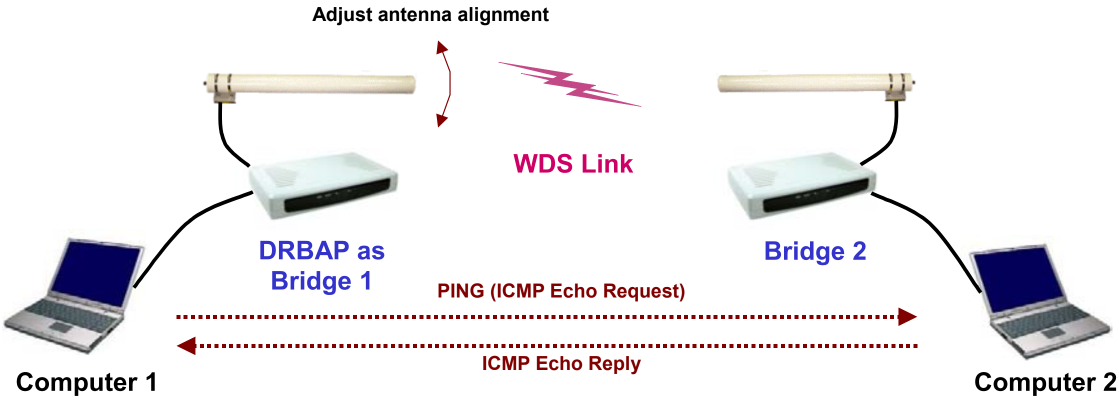
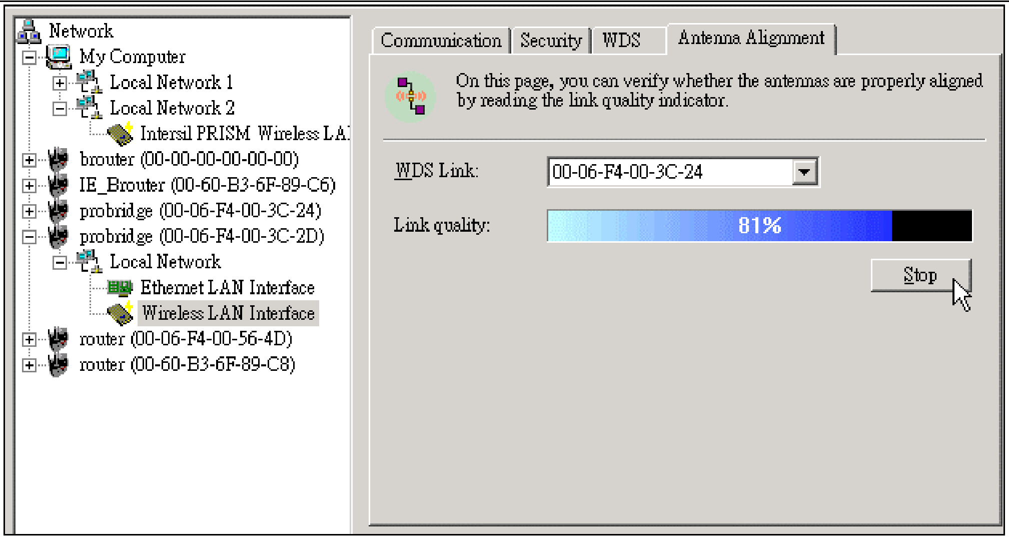


Fig. 16. Adjusting alignments of external directional antennas.

NOTE: There are two antenna connectors on one side of the DRBAP, which are labeled "**1**" and "**2**". Connector 1 is for the **WLAN 1** interface 1 and Connector 2 is for the **WLAN 2** interface.

TIP: You can make use of the Antenna Alignment Assistance feature to help you align the directional antennas.


Network
My Computer
Local Network 1
Local Network 2
Intersil PRISM Wireless LA
brouter (00-00-00-00-00-00)
IE_Brouter (00-60-B3-6F-89-C6)
probridge (00-06-F4-00-3C-24)
probridge (00-06-F4-00-3C-2D)
Local Network
Ethernet LAN Interface
Wireless LAN Interface
router (00-06-F4-00-56-4D)
router (00-60-B3-6F-89-C8)
Communication
Security
WDS
Antenna Alignment
Stop

On this page, you can verify whether the antennas are properly aligned by reading the link quality indicator.

WDS Link: 00-06-F4-00-3C-24

Link quality: 81%

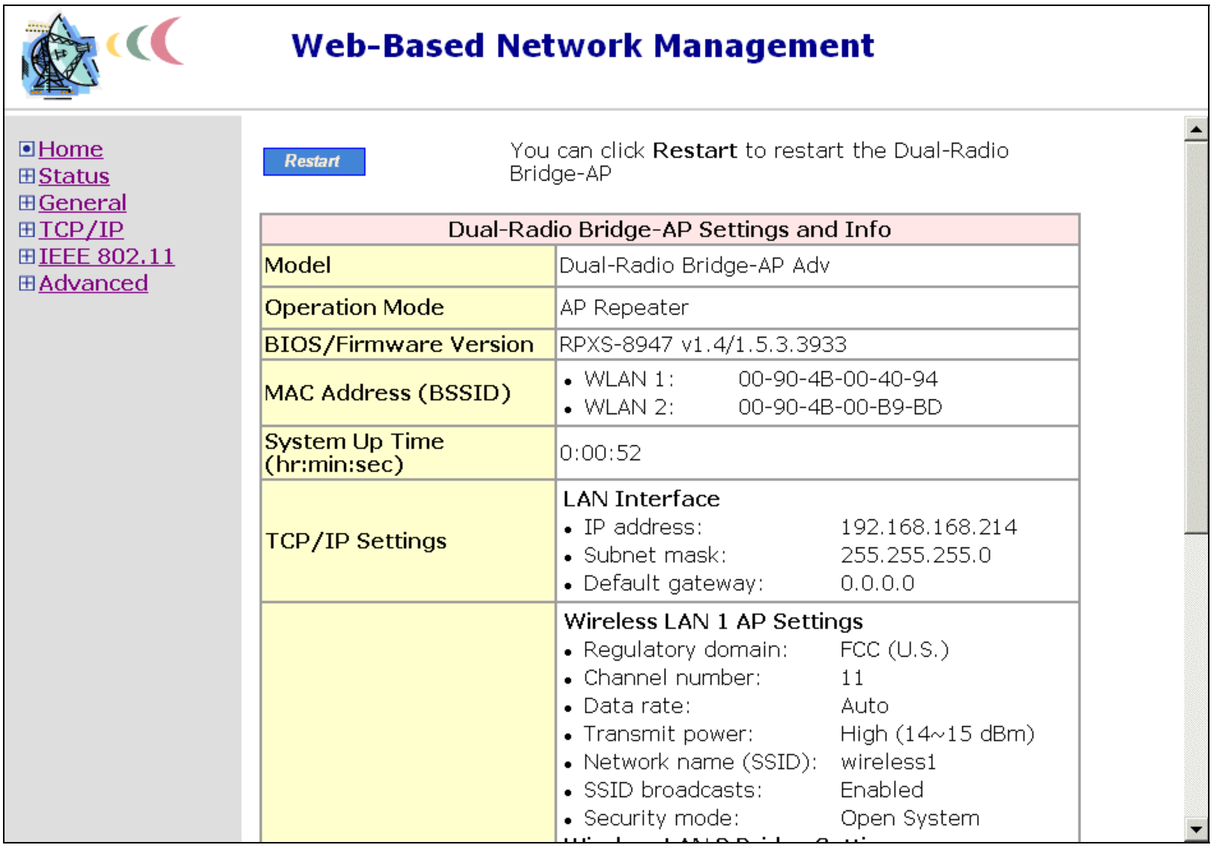
Fig. 17. Antenna alignment assistance.

Instead of using PING.exe, you can run Wireless Network Manager on Computer 1, and go to the **Antenna Alignment** tab. Click **Start** to begin monitoring the WDS link quality. Adjust the alignment of the antenna of DRBAP as Bridge 1 until the **Link quality** indicator shows a *relatively* maximal value. Finally, click **Stop** to stop monitoring WDS link quality.

3. Using Web-Based Network Manager

In this chapter, we'll explain each Web management page of the Web-based Network Manager.

3.1. Overview



You can click **Restart** to restart the Dual-Radio Bridge-AP

Dual-Radio Bridge-AP Settings and Info	
Model	Dual-Radio Bridge-AP Adv
Operation Mode	AP Repeater
BIOS/Firmware Version	RPXS-8947 v1.4/1.5.3.3933
MAC Address (BSSID)	• WLAN 1: 00-90-4B-00-40-94 • WLAN 2: 00-90-4B-00-B9-BD
System Up Time (hr:min:sec)	0:00:52
TCP/IP Settings	LAN Interface • IP address: 192.168.168.214 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
	Wireless LAN 1 AP Settings • Regulatory domain: FCC (U.S.) • Channel number: 11 • Data rate: Auto • Transmit power: High (14~15 dBm) • Network name (SSID): wireless1 • SSID broadcasts: Enabled • Security mode: Open System

Fig. 18. The Start page.

3.1.1. Menu Structure

The left side of the start page contains a menu for you to carry out commands. Here is a brief description of the hyperlinks in the menu:

- **Home.** For going back to the start page.
- **Status.** Status information.
  - **Wireless Clients.** The status of the wireless clients currently associated with the DRBAP.
  - **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.
  - **System Log.** System events log.
- **General.** Global operations.

    - **Password.** For gaining rights to change the settings of the DRBAP.
    - **Firmware Tools.** For upgrading the firmware of the DRBAP, backing up and restoring configuration, and configuration reset settings of the DRBAP.

- **TCP/IP.** TCP/IP-related settings.
    - **Addressing.** IP address settings for the DRBAP to work with TCP/IP.
    - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the DRBAP.
- **IEEE 802.11.** IEEE 802.11g-related settings.
    - **Communications.** Basic settings for the IEEE 802.11g interfaces of the DRBAP.
    - **Security.** Security settings for authenticating wireless users and encrypting wireless data for an AP interface. And security settings for encrypting data transmitted over the WDS links for a LAN-to-LAN bridge interface.
    - **IEEE 802.1x/RADIUS.** IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service) settings for an AP interface.
- **Advanced.** Advanced settings of the DRBAP.
    - **Packet Filters.** Ethernet Type Filters, IP Protocol Filters, and TCP/UDP Port Filters settings.
    - **Management.** UPnP, System Log, and SNMP settings.

