IEEE 802.11 b/g

Integrated High Powered Access Point

User Guide

Version: 1.0

Last Updated: 06/23/2006

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.

Table of Contents

1. Introduction 1
1.1. Overview 1
1.2. Features 1
1.3. LED Definitions 4
2. First-Time Installation and Configuration 4
2.1. Selecting a Power Supply Method 4
2.2. Mounting the IEEE 802.11b/g on a Wall 4
2.3. Preparing for Configuration 5
2.3.1. Connecting the Managing Computer and the AP 5
2.4. Configuring the AP 6
2.4.1. Entering the User Name and Password 6
2.4.2. Step 1: Selecting an Operational Mode 8
2.4.3. Step 2: Configuring TCP/IP Settings 9
2.4.4. Step 3: Configuring IEEE 802.11 Settings 9
2.4.5. Step 4: Reviewing and Applying Settings 10
2.5. Deploying the IEEE 802.11b/g 10
2.6. Setting up Client Computers 11
2.6.1. Configuring IEEE 802.11b-Related Settings 11
2.6.2. Configuring TCP/IP-Related Settings 12
2.7. Confirming the Settings of the IEEE 802.11b/g and Client Computers 12
2.7.1. Checking if the IEEE 802.11b-Related Settings Work 12
2.7.2. Checking if the TCP/IP-Related Settings Work 12
3. Using Web-Based Network Manager 14
3.1. Overview 14
3.1.1. Menu Structure 14
3.1.2. Save, Save & Restart, and Cancel Commands 15
3.1.3. Home and Refresh Commands 16
3.2. Viewing Status 17
3.2.1. Associated Wireless Clients 17
3.2.2. Current DHCP Mappings 17
3.2.3. System Log 17
3.2.4. Link Monitor 18
3.3. General Operations 18
3.3.1. Specifying Operational Mode 18
3.3.2. Changing Password 19
3.3.3. Managing Firmware 19
3.3.3.1. Upgrading Firmware by HTTP 20
3.3.3.2. Backing up and Restoring Configuration Settings by HTTP 20
3.3.3.3. Upgrading Firmware by TFTP 21
3.3.3.4. Backing up and Restoring Configuration Settings by TFTP 22
3.3.3.5. Resetting Configuration to Factory Defaults 24
3.4. Configuring TCP/IP Related Settings 24
3.4.1. Addressing 24
3.4.2. DHCP Server 25
3.4.2.1. Basic 25
3.4.2.2. Static DHCP Mappings 25
3.5. Configuring IEEE 802.11g-Related Settings 26
3.5.1. Communication 26
3.5.1.1. Basic 26
3.5.1.2. Multiple SSID 27
3.5.1.3. Link Integrity 27
3.5.1.4. Association Control 27

3.5.1.5. IEEE 802.11b/g Load Balancing 28
3.5.1.6. Wireless Distribution System 28
3.5.2. Security 31
3.5.2.1. Basic 33
3.5.2.2. MAC-Address-Based Access Control 35
3.5.3. IEEE 802.1x/RADIUS 36
3.6. Configuring Advanced Settings 38
3.6.1. Packet Filters 38
3.6.1.1. Ethernet Type Filters 38
3.6.1.2. IP Protocol Filters 39
3.6.1.3. TCP/UDP Port Filters 39
3.6.2. Management 40
3.6.2.1. UPnP 40
3.6.2.2. System Log 40
3.6.2.3. SNMP 41
Appendix A: Default Settings 42
Appendix B: Troubleshooting 43
B-1: Wireless Settings Problems 43
B-2: TCP/IP Settings Problems 44
B-3: Unknown Problems 45

1. Introduction

1.1. Overview

The IEEE 802.11b/g wireless access point (AP) enables 802.11g or IEEE 802.11b client computers to access the resources on the Ethernet network. With the sleek Web-based user interface, a network administrator can efficiently manage the IEEE 802.11b/g.

In Chapter 2, we describe the steps to install and configure the IEEE 802.11b/g. The detailed steps show how to setup the AP. In Chapter 2, detailed explanation of each Web management page is given so the user may fine-tune the settings of the IEEE 802.11b/g to meet their specific requirements.

1.2. Features

- **IEEE 802.11b/g Firmware Features**
  - **Operational modes**
    - **AP/Bridge.** This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
    - **AP Client.** This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.
  - **RF type selection.** The RF type of the 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).** For authentication and data encryption.
  - **Enabling/disabling SSID broadcasts.** When the IEEE 802.11b/g is in AP/Bridge mode, 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 IEEE 802.11b/g with an “any” network name (SSID, Service Set ID); the correct SSID has to be specified on client computers.
  - **MAC-address-based access control.** When the IEEE 802.11b/g is in AP/Bridge mode, it can be configured to block unauthorized wireless client computers based on MAC (Media Access Control) addresses. The ACL (Access Control List) can be downloaded from a TFTP server.
  - **IEEE 802.1x/RADIUS.** When the IEEE 802.11b/g is in AP/Bridge mode, it can be configured to authenticate wireless users and distribute encryption keys dynamically by IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service).
  - **WPA (Wi-Fi Protected Access).** The IEEE 802.11b/g 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 se-

curity.

  - **Repeater.** When the IEEE 802.11b/g is in AP/Bridge mode, it can communicate with other APs or wireless bridges via WDS (Wireless Distribution System). Therefore, a IEEE 802.11b/g can wirelessly forward packets from wireless clients to another IEEE 802.11b/g. Then the second IEEE 802.11b/g forwards the packets to the Ethernet network.

  - **Wireless client isolation.** When the IEEE 802.11b/g is in AP/Bridge mode, wireless-to-wireless traffic 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 IEEE 802.11b/g's can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the IEEE 802.11b/g's. This function is available when the IEEE 802.11b/g is in AP/Bridge mode.

  - **Transmit power control.** Transmit power of the IEEE 802.11b/g's RF module can be adjusted to change RF coverage of the IEEE 802.11b/g.

  - **Link integrity.** When the IEEE 802.11b/g is in AP/Bridge mode and its Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the IEEE 802.11b/g and no wireless client can associate with it.

  - **Association control.** When the IEEE 802.11b/g 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.** When the IEEE 802.11b/g is in AP/Bridge mode, it can show the status of all wireless clients that are associated with the IEEE 802.11b/g.

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

- **DHCP client.** The IEEE 802.11b/g can automatically obtain an IP address from a DHCP server.

- **DHCP server.** The IEEE 802.11b/g 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 IEEE 802.11b/g provides Layer 2, Layer 3, and Layer 4 filtering capabilities.

- **Firmware Management Tools**

  - **Firmware upgrade.** The firmware of the IEEE 802.11b/g 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 (HyperText Transfer Protocol).

    - **Configuration backup.** The configuration settings of the IEEE 802.11b/g 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**

    - **Web-based Network Manager** for configuring and monitoring the IEEE 802.11b/g via a Web browser. The management protocol is HTTP (Hyper Text Transfer Protocol)-based.

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

    - **UPnP.** The IEEE 802.11b/g responds to UPnP discovery messages so that a Windows XP user can locate the IEEE 802.11b/g in My Network Places and use a Web browser to configure it.

    - **Telnet.** The user is enabled to manage the IEEE 802.11b/g by Telnet.

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

        - **Local log.** System events are logged to the on-board RAM of the IEEE 802.11b/g 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.** 48VDC power is supplied to a IEEE 802.11b/g over an Ethernet cable using an 802.11af compliant power injector. This feature facilitates large-scale wireless LAN deployment.

- **Hardware Watchdog Timer.** If the firmware “hangs” in an invalid state, the hardware watchdog timer will detect this situation and restart the IEEE 802.11b/g. This way, the IEEE 802.11b/g can provide continuous services.

