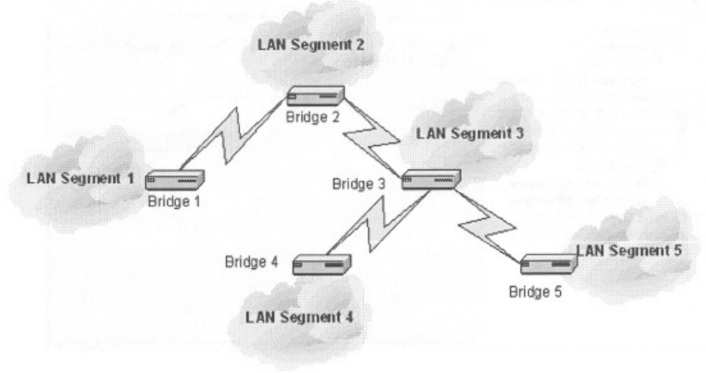


Fig. 12. Sample wireless bridge network topology.

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.

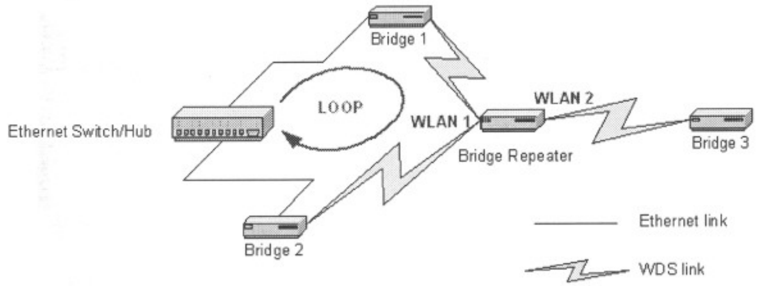
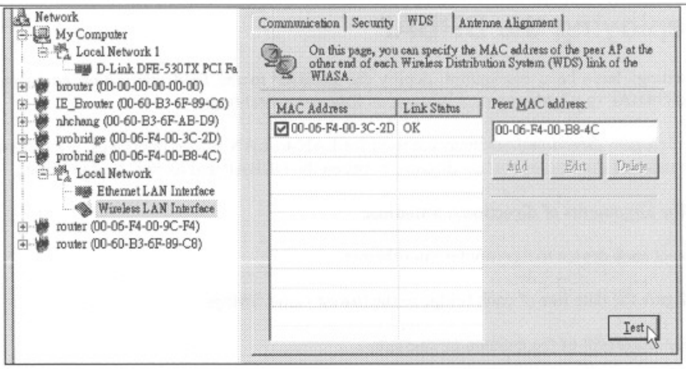


Fig. 13. Network topology containing a loop.

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.

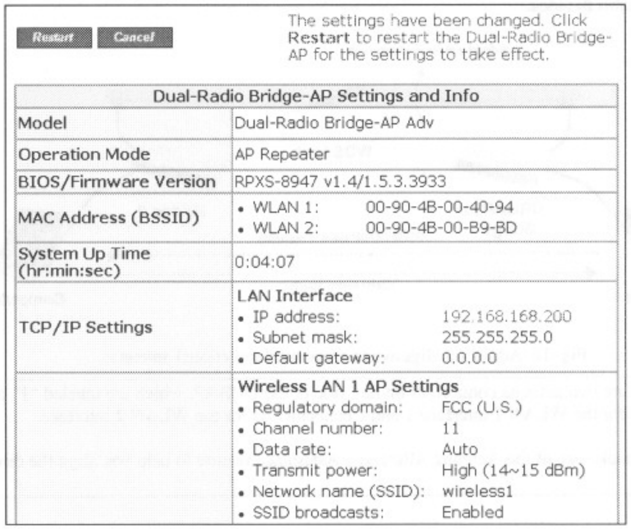
MAC Address	Link Status
☑ 00-06-F4-00-3C-2D	OK

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.