3.1.2. Save, Save & Restart, and Cancel Commands

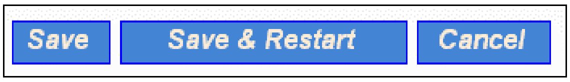
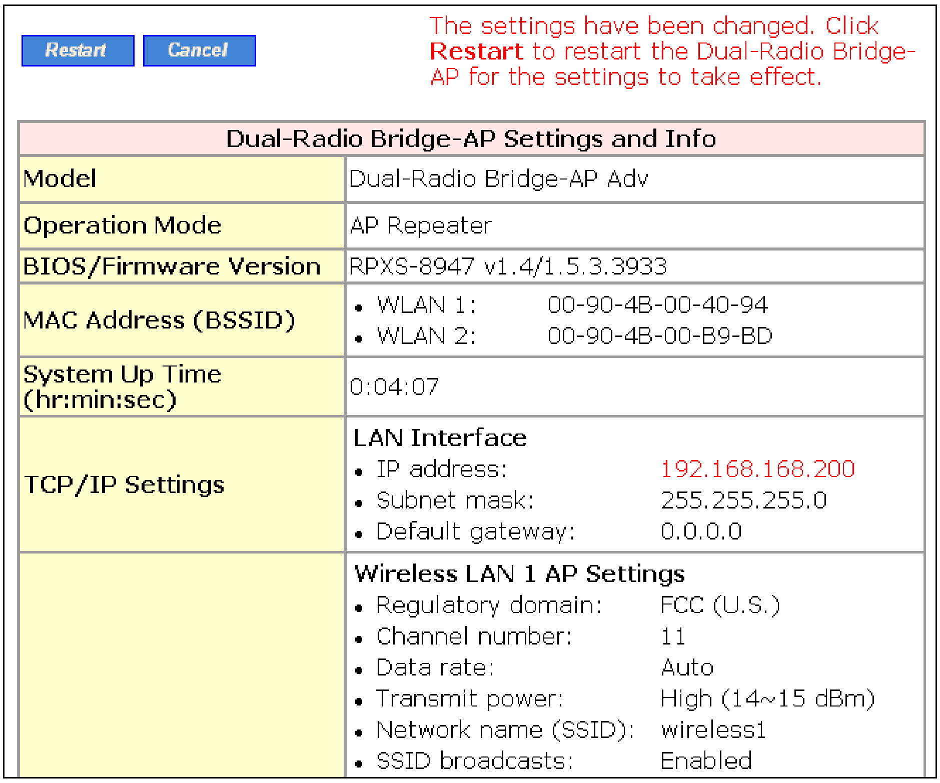


Fig. 19. Save, Save & Restart, and Cancel.

At the bottom of each page that contains settings you can configure, there are up to three buttons—**Save**, **Save & Restart**, and **Cancel**. Clicking **Save** stores the settings changes to the memory of the DRBAP and brings you back to the start page. Clicking **Save & Restart** stores the settings changes to the memory of the DRBAP and restarts the DRBAP immediately for the settings changes to take effect. Clicking **Cancel** discards any settings changes and brings you back to the start page.

If you click **Save**, the start page will reflect the fact that the configuration settings have been changed by showing two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in red. Clicking **Cancel** discards all the changes. Clicking **Restart** restarts the DRBAP for the settings changes to take effect.



The settings have been changed. Click **Restart** to restart the Dual-Radio Bridge-AP for the settings to take effect.

Dual-Radio Bridge-AP Settings and Info	
Model	Dual-Radio Bridge-AP Adv
Operation Mode	AP Repeater
BIOS/Firmware Version	RPXS-8947 v1.4/1.5.3.3933
MAC Address (BSSID)	• WLAN 1: 00-90-4B-00-40-94 • WLAN 2: 00-90-4B-00-B9-BD
System Up Time (hr:min:sec)	0:04:07
TCP/IP Settings	LAN Interface • IP address: 192.168.168.200 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
	Wireless LAN 1 AP Settings • Regulatory domain: FCC (U.S.) • Channel number: 11 • Data rate: Auto • Transmit power: High (14~15 dBm) • Network name (SSID): wireless1 • SSID broadcasts: Enabled

Fig. 20. Settings have been changed.

3.1.3. Home and Refresh Commands

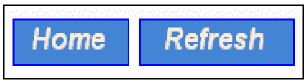
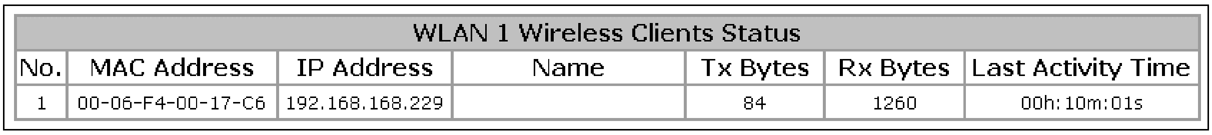


Fig. 21. Home and Refresh.

At the bottom of each status page that shows read-only information, there are two buttons—**Home** and **Refresh**. Clicking **Home** brings you back to the start page. Clicking **Refresh** updates the shown status information.

3.2. Viewing Status

3.2.1. Associated Wireless Clients

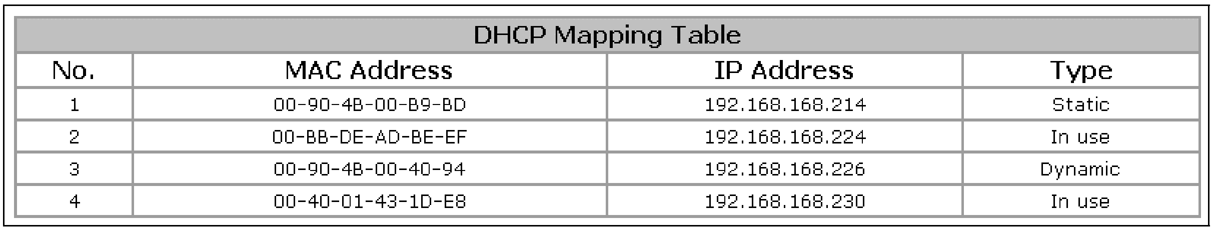


WLAN 1 Wireless Clients Status						
No.	MAC Address	IP Address	Name	Tx Bytes	Rx Bytes	Last Activity Time
1	00-06-F4-00-17-C6	192.168.168.229		84	1260	00h:10m:01s

Fig. 22. Status of associated wireless clients.

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1x authenticated), number of bytes it has send, number of bytes it has received, and the time of its last activity, is shown.

3.2.2. Current DHCP Mappings



DHCP Mapping Table

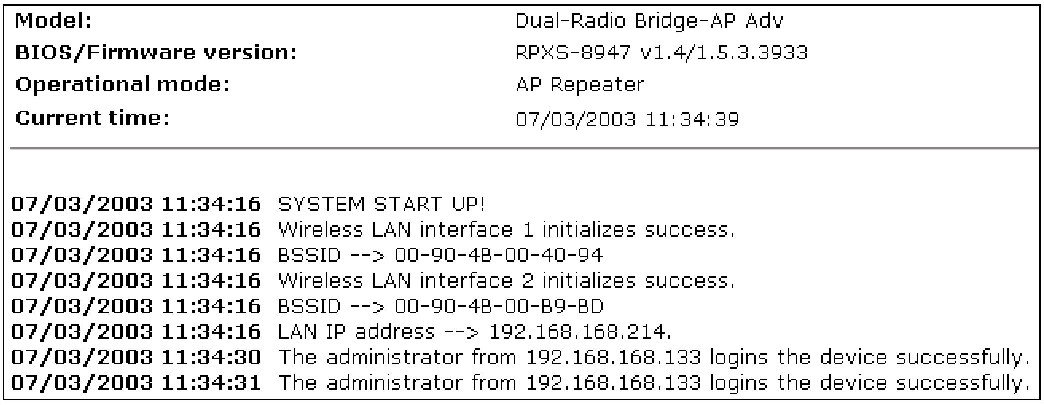
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

Fig. 23. Current DHCP mappings.

On this page, all the current *static* or *dynamic* DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

A static mapping indicates that the DHCP client always obtains the specified IP address from the DHCP server. You can set static DHCP mappings in the **Static DHCP Mappings** section of the **DHCP Server** configuration page (see Section 3.4.2). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool specified by the **First allocateable IP address** and **Allocateable IP address count** settings on the **DHCP Server** configuration page.

3.2.3. System Log



Model:	Dual-Radio Bridge-AP Adv
BIOS/Firmware version:	RPXS-8947 v1.4/1.5.3.3933
Operational mode:	AP Repeater
Current time:	07/03/2003 11:34:39

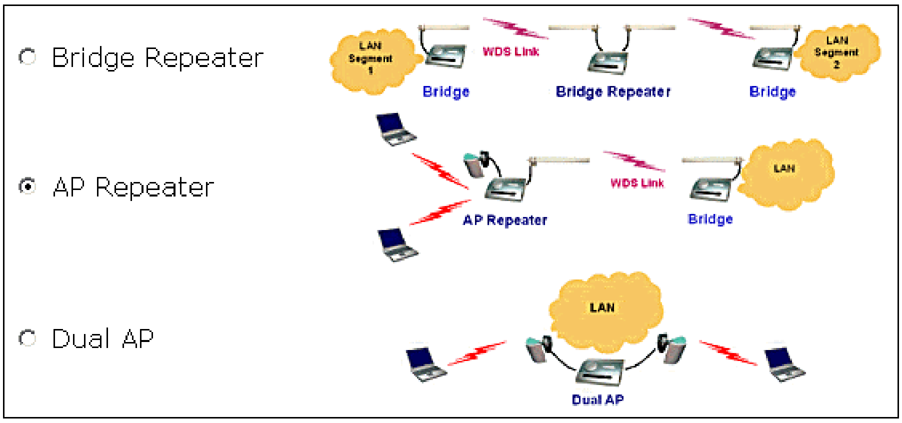
```
07/03/2003 11:34:16  SYSTEM START UP!
07/03/2003 11:34:16  Wireless LAN interface 1 initializes success.
07/03/2003 11:34:16  BSSID --> 00-90-4B-00-40-94
07/03/2003 11:34:16  Wireless LAN interface 2 initializes success.
07/03/2003 11:34:16  BSSID --> 00-90-4B-00-B9-BD
07/03/2003 11:34:16  LAN IP address --> 192.168.168.214.
07/03/2003 11:34:30  The administrator from 192.168.168.133 logins the device successfully.
07/03/2003 11:34:31  The administrator from 192.168.168.133 logins the device successfully.
```

Fig. 24. System log.