1.3. LED Definitions

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

- **DDC**: *Alive*. Blinks when the IEEE 802.11b/g is working normally.
- **RF**: IEEE 802.11b/g interface activity
- **LAN0**: Ethernet LAN0 port interface activity
- **LAN1**: Ethernet LAN1 interface activity
- **PWR**: Power

2. First-Time Installation and Configuration

2.1. Selecting a Power Supply Method

The IEEE 802.11b/g can be powered by the supplied power adapter or optionally via PoE (Power over Ethernet). The IEEE 802.11b/g automatically selects the suitable power supply.

To power the IEEE 802.11b/g 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 AP.

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 AP by PoE:

1. Plug one connector of an Ethernet cable to an available port of a PoE hub.

2. Plug the other connector of the Ethernet cable to the **LAN0** port of the IEEE 802.11b/g.

NOTE: The PoE capability of the bridge is 802.3af compatible.

2.2. Mounting the IEEE 802.11b/g on a Wall

The IEEE 802.11b/g is wall-mountable.

1. Stick the supplied drilling template on the wall.

2. Use a ϕ7.0mm driller to drill a 25mm-deep hole at each of the cross marks.

3. Insert the supplied plastic conical anchors into each hole.

4. Screw the supplied screw in each plastic conical anchor to the proper depth so that the IEEE 802.11b/g can hang on the screws.

5. Hang the wireless IEEE 802.11b/g on the screws.

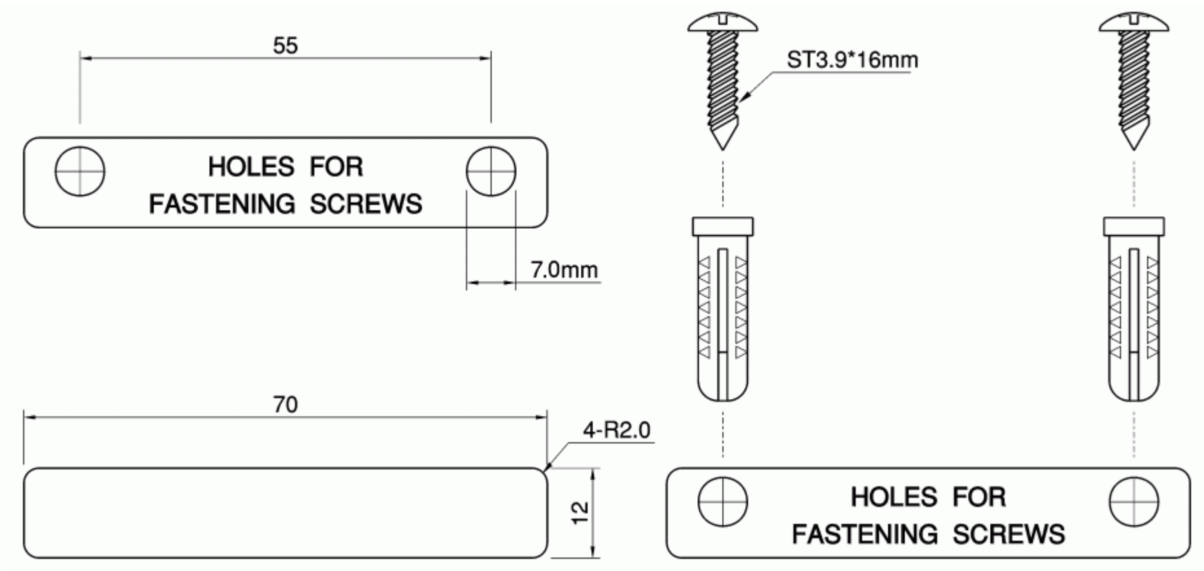


Fig. 1: Mounting the IEEE 802.11b/g on a wall

2.3. Preparing for Configuration

For you to configure a IEEE 802.11b/g, a *managing computer* with a Web browser is needed. For first-time configuration of an AP, an Ethernet network interface card (NIC) should have been installed in the managing computer. For maintenance-configuration of a deployed AP, either a wireless computer or a wired computer can be employed as the managing computer.

NOTE: If you are using the browser, *Opera*, to configure a IEEE 802.11b/g, 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 AP.

Since the configuration/management protocol is HTTP-based, make sure that **the IP address of the managing computer and the IP address of the *managed AP* are in the same IP subnet** (the default IP address of an IEEE 802.11b/g is **192.168.0.1** and the default subnet mask is **255.255.255.0**.)

2.3.1. Connecting the Managing Computer and the AP

To connect the Ethernet managing computer and the managed IEEE 802.11b/g for first-time configuration, you have two choices as illustrated in Fig. 2.

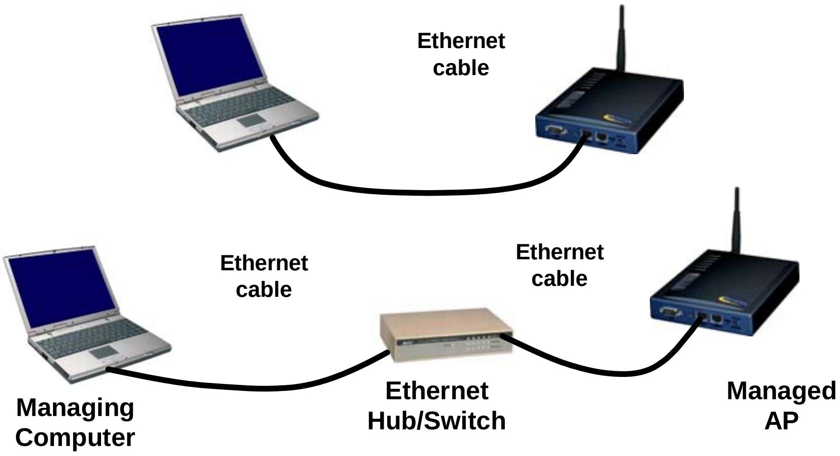


Fig. 2: Connecting a managing computer and the IEEE 802.11b/g via Ethernet

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

NOTE: One connector of the Ethernet cable must be plugged into the **LAN0** IEEE 802.11b/g port for configuration.

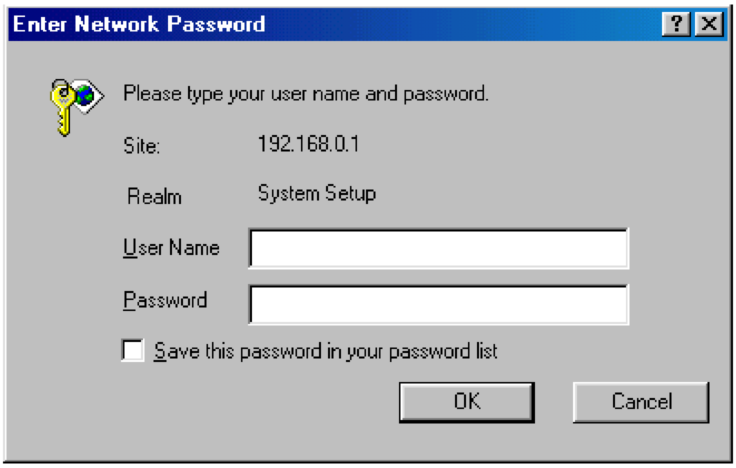
2.4. Configuring the AP

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* home page.

TIP: The IEEE 802.11b/g can be reached by its *host name* using a Web browser. For example, if the IEEE 802.11b/g is named "AP", you can use the URL "http://AP" to access the Web-based Network Manager of the IEEE 802.11b/g.

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.


Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

Realm System Setup

User Name

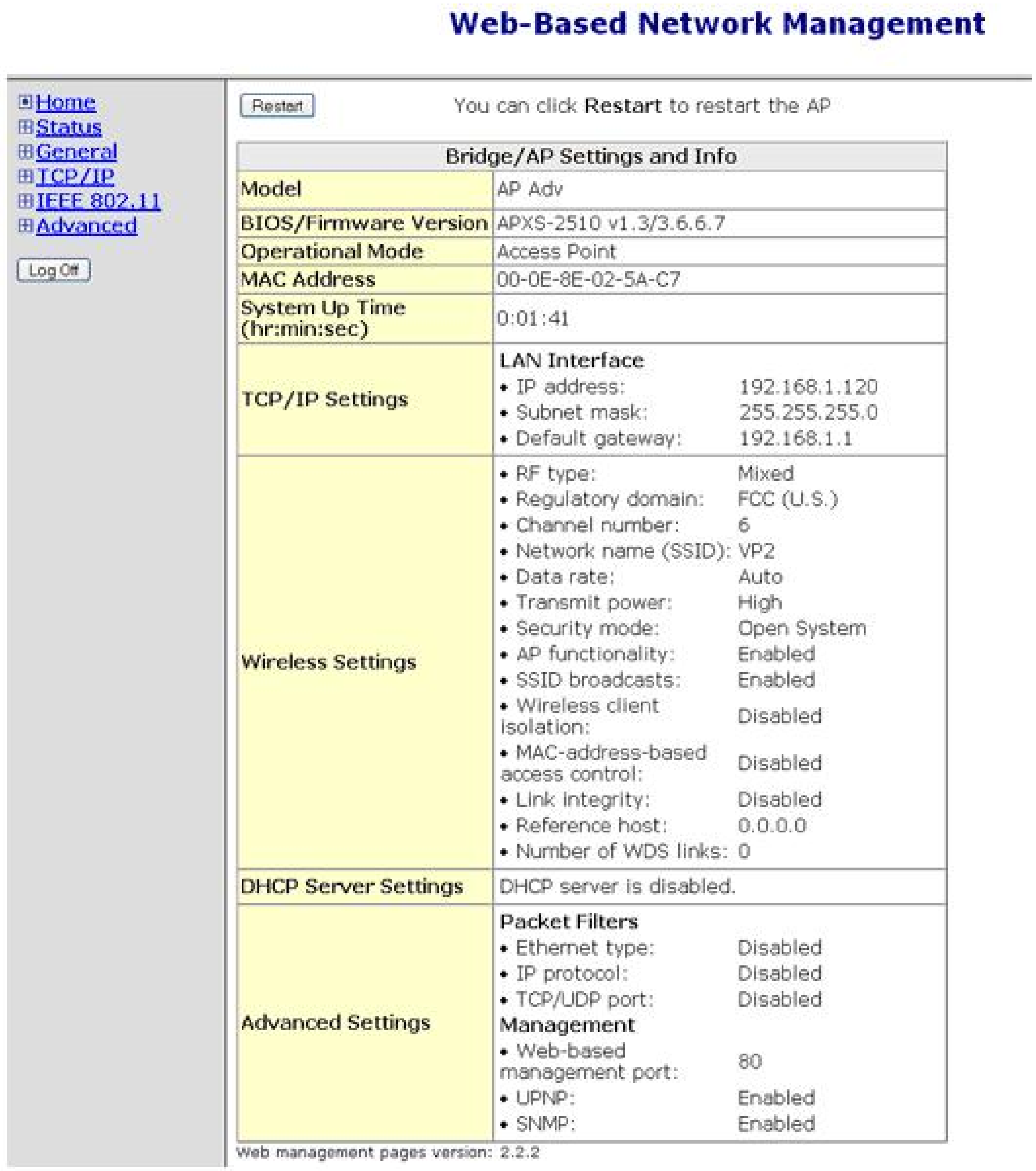
Password

□ 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 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 AP, it can be saved or printed within the Web browser for future reference.



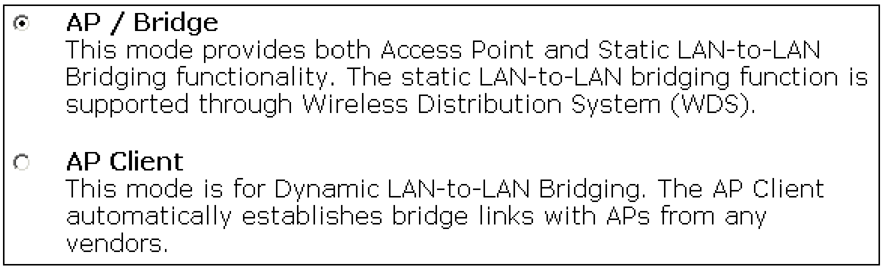
You can click **Restart** to restart the AP

Bridge/AP Settings and Info	
Model	AP Adv
BIOS/Firmware Version	APXS-2510 v1.3/3.6.6.7
Operational Mode	Access Point
MAC Address	00-0E-8E-02-5A-C7
System Up Time (hr:min:sec)	0:01:41
TCP/IP Settings	**LAN Interface** • IP address: 192.168.1.120 • Subnet mask: 255.255.255.0 • Default gateway: 192.168.1.1
Wireless Settings	• RF type: Mixed • Regulatory domain: FCC (U.S.) • Channel number: 6 • Network name (SSID): VP2 • Data rate: Auto • Transmit power: High • Security mode: Open System • AP functionality: Enabled • SSID broadcasts: Enabled • Wireless client isolation: Disabled • MAC-address-based access control: Disabled • Link integrity: Disabled • Reference host: 0.0.0.0 • Number of WDS links: 0
DHCP Server Settings	DHCP server is disabled.
Advanced Settings	**Packet Filters** • Ethernet type: Disabled • IP protocol: Disabled • TCP/UDP port: Disabled **Management** • Web-based management port: 80 • UPNP: Enabled • SNMP: Enabled

Web management pages version: 2.2.2

Fig. 4: The Start page

2.4.2. Step 1: Selecting an Operational Mode



● AP / Bridge
This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).

○ AP Client
This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Fig. 5: Operational mode settings

Go to the **General, Operational Mode** section, select an operational mode and click **Save** at the bottom of this page, and then you are brought back to the start page.

The IEEE 802.11b/g supports two operational modes:

- **AP/Bridge.** This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- **AP Client.** This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

In either mode, the IEEE 802.11b/g forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are two types of wireless links as specified by the IEEE 802.11 standard.

- **STA-AP.** This type of wireless link is established between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The AP Client mode is actually an STA.
- **WDS.** This type of wireless link is established between two IEEE 802.11 IEEE 802.11b/g's. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

The relationships among the operational modes and the wireless link types are shown in the following table:

	AP/Bridge	**AP Client**
AP/Bridge	WDS	STA-AP
AP Client	STA-AP	

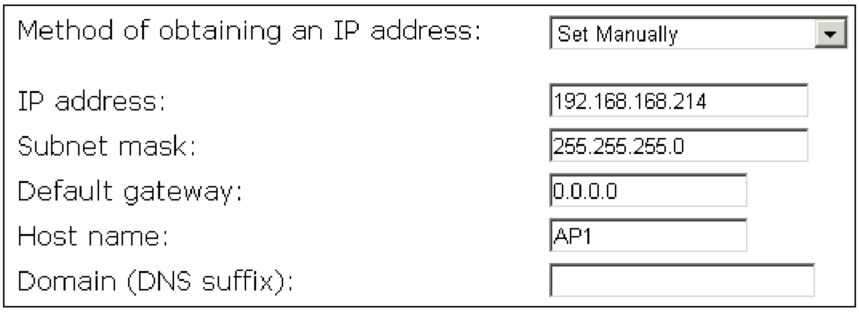
Table 1: Operational modes vs. wireless link types

To establish a *static* bridge link based on WDS, the AP/bridges at both end of the WDS link must be *manually* configured with each other's MAC addresses (see Section 3.5.1.6 for more information). To establish a *dynamic* bridge link between a IEEE 802.11b/g and an AP Client, both devices have to be configured with the same SSID and WEP settings. The AP Client automatically scans for any IEEE 802.11b/g that is using the matched SSID and establishes a bridge link with the scanned IEEE 802.11b/g.

NOTE: Although it's more convenient to use dynamic bridging, it has a limitation—the AP Client only can forward TCP/IP packets between its wireless interface and Ethernet interface; other type of traffic (such as IPX and AppleTalk) is not forwarded.