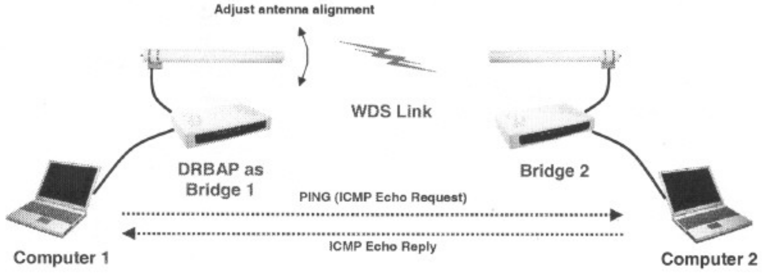
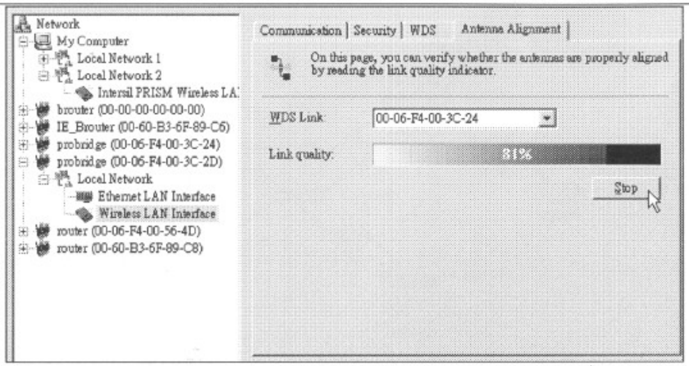


Fig. 16. Adjusting alignments of external directional antennas.

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%

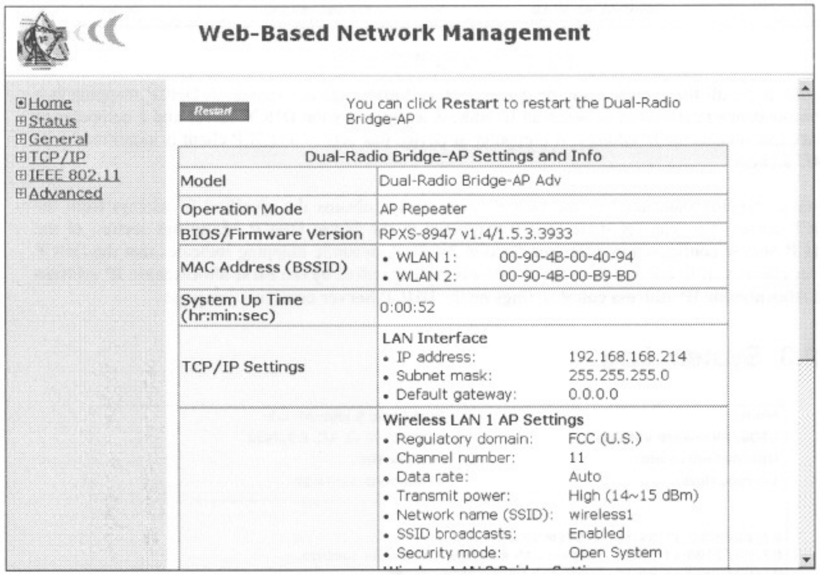
Fig. 17. Antenna alignment assistance.

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:

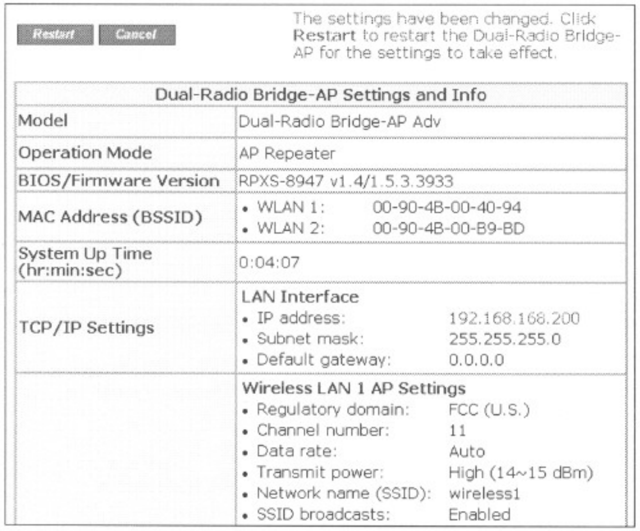
- **Home.** For going back to the start page.
- **Status.** Status information.
  - **Wireless Clients.** The status of the wireless clients currently associated with the DRBAP.
  - **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.
  - **System Log.** System events log.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