System events are recorded in the memory of the AP. The logged information is useful for troubleshooting purposes. The system events are divided into several categories, and you can select which categories of events to log. See Section 3.6.2.2 for more information.

3.3. General Operations

3.3.1. Specifying Operational Mode



○ Bridge Repeater

● AP Repeater

○ Dual AP

Fig. 25. Operational modes.

On this page, you can specify the operational mode for the DRBAP. There are 3 modes:

- **Bridge Repeater**. In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges. It's possible to use multiple bridge repeaters between two LAN-to-LAN bridges if the distance is very long.

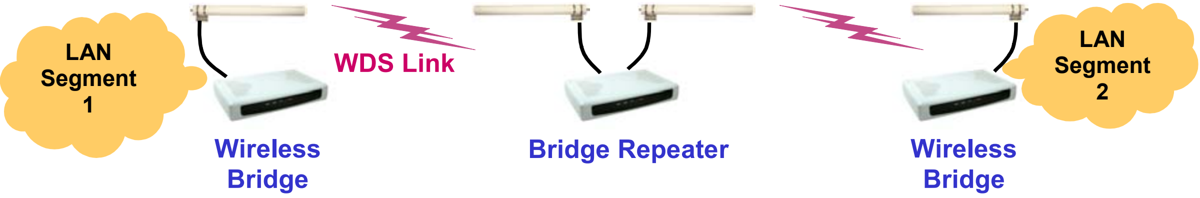


Fig. 26. **Bridge Repeater** mode.

- **AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface. The AP repeater is suitable for situations in which Ethernet wiring between the AP and the network backbone is impossible or costs highly.

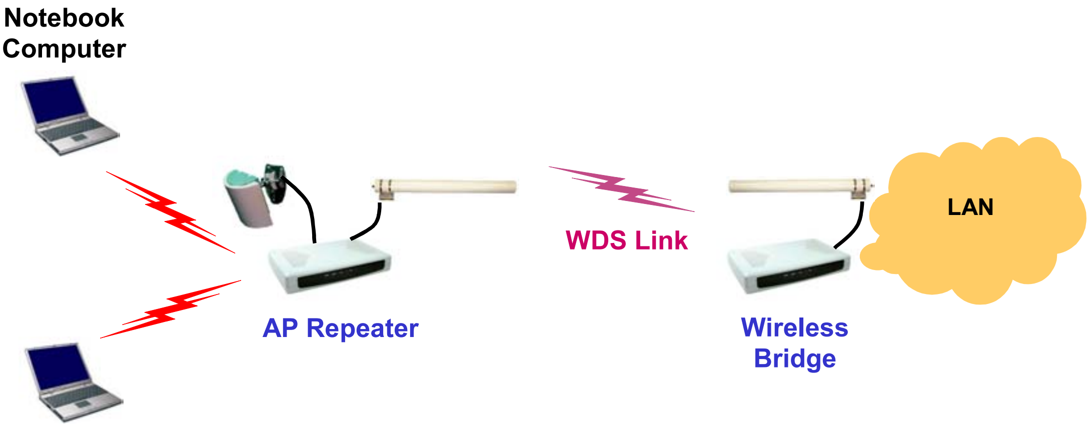


Fig. 27. **AP Repeater** mode.

- **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle *twice* the number of wireless clients than a normal AP. It can be treated as “two APs in a box.”

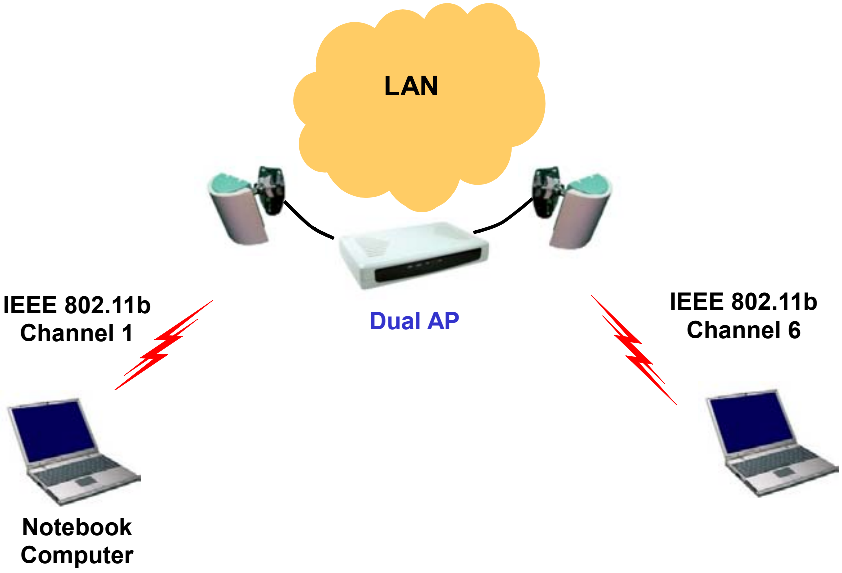
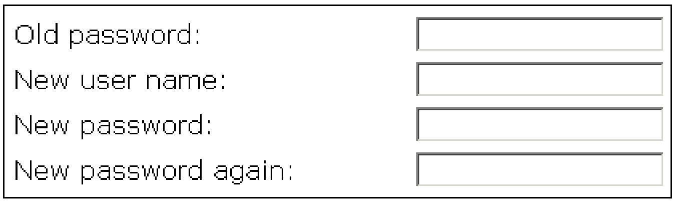


Fig. 28. **Dual AP** mode.

TIP: After you have selected the operational mode of the DRBAP, go to the **IEEE 802.11g, Addressing** section of the management UI (see Section 3.4.2) to configure the IEEE 802.11g settings of the WLAN interfaces.

3.3.2. Changing Password



Old password:	
New user name:	
New password:	
New password again:	

Fig. 29. Password.

On this page, you could change the password for the right to modify the configuration of the DRBAP. The new password must be typed twice for confirmation.

3.3.3. Managing Firmware

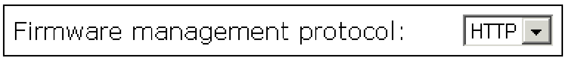

Firmware management protocol: HTTP

Fig. 30. Firmware management protocol setting.

Firmware management operations for the DRBAP include *firmware upgrade*, *configuration backup*, *configuration restore*, and *configuration reset*. Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP. The HTTP-based way is suggested because it's more user friendly. However, due to different behavior of different Web browser types and versions, HTTP-based firmware management operations may not work properly with some Web browsers. If you cannot successfully perform HTTP-based firmware management operations with your Web browser, try the TFTP-based way.

TIP: You can use Upgrade Wizard of Wireless Network Manager to upgrade firmware. See the on-line help of Wireless Network Manager for more information.

3.3.3.1. Upgrading Firmware by HTTP

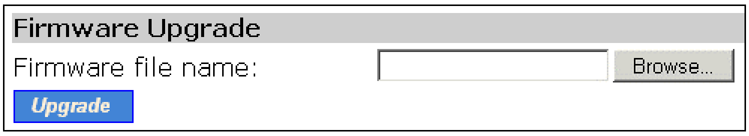


Fig. 31. Firmware upgrade by HTTP.

To upgrade firmware of the DRBAP by HTTP:

1. Click **Browse** and then select a correct firmware **.bin** file. The firmware file path will be shown in the **Firmware file name** text box.

2. Click **Upgrade** to begin the upgrade process.

3.3.3.2. Backing up and Restoring Configuration Settings by HTTP

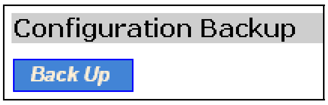


Fig. 32. Firmware backup by HTTP.

To back up configuration of the DRBAP by HTTP:

1. Click **Back Up**.

2. You'll be prompted to open or save the configuration file. Click **Save**.

3. The configuration file is named by the DRBAP's MAC address. For example, if the DRBAP's MAC address is 00-01-02-33-44-55, the configuration backup file should be

"000102334455.hex". Don't change the configuration file name in the **Save As** dialog box. Select a folder in which the configuration file is to be stored. And then, click **Save**.

NOTE: The procedure may be a little different with different Web browsers.

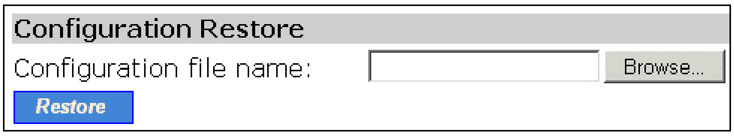


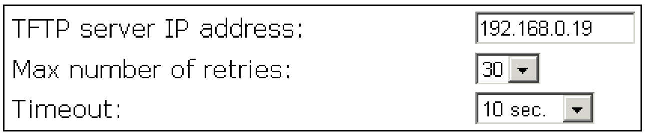
Fig. 33. Configuration restore by HTTP.

To restore configuration of the DRBAP by HTTP:

1. Click **Browse** and then select a correct configuration **.hex** file. You have to make sure the file name is the DRBAP's MAC address. The firmware file path will be shown in the **Firmware file name** text box.

2. Click **Restore** to upload the configuration file to the DRBAP.

3.3.3.3. Upgrading Firmware by TFTP



TFTP server IP address: 192.168.0.19
Max number of retries: 30
Timeout: 10 sec.

Fig. 34. TFTP server settings.

When use TFTP as the firmware management protocol, you can configure settings for the DRBAP's TFTP client to communicate with a TFTP server. If the TFTP client does not get a response from the TFTP server within a period specified by the **Timeout** setting, it will resend the previous request. The **Max number of retries** setting specifies the maximal number of resend before the TFTP client stops communicating with the TFTP server.

Within the folder "**Utilities**" on the companion CD-ROM disk, we offered a TFTP server program (**TftpSrvr.exe**) for firmware upgrade. Run this program on the computer that is to serve as a TFTP server.

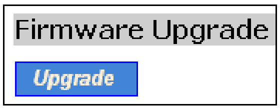


Fig. 35. Firmware upgrade by TFTP.

To upgrade firmware of the DRBAP by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.

2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.