TIP: When the IEEE 802.11b/g is configured to be in AP Client, it can be used as an Ethernet-to-wireless network adapter. For example, a notebook computer equipped with an Ethernet adapter can be connected to this device with a crossover Ethernet cable for wireless connectivity to another access point.

2.4.3. Step 2: Configuring TCP/IP Settings



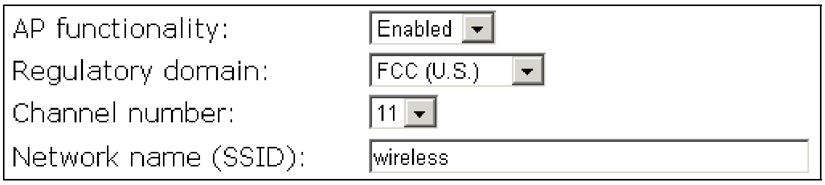
Method of obtaining an IP address:	Set Manually
IP address:	192.168.168.214
Subnet mask:	255.255.255.0
Default gateway:	0.0.0.0
Host name:	AP1
Domain (DNS suffix):	

Fig. 6: 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 AP.

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



AP functionality:	Enabled
Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	wireless

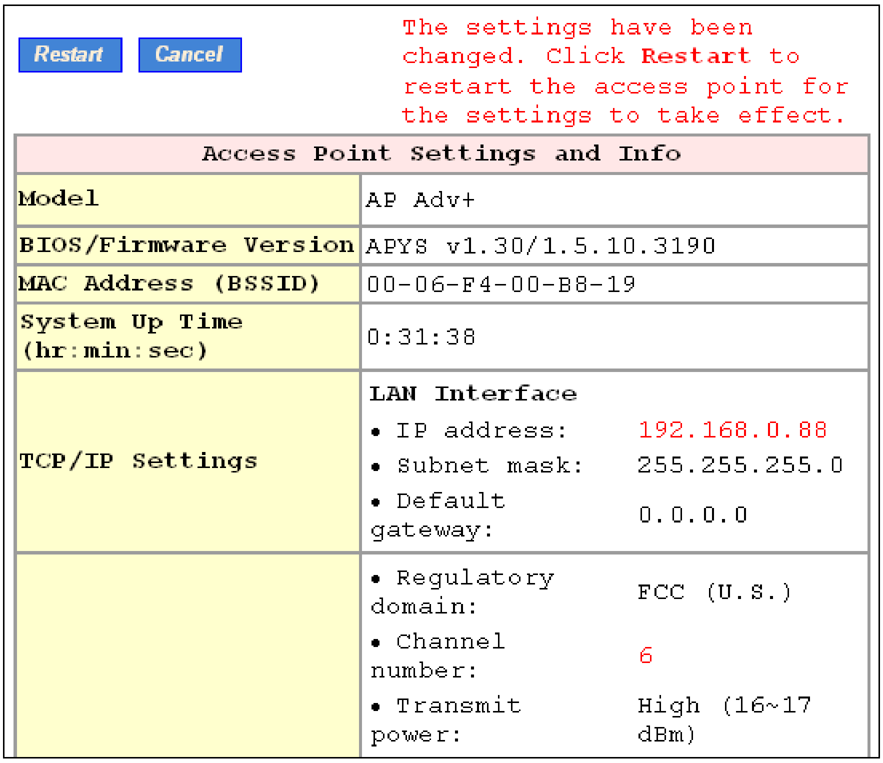
Fig. 7: IEEE 802.11b communication settings

Go to the **IEEE 802.11, Communication** section to configure IEEE 802.11b-related communication settings, including **Regulatory domain**, **Channel number**, and **Network name (SSID)**.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. **The SSID of a wireless client computer and the SSID of the IEEE 802.11b/g must be identical for them to communicate with each other.**

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

2.4.5. Step 4: Reviewing and Applying Settings



The settings have been changed. Click **Restart** to restart the access point for the settings to take effect.

Access Point Settings and Info	
Model	AP Adv+
BIOS/Firmware Version	APYS v1.30/1.5.10.3190
MAC Address (BSSID)	00-06-F4-00-B8-19
System Up Time (hr:min:sec)	0:31:38
TCP/IP Settings	**LAN Interface** • IP address: 192.168.0.88 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
	• Regulatory domain: FCC (U.S.) • Channel number: 6 • Transmit power: High (16~17 dBm)

Fig. 8: 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 IEEE 802.11b/g for the new settings to take effect.

NOTE: About *7* seconds are needed for the IEEE 802.11b/g to complete its restart process.

2.5. Deploying the IEEE 802.11b/g

After the settings have been configured, deploy the IEEE 802.11b/g to the field application environment. Connect the IEEE 802.11b/g to an Ethernet LAN through an Ethernet switch/hub.

If you are configuring a pair of the IEEE 802.11b/g's for a *dynamic* or *static* bridging application and external high-gain *directional* antennas are used, it's difficult to adjust alignments of the antennas when the pair of devices is distance away.

To adjust the alignments of a pair of bridges' directional antennas:

1. Connect each bridge 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 antenna on 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, 11Mbps, because of the distance and the gain of the antennas.

Fig. 9 illustrates the idea.

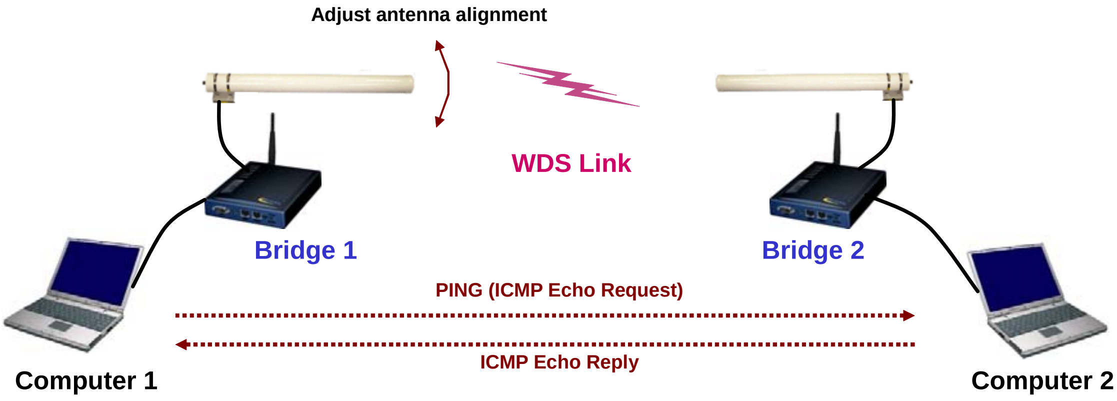


Fig. 9: Adjusting alignments of external directional antennas

TIP: When doing *dynamic* bridging, configure Bridge 1 to be in *AP Client* mode and configure Bridge 2 to be in *AP/Bridge* mode.

2.6. Setting up Client Computers

The TCP/IP and IEEE 802.11b-related settings of wireless client computers must match those of the IEEE 802.11b/g.

2.6.1. Configuring IEEE 802.11b-Related Settings

Before the TCP/IP networking system of a wireless client computer can communicate with other hosts, the underlying wireless link must be established between this wireless computer and an IEEE 802.11b/g.

To establish a wireless link to an AP:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.

2. Use the utility to make appropriate *Operating Mode*, *SSID* and *WEP* settings.

NOTE: A wireless client computer must be in *infrastructure* mode, so that it can associate with an AP.

NOTE: The SSID of the wireless client computer and the SSID of the IEEE 802.11b/g must be identical. Or, in case the **SSID broadcasts** capability of the IEEE 802.11b/g is enabled (by default), the SSID of the wireless client computer could be set to “any”.

NOTE: Both the wireless client computer and the IEEE 802.11b/g must have the same WEP settings for them to communicate with each other.

NOTE: For better wireless security, IEEE 802.1x capability of the IEEE 802.11b/g must be enabled so that only authenticated wireless users can access the wireless network. Refer to the IEEE 802.1x-related white papers on the companion CD-ROM for more information about deploying secure WLANs with IEEE 802.1x support.