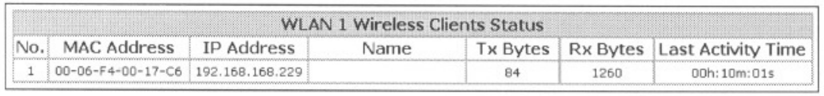
3.1.3. Home and Refresh Commands

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



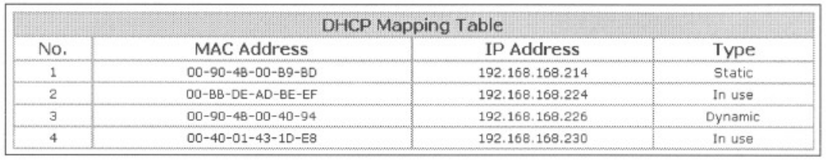
WLAN 1 Wireless Clients Status

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

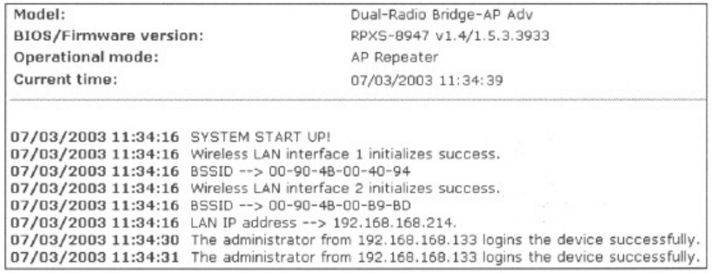
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