3. Configure IP address of the computer so that the DRBAP and the computer are in the same IP subnet.

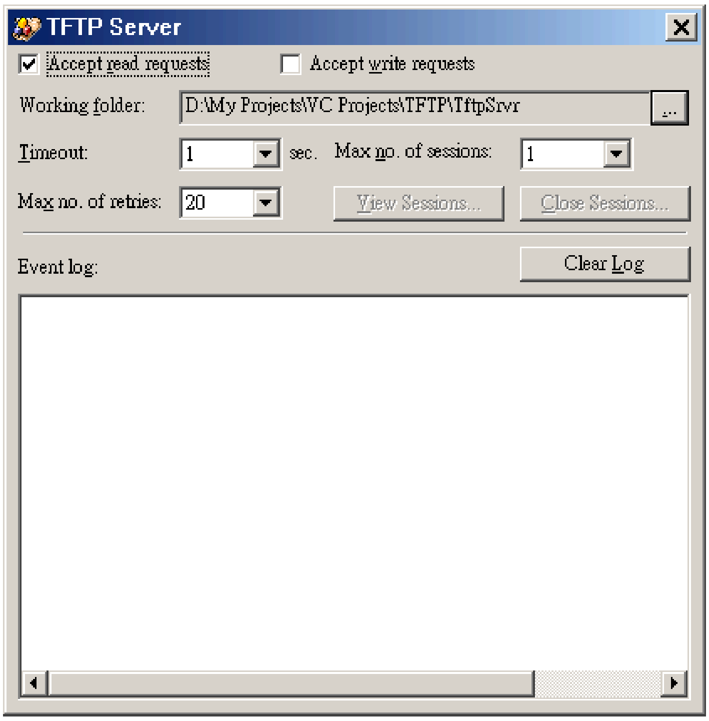
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.

5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6. Choose **TFTP** as the **Firmware management protocol**.

7. Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the firmware upgrade process by clicking **Upgrade**.



TFTP Server

☑ Accept read requests   □ Accept write requests

Working folder: D:\My Projects\VC Projects\TFTP\TftpSrvr

Timeout: 1 sec.   Max no. of sessions: 1

Max no. of retries: 20

Event log:

Fig. 36. TFTP Server.

NOTE: After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.

NOTE: Make sure the **Accept read requests** check box of TFTP Server is selected.

NOTE: The LAN IP address of the DRBAP and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless DRBAP be connected by Ethernet, and on the same LAN, so that the upgrade process would be smooth.

NOTE: After the firmware is upgraded, be sure to delete the contents of the Web browser cache, so that the Web management pages can be shown correctly.

NOTE: A failed upgrade may corrupt the firmware and make the DRBAP unstartable. When this occurs, call for technical support.

TIP: If you want to remotely upgrade the firmware of a deployed DRBAP from the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP upgrade to succeed.

3.3.3.4. Backing up and Restoring Configuration Settings by TFTP

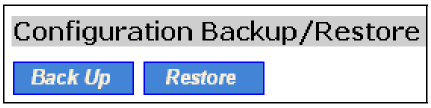


Fig. 37. Configuration backup/restore.

To back up configuration of the DRBAP by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the backup process.

2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.

3. Configure the IP address of the computer so that the computer and the DRBAP are in the same IP subnet.

4. On the computer, run the TFTP Server utility. Select the **Accept write requests** check box, and specify the folder to which the configuration settings of the DRBAP will be saved.

5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6. Choose **TFTP** as the **Firmware management protocol**.

7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the backup process by clicking **Back Up**. The DRBAP's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "AaBbCcDdEeFf" is the DRBAP's MAC address. For example, if the DRBAP's MAC address is 00-01-02-33-44-55, the configuration backup file will be "000102334455.hex".

NOTE: Remember to select the **Accept write requests** check box of TFTP Server.

To restore configuration of the DRBAP by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the restoring process.

2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.

3. Configure the IP address of the computer so that the computer and the DRBAP are in the same IP subnet.

4. On the computer, run the TFTP Server utility. And specify the folder in which the configuration backup file resides. A configuration backup file is named by the DRBAP's MAC address. For example, if the DRBAP's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".

5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6. Choose **TFTP** as the **Firmware management protocol**.

7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the restoring process by clicking **Restore**. The DRBAP will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the DRBAP.

TIP: If you want to remotely back up or restore configuration from the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

3.3.3.5. Resetting Configuration to Factory Defaults

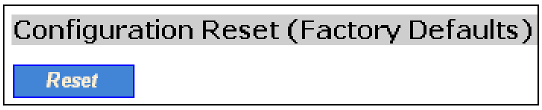

Configuration Reset (Factory Defaults)

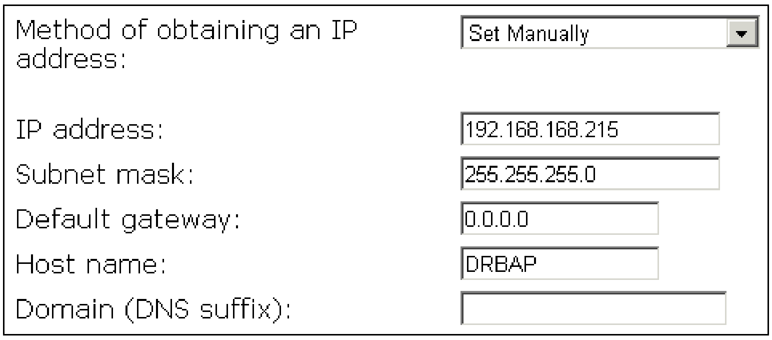
Fig. 38. Configuration reset.

Clicking the **Reset** button resets the device configuration to factory defaults.

WARNING: Think twice before clicking the **Reset** button. You'll lose all your current configuration settings.

3.4. Configuring TCP/IP Related Settings

3.4.1. Addressing


Method of obtaining an IP address: Set Manually

IP address: 192.168.168.215

Subnet mask: 255.255.255.0

Default gateway: 0.0.0.0

Host name: DRBAP

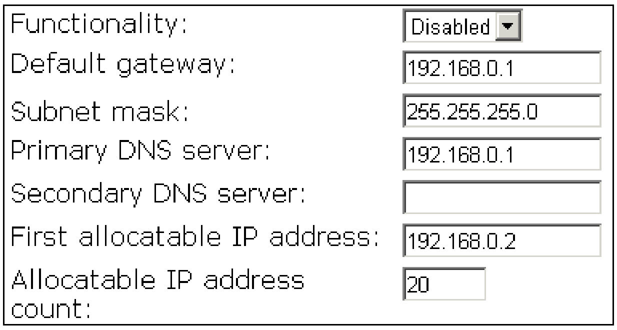
Domain (DNS suffix):

Fig. 39. TCP/IP settings.

The IP address of the DRBAP can be manually set (**Set Manually**) or automatically assigned by a DHCP server on the LAN (**Obtain from a DHCP Server**). If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain** (DNS suffix) of the DRBAP.

3.4.2. DHCP Server

3.4.2.1. Basic



Functionality:	Disabled ▾
Default gateway:	192.168.0.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.0.1
Secondary DNS server:	
First allocatable IP address:	192.168.0.2
Allocatable IP address count:	20

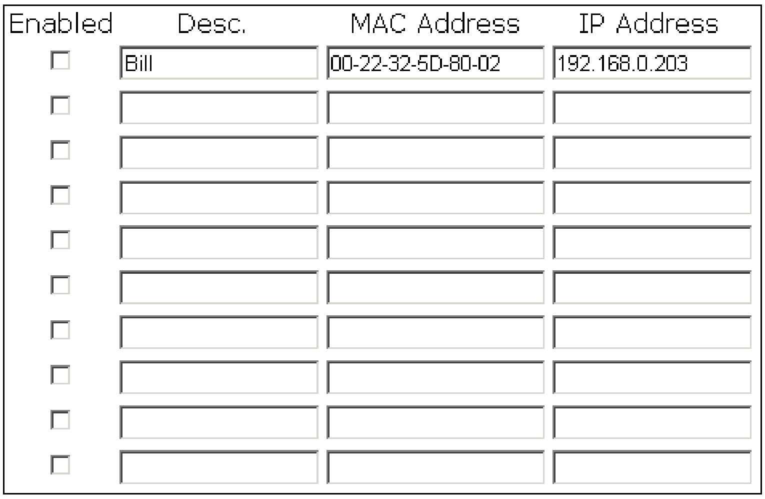
Fig. 40. Basic DHCP server settings.

The DRBAP can automatically assign IP addresses to client computers by DHCP. In this section of the management page, you can specify the **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings that will be sent to a client at its request. Additionally, you can specify the first IP address that will be assigned to the clients and the number of allocateable IP addresses.

NOTE: There should be only *one* DHCP server on the LAN; otherwise, DHCP would not work properly. If there is already a DHCP server on the LAN, disable the DHCP server functionality of the DRBAP.

NOTE: By default the DHCP server function is disabled.

3.4.2.2. Static DHCP Mappings



Enabled	Desc.	MAC Address	IP Address
☐	Bill	00-22-32-5D-80-02	192.168.0.203
☐			
☐			
☐			
☐			
☐			
☐			
☐			
☐			
☐			

Fig. 41. Static DHCP mappings.

IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. By **Static DHCP Mappings**, you can ensure that a host will get the same IP address when it requests one from the DHCP server. Therefore, instead of configuring the IP address of an intranet server manually, you can configure the server to obtain an IP address by DHCP and it is always assigned the same IP address.

To always assign a static IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. Then, give a description for this mapping.

2. Select the corresponding **Enabled** check box.

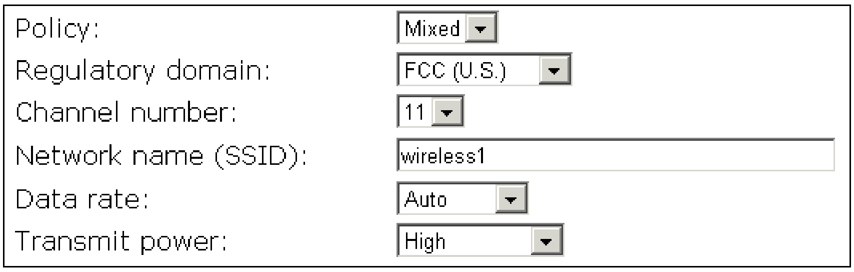
3.5. Configuring IEEE 802.11g-Related Settings

3.5.1. Communication

An AP interface needs the Basic communication settings, and a LAN-to-LAN bridge interface needs the Basic communication settings and the Bridge Links settings.