2.6.2. Configuring TCP/IP-Related Settings

Use **Windows Network Control Panel Applet** to change the TCP/IP settings of the client computers, so that the IP addresses of the client computers and the IP address of the IEEE 802.11b/g are in the same IP subnet.

If a client computer is originally set a static IP address, you can either change its IP address to match the IP address of the AP, or select an automatically-obtain-an-IP-address option if there is a DHCP server on the network.

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

2.7. Confirming the Settings of the IEEE 802.11b/g and Client Computers

After the deploying the IEEE 802.11b/g and setting up client computers, confirm that the settings are correct.

2.7.1. Checking if the IEEE 802.11b-Related Settings Work

To check if a wireless client computer can associate with the AP:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.

2. Check if the client computer is associated to an access point, and the access point is the IEEE 802.11b/g.

If the check fails, see Appendix B-1, "Wireless Settings Problems" for troubleshooting.

2.7.2. Checking if the TCP/IP-Related Settings Work

To check if a client computer can access the Internet:

1. Open a **Windows Command Prompt** window on the client computer.

2. Type "**ping** *advap*", where *advap* is a placeholder for the IP address of the AP. Replace it with your real IP address—for example, 192.168.0.1. Then press **Enter**.

   If the IEEE 802.11b/g responds, go to the next step; else, see Appendix B-2, "TCP/IP Settings Problems" for troubleshooting.

3. Type "**ping** *default_gateway*", where *default_gateway* is a placeholder for the IP address of the default gateway of the wireless client computer. Then press **Enter**.

   If the gateway responds, go to the next step; else, see Appendix B-2, "TCP/IP Settings Problems" for troubleshooting.

4. Type “**ping** *1st_dns_server*”, where *1st_dns_server* is a placeholder for the IP address of the primary DNS server of the wireless client computer. Then press **Enter**.

   If this DNS server responds, go to the next step; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

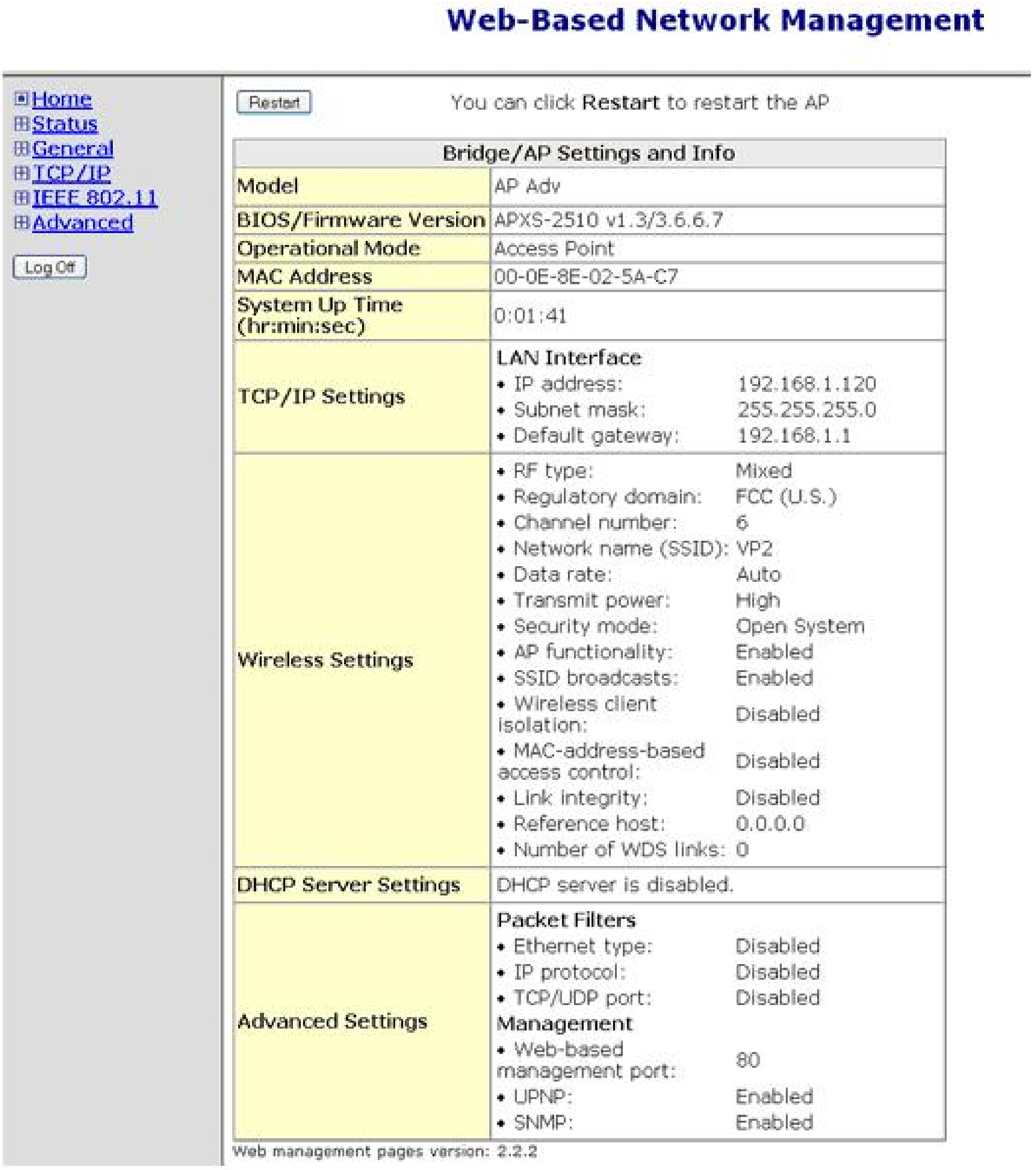
5. Type “**ping** *2nd_dns_server*”, where *2nd_dns_server* is a placeholder for the IP address of the secondary DNS server of the wireless client computer. Then press **Enter**.

   If this DNS server responds the client should have no problem with TCP/IP networking; else, see Appendix B-2, “TCP/IP Settings Problems” for troubleshooting.

3. Using Web-Based Network Manager

This chapter details the features of the Web management page of the Web-based Network Manager.

3.1. Overview



You can click **Restart** to restart the AP

Bridge/AP Settings and Info	
Model	AP Adv
BIOS/Firmware Version	APXS-2510 v1.3/3.6.6.7
Operational Mode	Access Point
MAC Address	00-0E-8E-02-5A-C7
System Up Time (hr:min:sec)	0:01:41
TCP/IP Settings	LAN Interface • IP address: 192.168.1.120 • Subnet mask: 255.255.255.0 • Default gateway: 192.168.1.1
Wireless Settings	• RF type: Mixed • Regulatory domain: FCC (U.S.) • Channel number: 6 • Network name (SSID): VP2 • Data rate: Auto • Transmit power: High • Security mode: Open System • AP functionality: Enabled • SSID broadcasts: Enabled • Wireless client isolation: Disabled • MAC-address-based access control: Disabled • Link integrity: Disabled • Reference host: 0.0.0.0 • Number of WDS links: 0
DHCP Server Settings	DHCP server is disabled.
Advanced Settings	Packet Filters • Ethernet type: Disabled • IP protocol: Disabled • TCP/UDP port: Disabled Management • Web-based management port: 80 • UPNP: Enabled • SNMP: Enabled