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



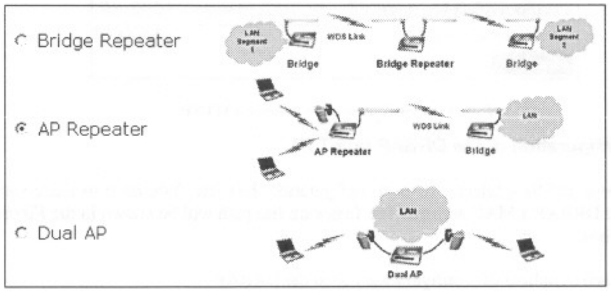
```
Model:                        Dual-Radio Bridge-AP Adv
BIOS/Firmware version:        RPXS-8947 v1.4/1.5.3.3933
Operational mode:             AP Repeater
Current time:                 07/03/2003 11:34:39

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.

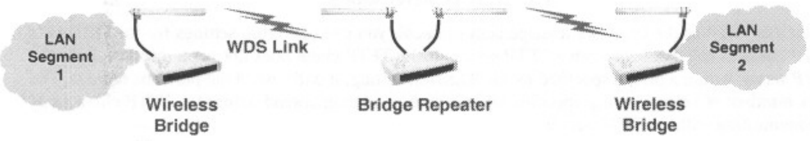


Fig. 26. **Bridge Repeater** mode.

- **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.

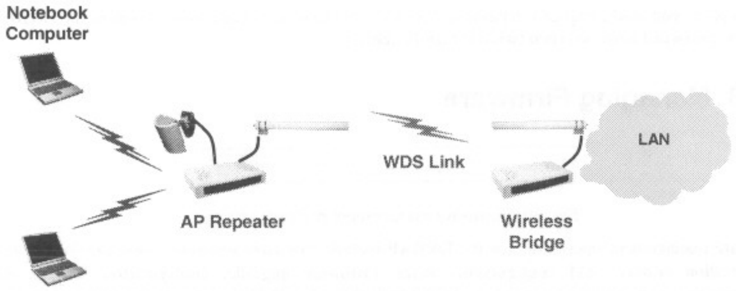


Fig. 27. **AP Repeater** mode.

- **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."

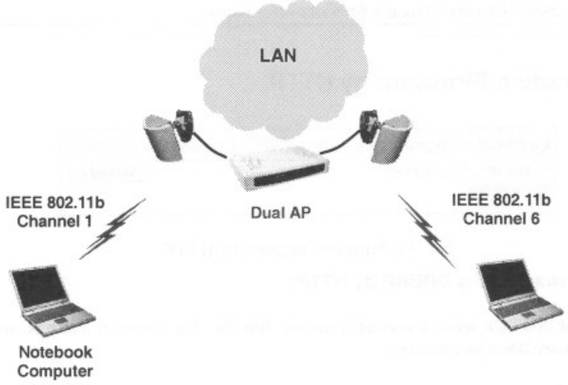
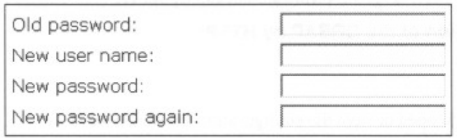


Fig. 28. **Dual AP** mode.

> 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

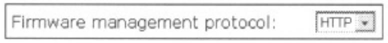
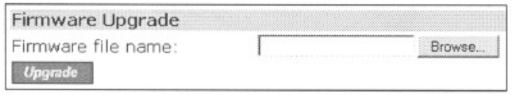

Firmware management protocol: HTTP

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


Firmware Upgrade

Firmware file name:

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

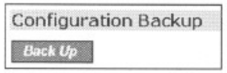

Configuration Backup

Fig. 32. Firmware backup by HTTP.

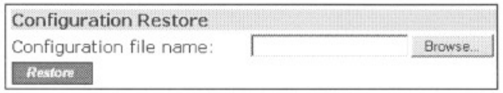
To back up configuration of the DRBAP by HTTP:

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.


Configuration Restore

Configuration file name:

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

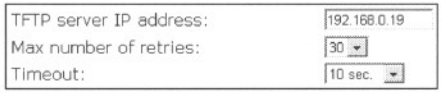

TFTP server IP address:	192.168.0.19
Max number of retries:	30
Timeout:	10 sec.

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.

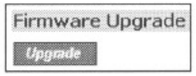

Firmware Upgrade

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.

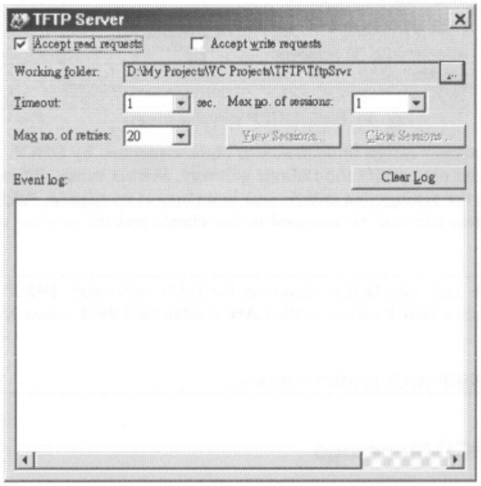
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.

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.

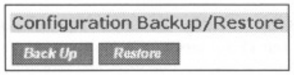
NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless DRBAP be connected by Ethernet, and on the same LAN, so that the upgrade process would be smooth.