3.5.1.1. Basic

Basic IEEE 802.11g-related communication settings include **Policy** (RF type), **Regulatory domain**, **Channel number**, **Network name (SSID)**, **Data rate**, and **Transmit power**.



Policy:	Mixed
Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	wireless1
Data rate:	Auto
Transmit power:	High

Fig. 42. Basic IEEE 802.11g communication settings.

The RF type (**Policy**) of the WLAN interface can be configured to work in IEEE 802.11b only (**b Only**), IEEE 802.11g only (**g Only**), or mixed mode (**Mixed**—802.11g and 802.11b simultaneously).

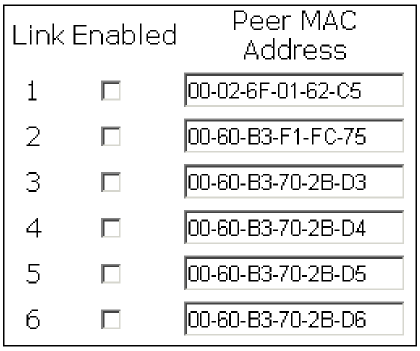
The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. **For two wireless devices to communicate with each other, they must be set to identical SSID (Service Set IDentifier).**

If there is RF interference, you may want to reduce the **Data rate** for more reliable wireless transmission. In most cases, leave the setting to **Auto**.

The transmit power of the RF module of the DRBAP can be adjusted so that the RF coverage of the DRBAP can be changed.

3.5.1.2. Bridge Links

A bridge link is an IEEE 802.11 WDS (Wireless Distribution System) link. A LAN-to-LAN bridge interface is equipped with *6* WDS links so it can be connected to at most 6 other wireless bridges.



Link	Enabled	Peer MAC Address
1	□	00-02-6F-01-62-C5
2	□	00-60-B3-F1-FC-75
3	□	00-60-B3-70-2B-D3
4	□	00-60-B3-70-2B-D4
5	□	00-60-B3-70-2B-D5
6	□	00-60-B3-70-2B-D6

Fig. 43. Bridge links settings.

To enable a WDS link:

1. Specify the MAC address of the bridge at the other end of the WDS link.

2. Select the corresponding **Enabled** check box.

For example, assume you want a DRBAP with MAC addresses 00-02-65-01-62-C5 and a wireless bridge/AP with MAC address 00-02-65-01-62-C6 to establish a WDS link between them. On DRBAP 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on wireless bridge 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

TIP: Plan your wireless network and draw a diagram, so that you know how a DRBAP is connected to other peer bridges and can therefore set the bridge links settings correctly.

WARNING: Don't let your network topology consisting of wireless DRBAPs, wireless bridges, Ethernet switches, Ethernet links, and WDS links contains *loops*. If any loops exist, packets will circle around the loops and network performance will be seriously degraded.

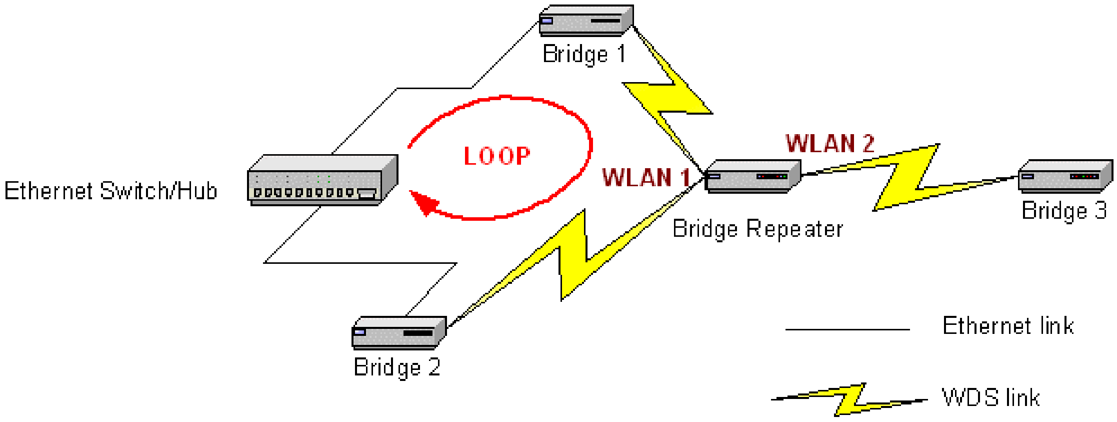
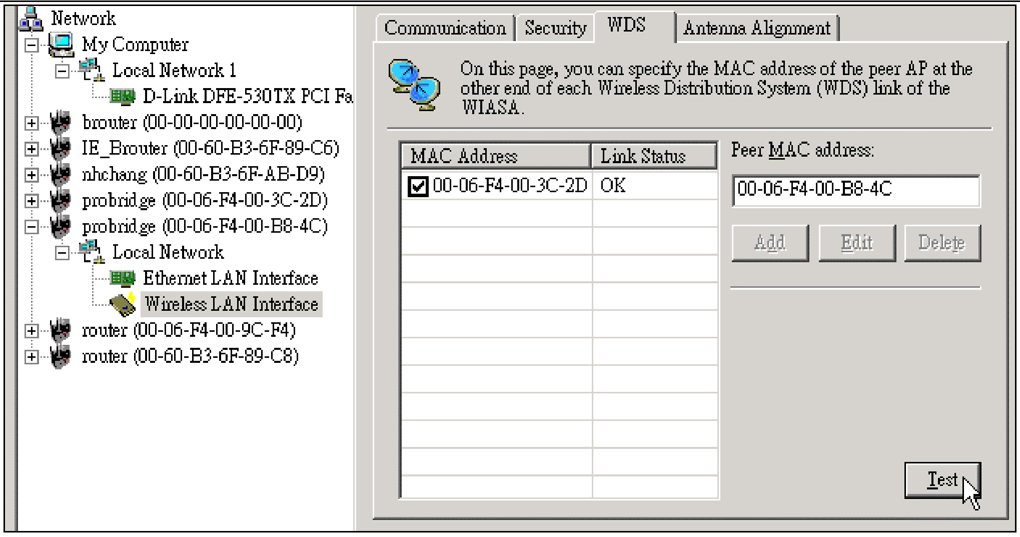


Fig. 44. Network topology containing a loop.

TIP: You can check whether the WDS links of the DRBAP are functioning by using Wireless Network Manager.


Network
My Computer
Local Network 1
D-Link DFE-530TX PCI Fa
brouter (00-00-00-00-00-00)
IE_Brouter (00-60-B3-6F-89-C6)
nhchang (00-60-B3-6F-AB-D9)
probridge (00-06-F4-00-3C-2D)
probridge (00-06-F4-00-B8-4C)
Local Network
Ethernet LAN Interface
Wireless LAN Interface
router (00-06-F4-00-9C-F4)
router (00-60-B3-6F-89-C8)
Communication
Security
WDS
Antenna Alignment
Add
Edit
Delete
Test

On this page, you can specify the MAC address of the peer AP at the other end of each Wireless Distribution System (WDS) link of the WIASA.

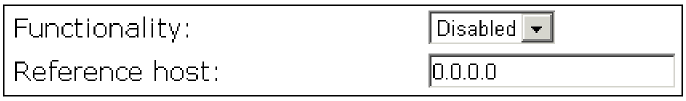
MAC Address	Link Status
☑ 00-06-F4-00-3C-2D	OK

Peer MAC address: 00-06-F4-00-B8-4C

Fig. 45. Link health monitoring.

Run Wireless Network Manager on a computer and locate the bridge you want to manage. Go to the WDS tab, and then click **Test**. The test results (*OK* or *Broken*) will be shown in the **Link Status** column of the WDS links table.

3.5.1.3. Link Integrity



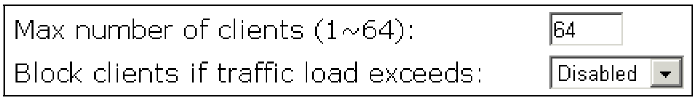
Functionality: Disabled

Reference host: 0.0.0.0

Fig. 46. Link integrity settings.

When the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the AP interface(s) of the DRBAP and no wireless client can associate with the AP interface(s). The detection mechanism is based on pinging the IP address specified in **Reference host**.

3.5.1.4. Association Control



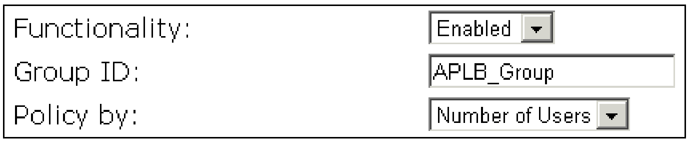
Max number of clients (1~64): 64

Block clients if traffic load exceeds: Disabled

Fig. 47. Association control settings.

If the number of currently associated wireless clients exceeds the value specified in the **Max number of clients** setting, no more wireless client can associate with the AP interface(s). If traffic load of the AP interface(s) exceeds the load specified in the **Block clients if traffic load exceeds** setting, no more wireless client can associate with the AP interface(s).

3.5.1.5. AP Load Balancing



Functionality: Enabled

Group ID: APLB_Group

Policy by: Number of Users

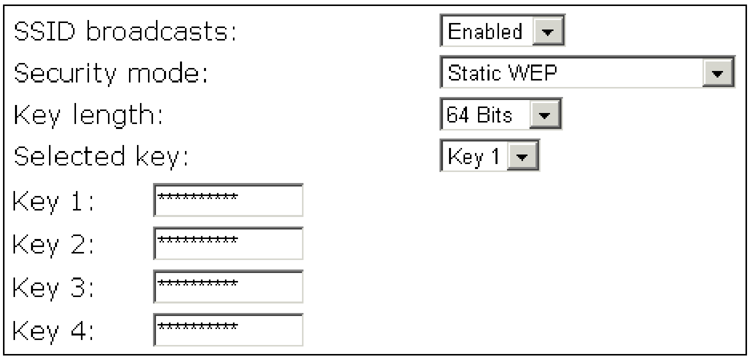
Fig. 48. AP load balancing settings.

Several APs can form a load-balancing group if they are set with the same **Group ID**. The load-balancing policy can be by **Number of Users** or by **Traffic Load**.

If the *by-number-of-users* policy is selected, a new wireless user can only associate with an AP that has the smallest number of associated wireless users in the group. On the other hand, if the *by-traffic-load policy* is selected, a new wireless user can only associate with an AP that has the less traffic load in the group.