Web management pages version: 2.2.2

Fig. 10: 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 on 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 AP.
  - **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.
  - **System Log.** System events log.
  - **Link Monitor.** When the IEEE 802.11b/g is in *AP Client* mode, this page shows the signal strength and link quality of the wireless link to its associated access point.
- **General.** Global operations.
  - **Operational Mode.** Operational mode of the IEEE 802.11b/g —*AP/Bridge* or *AP Client*.
  - **Password.** For gaining rights to change the settings of the IEEE 802.11b/g.
  - **Firmware Tools.** For upgrading the firmware of the IEEE 802.11b/g, backing up and restoring configuration, and configuration reset settings of the IEEE 802.11b/g.
- **TCP/IP.** TCP/IP-related settings.
  - **Addressing.** IP address settings for the IEEE 802.11b/g to work with TCP/IP.
  - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the IEEE 802.11b/g.
- **IEEE 802.11.** IEEE 802.11g-related settings.
  - **Communication.** Basic settings for the IEEE 802.11b/g interface of the IEEE 802.11b/g to work properly with wireless clients.
  - **Security.** Security settings for authenticating wireless users and encrypting wireless data.
  - **IEEE 802.1x/RADIUS.** IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service) settings for better wireless security.
- **Advanced.** Advanced settings of the IEEE 802.11b/g.
  - **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

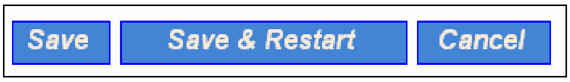
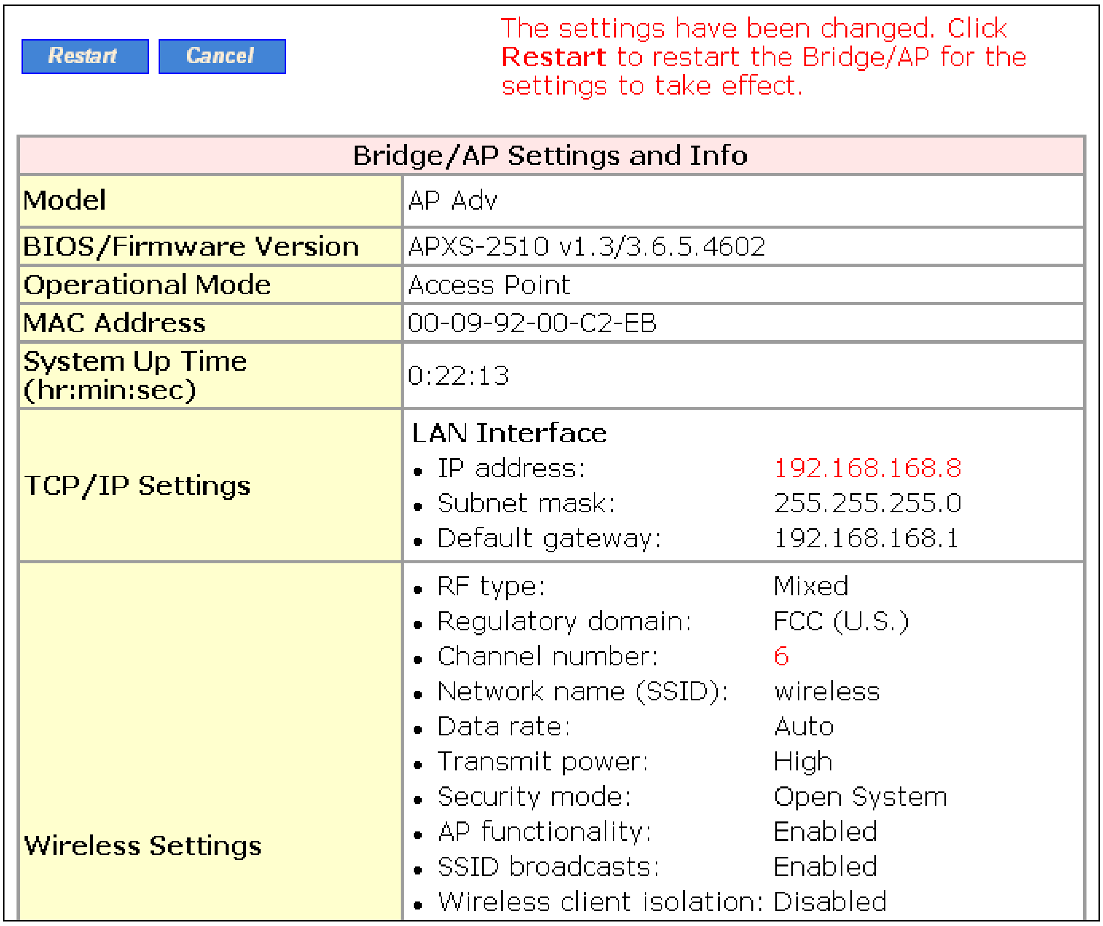


Fig. 11: Save, Save & Restart, and Cancel

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 IEEE 802.11b/g and brings you back to the start page. Clicking **Save & Restart** stores the settings changes to the memory of the IEEE 802.11b/g and restarts the IEEE 802.11b/g 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 IEEE 802.11b/g for the settings changes to take effect.



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

Bridge/AP Settings and Info	
Model	AP Adv
BIOS/Firmware Version	APXS-2510 v1.3/3.6.5.4602
Operational Mode	Access Point
MAC Address	00-09-92-00-C2-EB
System Up Time (hr:min:sec)	0:22:13
TCP/IP Settings	LAN Interface • IP address: 192.168.168.8 • Subnet mask: 255.255.255.0 • Default gateway: 192.168.168.1
Wireless Settings	• RF type: Mixed • Regulatory domain: FCC (U.S.) • Channel number: 6 • Network name (SSID): wireless • Data rate: Auto • Transmit power: High • Security mode: Open System • AP functionality: Enabled • SSID broadcasts: Enabled • Wireless client isolation: Disabled

Fig. 12: Settings have been changed

3.1.3. Home and Refresh Commands

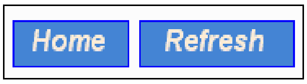
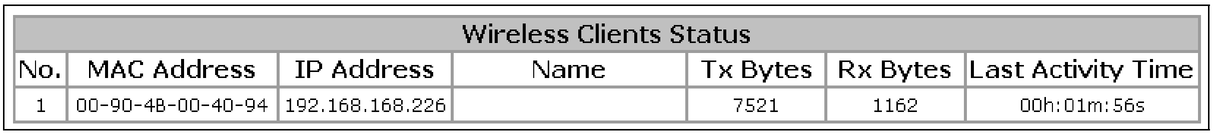


Fig. 13: Home and Refresh

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

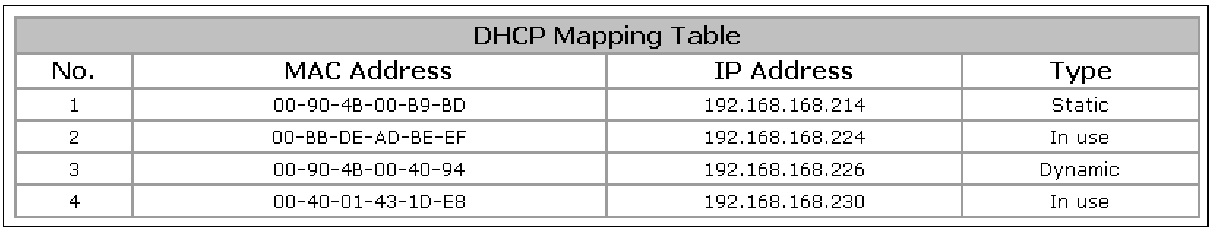


Wireless Clients Status						
No.	MAC Address	IP Address	Name	Tx Bytes	Rx Bytes	Last Activity Time
1	00-90-4B-00-40-94	192.168.168.226		7521	1162	00h:01m:56s

Fig. 14: 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



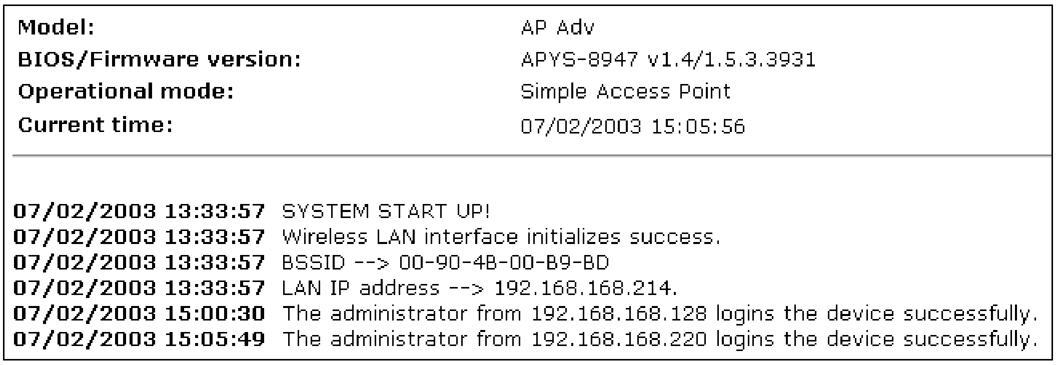
DHCP Mapping Table			
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

Fig. 15: 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 allocable IP address** and **Allocable IP address count** settings on the **DHCP Server** configuration page.