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



Configuration Backup/Restore

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**.

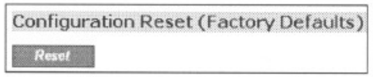
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

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)

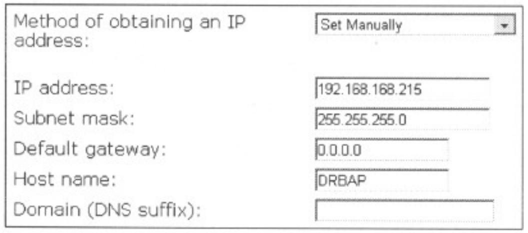
Fig. 38. Configuration reset.

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



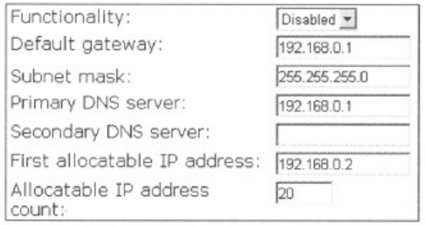
Method of obtaining an IP address:	Set Manually
IP address:	192.168.168.215
Subnet mask:	255.255.255.0
Default gateway:	0.0.0.0
Host name:	DRBAP
Domain (DNS suffix):	

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

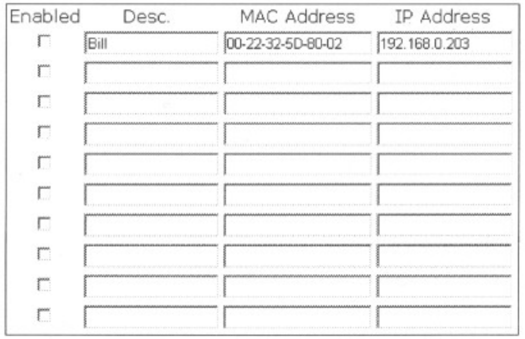
Fig. 40. Basic DHCP server settings.

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.

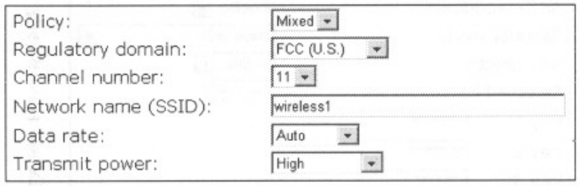
3.5. Configuring IEEE 802.11g-Related Settings

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).

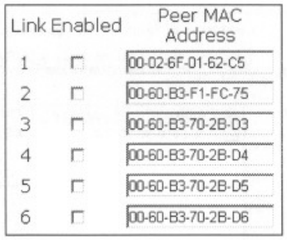
The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. **For two wireless devices to communicate with each other, they must be set to identical SSID (Service Set IDentifier).**

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.

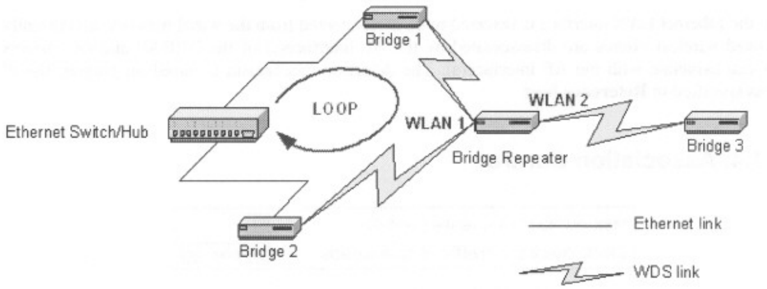
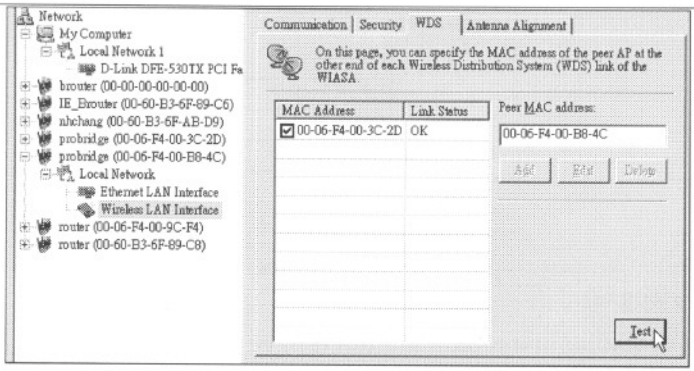


Fig. 44. Network topology containing a loop.

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.

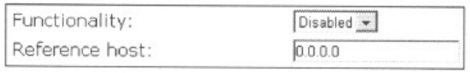
MAC Address	Link Status
☑ 00-06-F4-00-3C-2D	OK

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

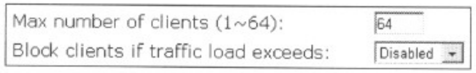


Functionality:	Disabled
Reference host:	0.0.0.0

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

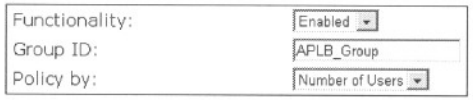


Max number of clients (1~64):	64
Block clients if traffic load exceeds:	Disabled

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

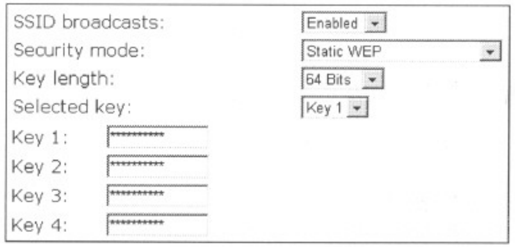
Fig. 48. AP load balancing settings.

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