3.5.2. Security

3.5.2.1. AP Interface



SSID broadcasts: Enabled

Security mode: Static WEP

Key length: 64 Bits

Selected key: Key 1

Key 1: ***********

Key 2: ***********

Key 3: ***********

Key 4: ***********

Fig. 49. IEEE 802.11g security settings for an AP interface.

IEEE 802.11g security settings for an AP interface include **SSID broadcasts**, **Security mode**, **WEP keys**, **MAC-Address-Based Access Control**.

NOTE: If the DRBAP is set to be in **Dual AP** mode, the two AP interfaces share the same IEEE 802.11g security settings.

For security reasons, it's highly recommended that the security mode be set to options other than *Open System*. When the security mode is set to Open System, no authentication and data encryption will be performed. Additionally, you can *disable* the SSID broadcasts functionality so that a wireless client computer with an "any" SSID cannot associate with the AP.

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients of this DRBAP as an AP cannot see each other, and wireless-to-wireless traffic is blocked. When the setting is set to **All APs in This Subnet**, traffic among wireless users of different APs in the same IP subnet is blocked. This feature is useful for WLANs deployed in public places. In this way, hackers have no chance to attack other wireless users in a *hotspot*.

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients (STAs) of this

DRBAP as an AP cannot see each other, and wireless-to-wireless traffic between the STAs is blocked. When the setting is set to **All APs in This Subnet**, traffic among wireless users of different APs in the same IP subnet is blocked. The behaviors are illustrated in the following figures.

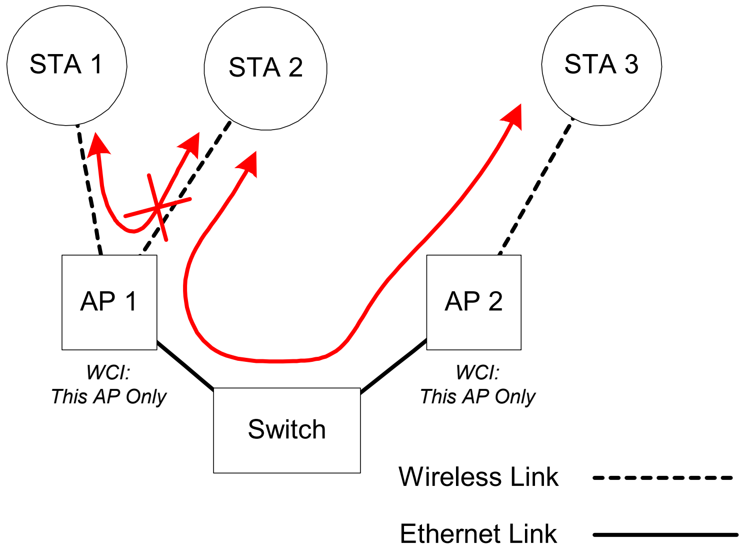


Fig. 50. Behavior of the "This AP Only" wireless client isolation option.

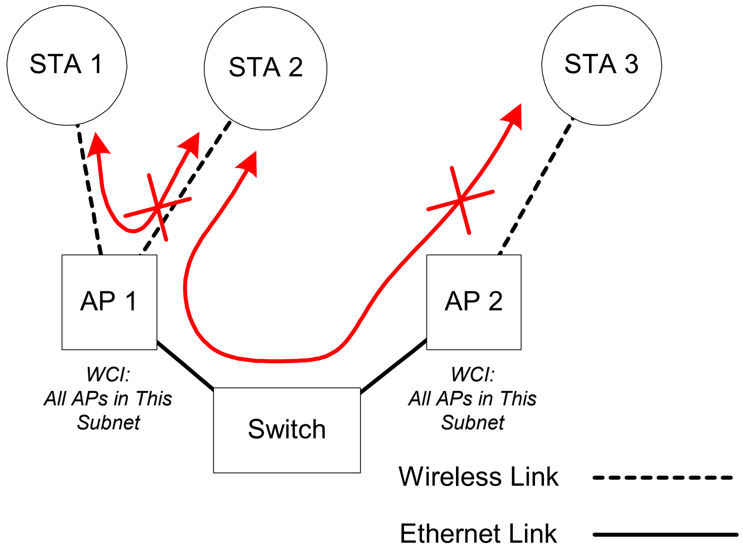


Fig. 51. Behavior of the "All APs on This Subnet" wireless client isolation option.

As illustrated in Fig. 50 when AP 1 and AP 2 are using the "This AP Only" option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, while wireless traffic between STA 2 and STA 3, which are associated with different APs, is still allowed. If the "All APs in This Subnet" option is used as shown in Fig. 51, AP 1 and AP 2 communicates with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

There are up to 7 security modes depending on AP model variations:

- **Open System.** No authentication, no data encryption.

- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.

- **Static TKIP (WPA-PSK).** Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you have to specify the **Pre-shared key**, which will be used by the TKIP engine as a *master key* to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

> **NOTE:** The number of characters of the **Pre-shared key** setting must be at least 8 and can be up to 63.

- **IEEE 802.1x EAP without Encryption (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. No data encryption.

- **IEEE 802.1x EAP with Static WEP (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. Data encryption is achieved by static WEP.

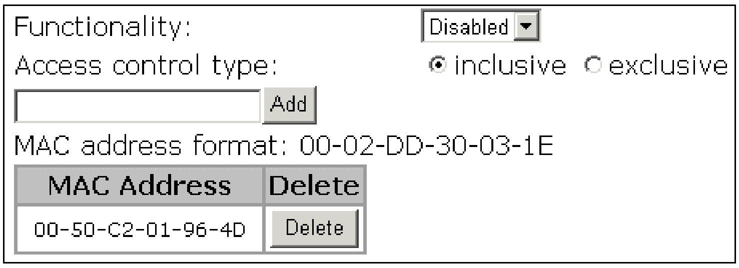
- **IEEE 802.1x EAP with Dynamic WEP (EAP-TLS, EAP-TTLS, PEAP).** The IEEE 802.1x functionality is enabled and dynamic WEP key distribution authentication (EAP-TLS, EAP-TTLS, or PEAP) is used. Data encryption is achieved by dynamic WEP.

- **IEEE 802.1x EAP with Dynamic TKIP (WPA).** This is a full WPA mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The AP is highly secured in this mode.

In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1x functionality is enabled. See Section 3.5.3 for more information about IEEE 802.1x and RADIUS.

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

> **NOTE:** Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".



Functionality: Disabled ▾

Access control type: ● inclusive ○ exclusive

MAC address format: 00-02-DD-30-03-1E

MAC Address	Delete
00-50-C2-01-96-4D	Delete

Fig. 52. MAC-address-based access control settings for an AP interface.

With **MAC-Address-Based Access Control**, you can specify the wireless client computers that are permitted or not permitted to connect to the AP interface. When the table type is set to **inclusive**, entries in the table are permitted to connect to the AP interface. When the table type is set to **exclusive**, entries in the table are not permitted to connect to the AP interface.

To *deny* wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.

2. Set the **Access control type** to *exclusive*.

3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Steps 3 for other wireless clients.

To *grant* wireless clients’ access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.

2. Set the **Access control type** to *inclusive*.

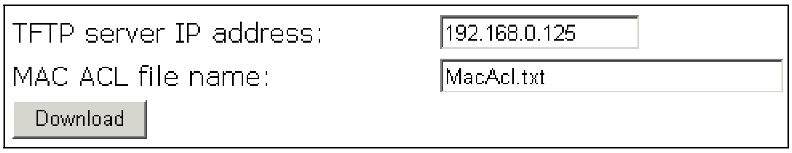
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Steps 3 for other wireless clients.

To delete an entry in access control table:

- Click **Delete** next to the entry.

NOTE: The size of the access control table is 64.

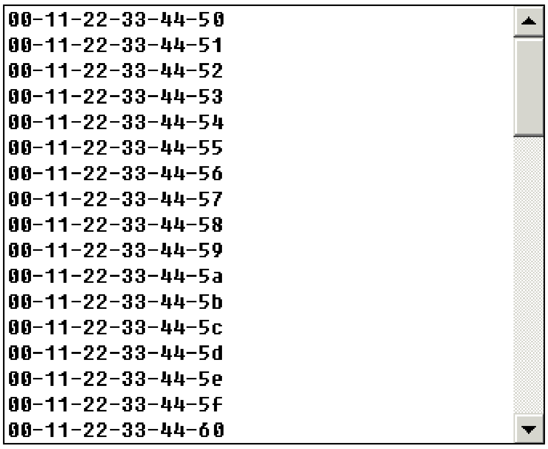


TFTP server IP address: 192.168.0.125

MAC ACL file name: MacAcl.txt

Fig. 53. MAC ACL download settings.

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then command the AP to download the MAC ACL (Access Control List) file from the TFTP server. Fig. 54 shows the contents of a sample ACL file.



```
00-11-22-33-44-50
00-11-22-33-44-51
00-11-22-33-44-52
00-11-22-33-44-53
00-11-22-33-44-54
00-11-22-33-44-55
00-11-22-33-44-56
00-11-22-33-44-57
00-11-22-33-44-58
00-11-22-33-44-59
00-11-22-33-44-5a
00-11-22-33-44-5b
00-11-22-33-44-5c
00-11-22-33-44-5d
00-11-22-33-44-5e
00-11-22-33-44-5f
00-11-22-33-44-60
```

Fig. 54. Sample MAC ACL file.

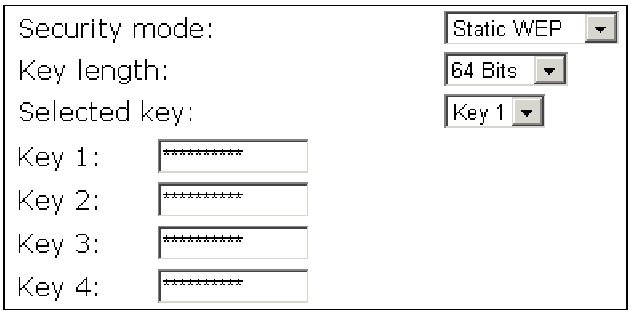
To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.

2. Specify the name of the MAC ACL file on the TFTP server in the **MAC ACL file name** text box.

3. Click **Download**.

3.5.2.2. LAN-to-LAN Bridge Interface



Security mode: Static WEP

Key length: 64 Bits

Selected key: Key 1

Key 1: **********

Key 2: **********

Key 3: **********

Key 4: **********

Fig. 55. IEEE 802.11g security settings for a LAN-to-LAN bridge interface.