3.2.3. System Log



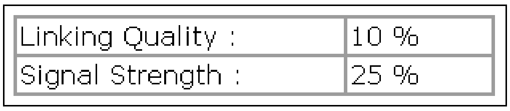
```
Model:                      AP Adv
BIOS/Firmware version:      APYS-8947 v1.4/1.5.3.3931
Operational mode:           Simple Access Point
Current time:               07/02/2003 15:05:56

07/02/2003 13:33:57  SYSTEM START UP!
07/02/2003 13:33:57  Wireless LAN interface initializes success.
07/02/2003 13:33:57  BSSID --> 00-90-4B-00-B9-BD
07/02/2003 13:33:57  LAN IP address --> 192.168.168.214.
07/02/2003 15:00:30  The administrator from 192.168.168.128 logins the device successfully.
07/02/2003 15:05:49  The administrator from 192.168.168.220 logins the device successfully.
```

Fig. 16: System log

System events are recorded in the memory of the IEEE 802.11b/g. 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.

3.2.4. Link Monitor



Linking Quality :	10 %
Signal Strength :	25 %

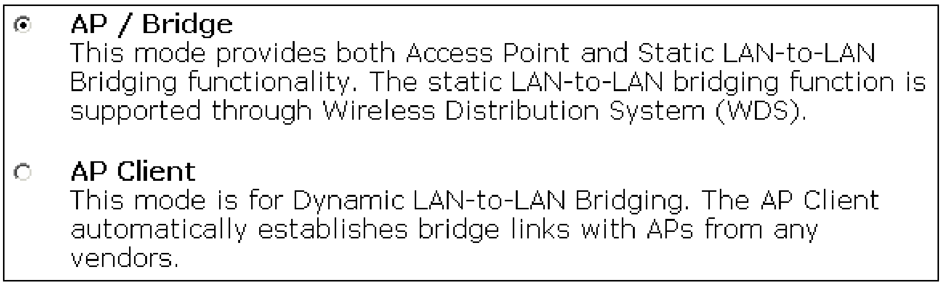
Fig. 17: Link monitor

When the IEEE 802.11b/g is in *AP Client* mode, you can use the Link Monitor status page to monitor the link quality and signal strength sensed by its RF module. Larger values means better wireless connectivity to its associated Access Point. This feature is especially useful when you are aligning a pair of directional antennas for bridging applications.

NOTE: The values are updated every 20 seconds.

3.3. General Operations

3.3.1. Specifying Operational Mode



● AP / Bridge
This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).

○ AP Client
This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Fig. 18: Operational modes settings

The IEEE 802.11b/g supports two operational modes:

- **AP/Bridge.** This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).

- **AP Client.** This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

In either mode, the IEEE 802.11b/g forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are 2 types of wireless links as specified by the IEEE 802.11 standard.

- **STA-AP.** This type of wireless link is established between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The AP Client mode is actually an STA.

- **WDS.** This type of wireless link is established between two IEEE 802.11 IEEE 802.11b/g's. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

The relationships among the operational modes and the wireless link types are shown in the following table:

	AP/Bridge	AP Client
AP/Bridge	WDS	STA-AP
AP Client	STA-AP	

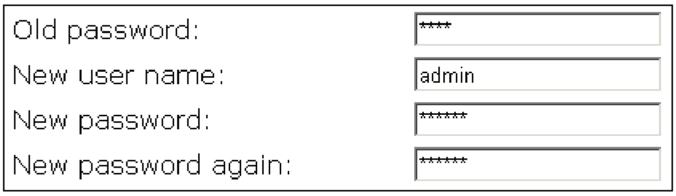
Table 2: Operational modes vs. wireless link types

To establish a *static* bridge link based on WDS, the AP/bridges at both end of the WDS link must be *manually* configured with each other's MAC addresses (see Section 3.5.1.6 for more information). To establish a *dynamic* bridge link between a IEEE 802.11b/g and an AP Client, both devices have to be configured with the same SSID and WEP settings. The AP Client automatically scans for any IEEE 802.11b/g that is using the matched SSID and establishes a bridge link with the scanned IEEE 802.11b/g.

NOTE: Although it's more convenient to use dynamic bridging, it has a limitation—the AP Client only can forward TCP/IP packets between its wireless interface and Ethernet interface; other type of traffic (such as IPX and AppleTalk) is not forwarded.

TIP: When the IEEE 802.11b/g is configured to be in AP Client, it can be used as an Ethernet-to-wireless network adapter. For example, a notebook computer equipped with an Ethernet adapter can be connected to this device with a crossover Ethernet cable for wireless connectivity to another access point.

3.3.2. Changing Password

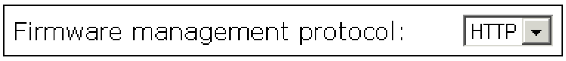


Old password:	****
New user name:	admin
New password:	******
New password again:	******

Fig. 19: Password

On this page the user name and password may be changed. The new password must be typed twice for confirmation.

3.3.3. Managing Firmware



Firmware management protocol: HTTP

Fig. 20: Firmware management protocol settings

Firmware management operations for the IEEE 802.11b/g 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 method is suggested since it is more user friendly. However, due to different behavior of various Web browsers, 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-method.

3.3.3.1. Upgrading Firmware by HTTP

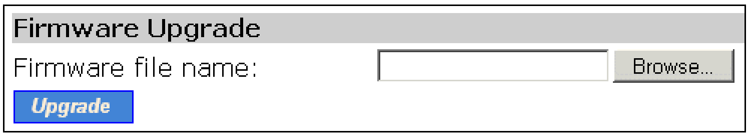


Fig. 21: Firmware upgrade by HTTP

To upgrade firmware of the IEEE 802.11b/g 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

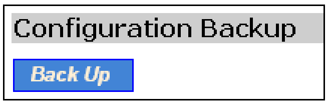


Fig. 22: Firmware backup by HTTP

To back up configuration of the IEEE 802.11b/g 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 IEEE 802.11b/g's MAC address. For example, if the IEEE 802.11b/g'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.

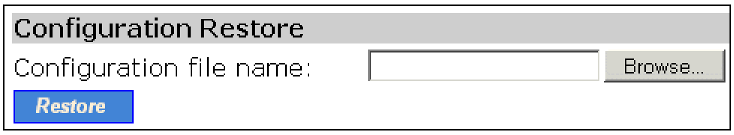


Fig. 23: Configuration restore by HTTP

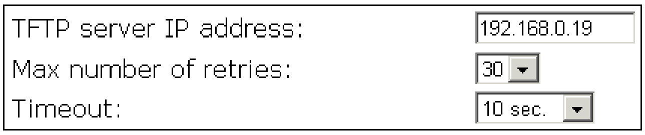
To restore configuration of the IEEE 802.11b/g by HTTP:

1. Click **Browse** and then select a correct configuration **.hex** file. You have to make sure the file

name is the AP’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 IEEE 802.11b/g.

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. 24: TFTP server settings

When use TFTP as the firmware management protocol, you can configure settings for the IEEE 802.11b/g’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. 25: Firmware upgrade by TFTP

To upgrade firmware of the IEEE 802.11b/g 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 IEEE 802.11b/g and the computer are in the same IP subnet.