Data transmitted over the bridge links can be encrypted by WEP (Wired Equivalent Privacy). Therefore, there are 3 security modes:

- **Open System.** No data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.

When Static WEP is chosen as the security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting outgoing WDS traffic. All 4 WEP keys are used as *receive-keys* to decrypt incoming WDS traffic.

NOTE: Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".

3.5.3. IEEE 802.1x/RADIUS

IEEE 802.1x *Port-Based Network Access Control* is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before granted access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her *user name* and *password* or *digital certificate* to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the advanced wireless access point is controlled by the *security mode* (see Section 3.5.2.1). So far, the wireless access point supports two authentication mechanisms—EAP-MD5 (Message Digest version 5) and EAP-TLS (Transport Layer Security). If EAP-MD5 is used, the user has to give his or her *user name* and *password* for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's *digital certificate* that is stored in the computer hard disk or a smart card for authentication. And after a successful EAP-TLS authentication, a session key is automatically generated for wireless packets encryption between the wireless client computer and its associated wireless access point. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

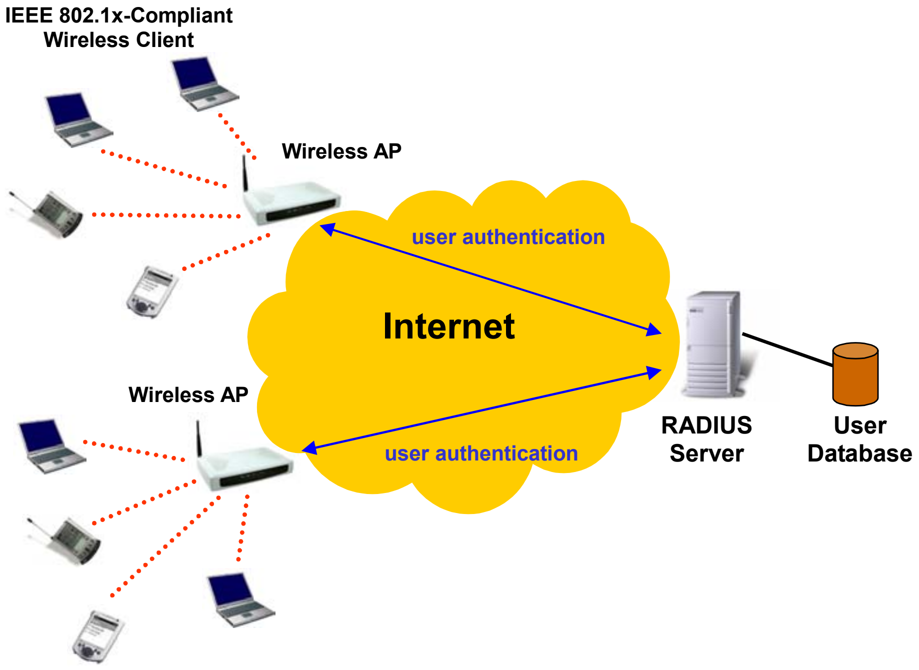
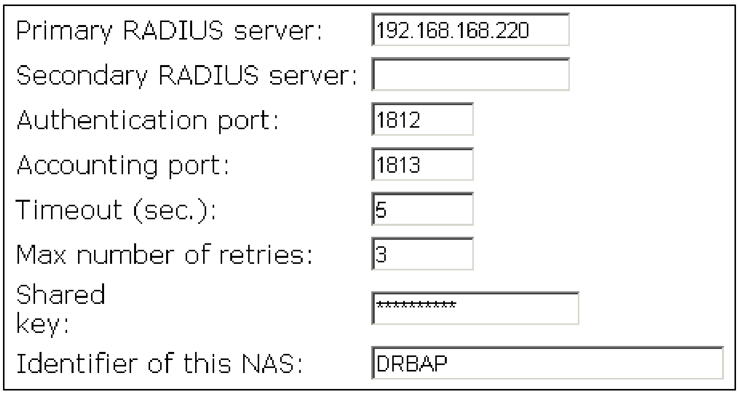


Fig. 56. IEEE 802.1x and RADIUS.

A wireless access point supporting IEEE 802.1x can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the wireless access point will try to communicate with the secondary RADIUS server. The administrator can specify the length of timeout and the number of retries before communicating with the *secondary* RADIUS server after failing to communicate with the primary RADIUS server.

An IEEE 802.1x-capable wireless access point and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, a wireless access point can identify itself by an NAS (Network Access Server) identifier. Each IEEE 802.1x-capable wireless access point must have a *unique* NAS identifier.



Primary RADIUS server:	192.168.168.220
Secondary RADIUS server:	
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared key:	***********
Identifier of this NAS:	DRBAP

Fig. 57. IEEE 802.1x/RADIUS settings.

NOTE: This feature is only available for AP interfaces. If the DRBAP is set to be in **Bridge Repeater** mode, the **IEEE 802.11, IEEE 802.1x/RADIUS** section of the management UI will be hidden from accessing.

TIP: Refer to the IEEE 802.1x-related white papers on the accompanying CD-ROM for more information about deploying secure WLANs with IEEE 802.1x support.

3.6. Configuring Advanced Settings

3.6.1. Packet Filters

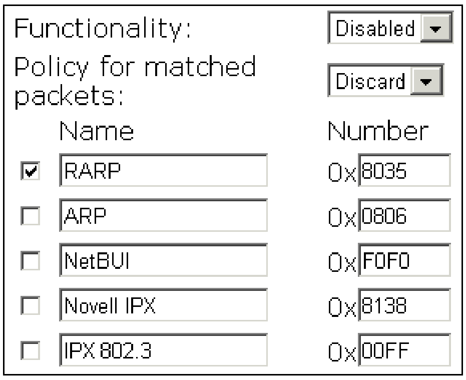
The DRBAP provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

Functionality: whether this filtering capability is *enabled* or *disabled*.

Policy for matched packets: how a matched packet is processed—*discard* or *pass*.

To enable a filtering rule: select the check box to the left of the rule.

3.6.1.1. Ethernet Type Filters



Functionality: Disabled

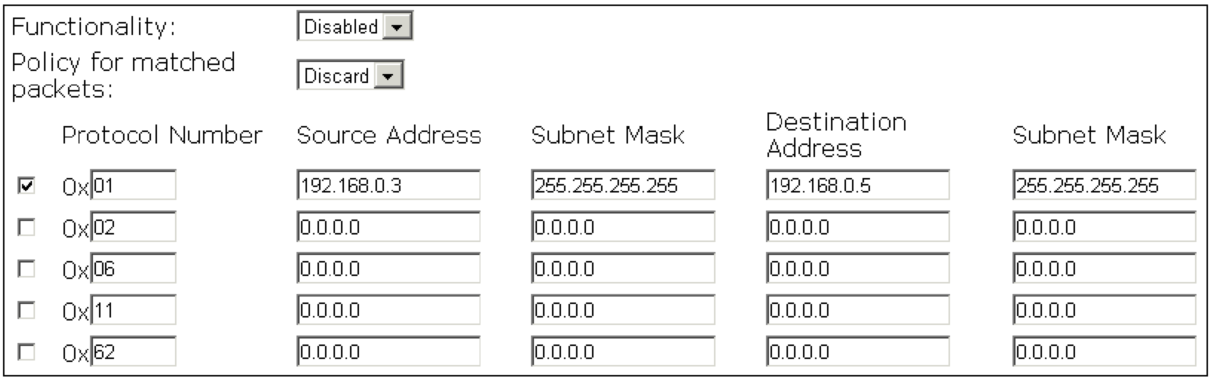
Policy for matched packets: Discard

	Name	Number
☑	RARP	0x8035
□	ARP	0x0806
□	NetBUI	0xF0F0
□	Novell IPX	0x8138
□	IPX 802.3	0x00FF

Fig. 58. Ethernet type filters settings.

The *Ethernet type* filed of the MAC (Media Access Control) header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal Ethernet type number and give the rule a name.

3.6.1.2. IP Protocol Filters



Functionality: Disabled

Policy for matched packets: Discard

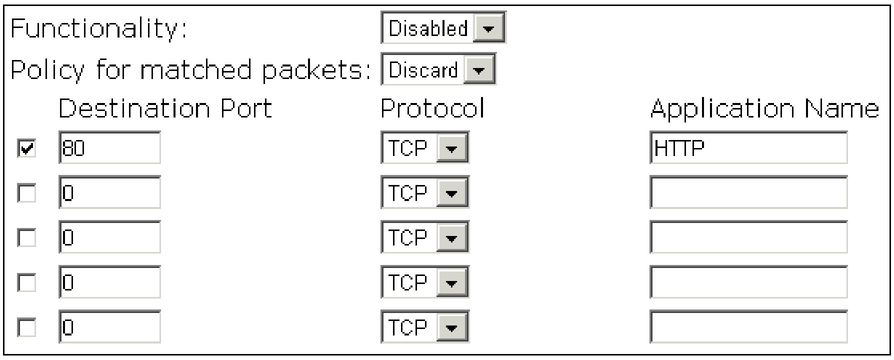
	Protocol Number	Source Address	Subnet Mask	Destination Address	Subnet Mask
☑	0x01	192.168.0.3	255.255.255.255	192.168.0.5	255.255.255.255
□	0x02	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
□	0x06	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
□	0x11	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
□	0x62	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Fig. 59. IP protocol filters settings.

The protocol, source address, and destination address fields of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal protocol number, source IP address range (Source IP Address AND Source Subnet Mask), and destination IP address range (Destination IP Address AND Destination Subnet Mask).

A source (destination) IP address range is determined by performing an AND operation on the source (destination) IP address field and the source (destination) subnet mask field. For example, if the source IP address field is 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

3.6.1.3. TCP/UDP Port Filters



Functionality: Disabled

Policy for matched packets: Discard

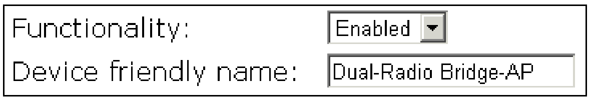
	Destination Port	Protocol	Application Name
☑	80	TCP	HTTP
□	0	TCP	
□	0	TCP	
□	0	TCP	
□	0	TCP	

Fig. 60. TCP/UDP port filters settings.

The *destination port* field the TCP or UDP header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the decimal **Destination Port**, **Protocol** type (TCP/UDP), and the name of the higher-level protocol (**Application Name**).

3.6.2. Management

3.6.2.1. UPnP



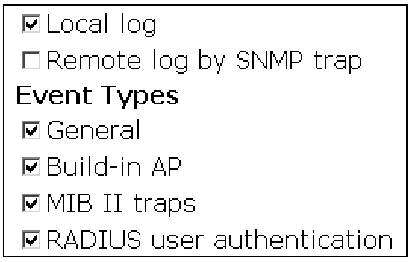
Functionality: Enabled

Device friendly name: Dual-Radio Bridge-AP

Fig. 61. UPnP settings.

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices by HTTP. When the UPnP functionality is enabled, you can see the DRBAP in My Network Places of Windows XP. The DRBAP can be given a *friend name* that will be shown in My Network Places. *Double-clicking* the icon in My Network Places that stands for the DRBAP will launch the default Web browser for you to configure the DRBAP.

3.6.2.2. System Log



☑ Local log

□ Remote log by SNMP trap

Event Types

☑ General

☑ Build-in AP

☑ MIB II traps

☑ RADIUS user authentication

Fig. 62. System log settings.

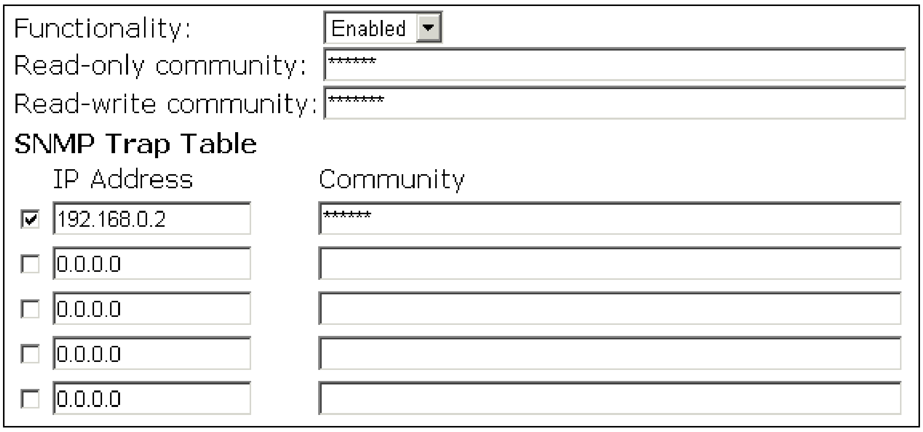
System events can be logged to the on-board RAM of the DRBAP (**Local log**) or sent to a remote computer on which an SNMP trap monitor program runs (**Remote log by SNMP trap**). See the next subsection for more information about SNMP trap settings.

The system events are divided into the following categories:

- **General**: system and network connectivity status changes.
- **Built-in AP**: wireless client association and WEP authentication status changes.
- **MIB II traps**: *Cold Start*, *Warm Start*, *Link Up*, *Link Down* and *SNMP Authentication Failure*.
- **RADIUS user authentication**: RADIUS user authentication status changes.

NOTE: The *SNMP Authentication Failure* trap is issued when using an incorrect community string to manage the DRBAP via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (*disabled* by default).

3.6.2.3. SNMP



Functionality:	Enabled
Read-only community:	******
Read-write community:	*******

SNMP Trap Table

	IP Address	Community
☑	192.168.0.2	******
□	0.0.0.0	
□	0.0.0.0	
□	0.0.0.0	
□	0.0.0.0	

Fig. 63. SNMP settings.

The SNMP (Simple Network Management Protocol) functionality can be disabled, and you can specify the name (used as a *password*) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the **SNMP Trap Table**.

To specify a trap target:

1. Type the IP address of the target host.

2. Type the **Community** for the host.

3. Select the corresponding check box next to the IP address text box.

Appendix A: Default Settings

TIP: Press the **SF-Reset** switch on the housing of a *powered-on* DRBAP to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
Operational Mode	AP Repeater
IEEE 802.11g	
Regulatory Domain	FCC (U.S.)
Channel Number for WLAN 1	11
Channel Number for WLAN 2	6
SSID for WLAN 1	wireless1
SSID for WLAN 2	wireless2
Transmission Rate for WLAN 1	Auto
Transmission Rate for WLAN 2	11Mbps
MAC Address of WLAN 1 and of WLAN 2	See the label on the housing of the DRBAP.
WDS Links	None
Security Mode	Open System
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management	
UPnP	Enabled
System Log	Local Log
SNMP	Enabled
SNMP read community	public
SNMP write community	private

Appendix B: Troubleshooting

- **Check the following first:**

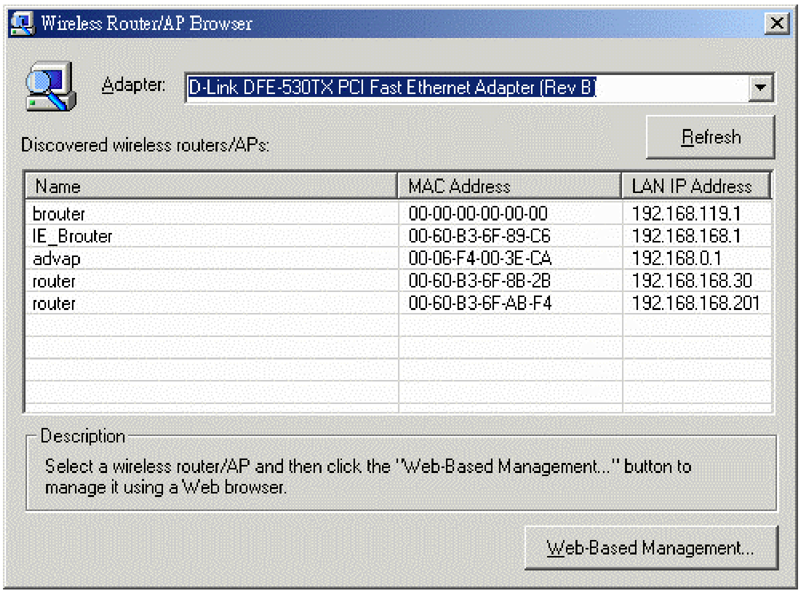
  - Make sure that the power of the DRBAP is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the DRBAP.

  - Make sure that the LED ALV of the DRBAP is blinking to indicate the DRBAP is working.

  - Make sure the types of the Ethernet cables are correct. Recall that there are two types—*normal* and *crossover*.

- **The DRBAP has been set to obtain an IP address automatically by DHCP. How can I know its acquired IP address so that I can manage it using a Web browser?**

  - Use the utility, Wireless Router/AP Browser (**WLBrwsr.exe**), in the "**Utilities**" folder on the companion CD-ROM disc. This utility can discover nearby DRBAPs and show their MAC addresses and IP addresses. In addition, it can launch the default Web browser on your computer.



Adapter: D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev B)

Discovered wireless routers/APs:

Name	MAC Address	LAN IP Address
brouter	00-00-00-00-00-00	192.168.119.1
IE_Brouter	00-60-B3-6F-89-C6	192.168.168.1
advap	00-06-F4-00-3E-CA	192.168.0.1
router	00-60-B3-6F-8B-2B	192.168.168.30
router	00-60-B3-6F-AB-F4	192.168.168.201

Description

Select a wireless router/AP and then click the "Web-Based Management..." button to manage it using a Web browser.

Fig. 64. Wireless Router/AP Browser.

- **The DRBAP stops working and does not respond to Web management requests.**

  - The firmware of the DRBAP may be stuck in an incorrect state.

    - Unplug the power connector from the power jack, and then re-plug the connector to restart the DRBAP.

    - Contact our technical support representatives to report this problem, so that the bugs can be static in future firmware versions.

  - If the DRBAP still does not work after restarting, there may be hardware component failures in the DRBAP.

- Contact our technical support representatives for repair.

Appendix C: Additional Information

C-1: Firmware Upgrade Using Xmodem Upgrade

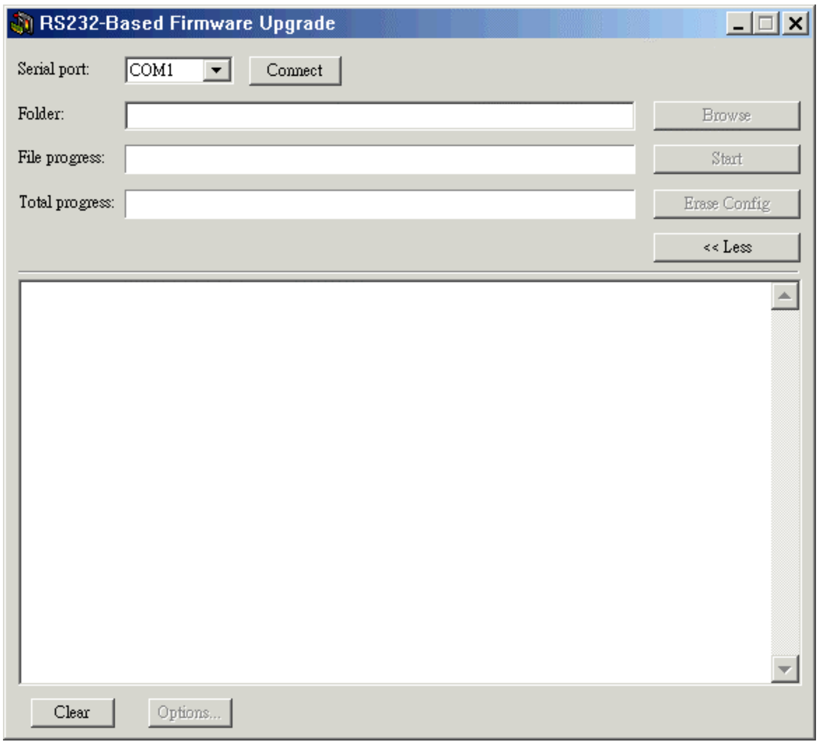


Fig. 65. Xmodem Upgrade.

To upgrade the firmware of DRBAP using Xmodem Upgrade over RS232:

1. Power off the DRBAP whose firmware will be upgraded.

2. Connect the managing PC and the DRBAP with an *RS232 Null Modem* cable.

3. Select the serial port (COM1 or COM2) you use for connecting the device from the **Serial port** drop-down list and click **Connect**.

4. Chose the folder in which the firmware files reside by click **Browse**.

5. Power on the DRBAP and you'll see bootup information.

6. Click **Start** to begin upgrade the firmware of the DRBAP.

7. You will be prompted when the upgrade process completes.

Click **Erase Config** to reset the configuration settings of the DRBAP to default values.