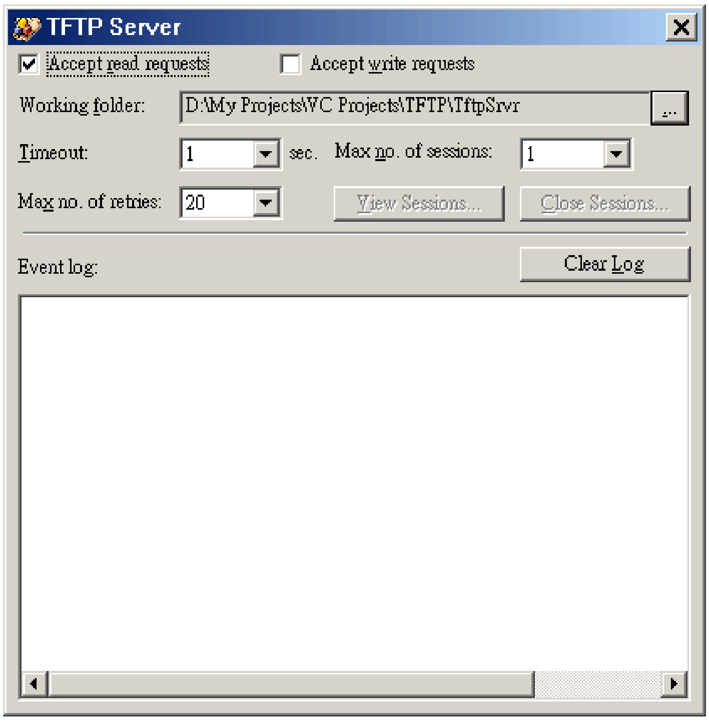
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.

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 IpcConfig, 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. 26: 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 IEEE 802.11b/g and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

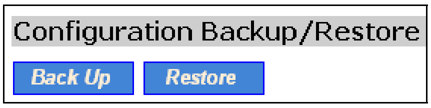
NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless IEEE 802.11b/g be connected by Ethernet, and on the same LAN, so that the upgrade process would be smooth.

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 IEEE 802.11b/g unbootable. When this occurs, call for technical support.

TIP: If you want to remotely upgrade the firmware of a deployed IEEE 802.11b/g 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. 27: Configuration backup/restore

To back up configuration of the IEEE 802.11b/g 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 IEEE 802.11b/g 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 IEEE 802.11b/g 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 IEEE 802.11b/g's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "AaBbCcDdEeFf" is the AP's MAC address. For example, if the AP'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 IEEE 802.11b/g 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 IEEE 802.11b/g 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 AP's MAC address. For example, if the AP'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**.

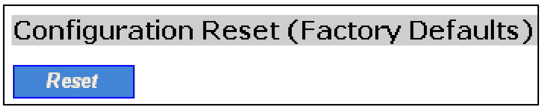
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.

8. Trigger the restoring process by clicking **Restore**. The IEEE 802.11b/g will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the IEEE 802.11b/g.

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)

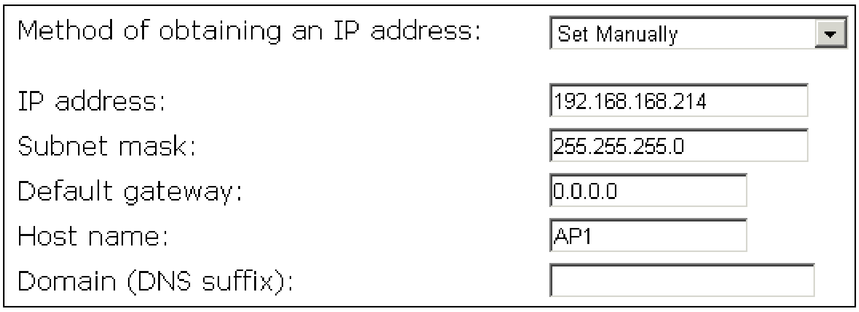
Fig. 28: Configuration reset

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: 192.168.168.214

Subnet mask: 255.255.255.0

Default gateway: 0.0.0.0

Host name: AP1

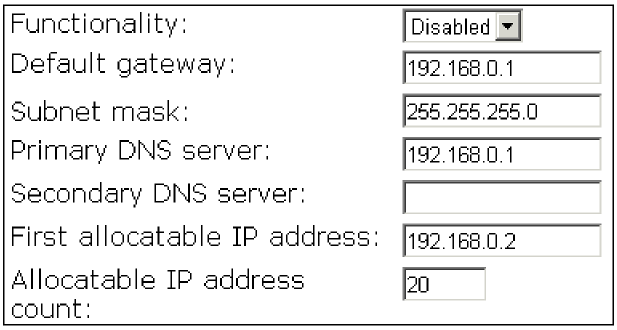
Domain (DNS suffix):

Fig. 29: TCP/IP settings

The IP address of the IEEE 802.11b/g 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 IEEE 802.11b/g.

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

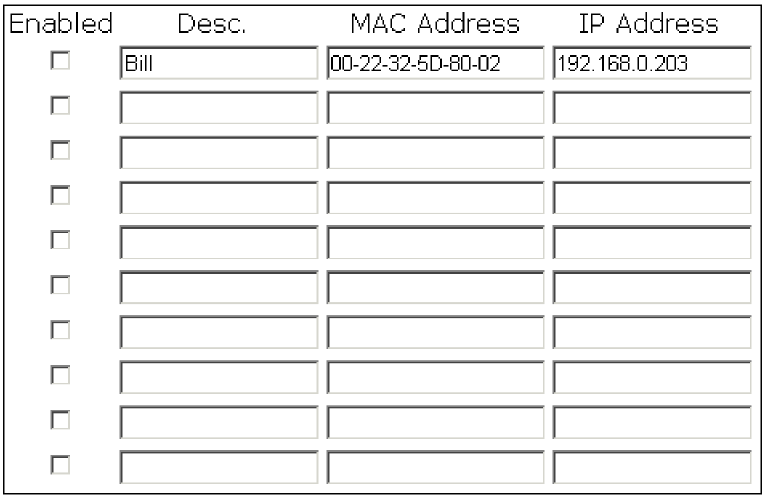
Fig. 30: Basic DHCP server settings

The IEEE 802.11b/g 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 allocable 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 IEEE 802.11b/g.

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. 31: 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.

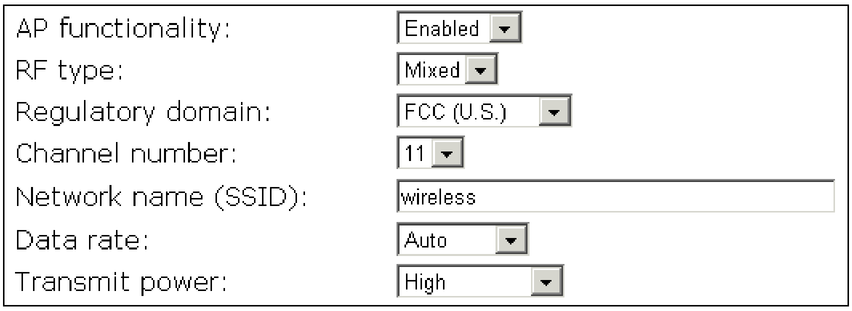
2. Select the corresponding **Enabled** check box.

3.5. Configuring IEEE 802.11g-Related Settings

3.5.1. Communication

3.5.1.1. Basic

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



AP functionality:	Enabled
RF type:	Mixed
Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	wireless
Data rate:	Auto
Transmit power:	High

Fig. 32: Basic IEEE 802.11g communication settings

For specific needs such as configuring the IEEE 802.11b/g as a wireless LAN-to-LAN bridge, the IEEE 802.11b/g functionality can be disabled, so that no wireless client can associate with the IEEE 802.11b/g.

The RF type 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. The SSID of a wireless client computer and the SSID of the IEEE 802.11b/g must be identical for them to communicate with each other.

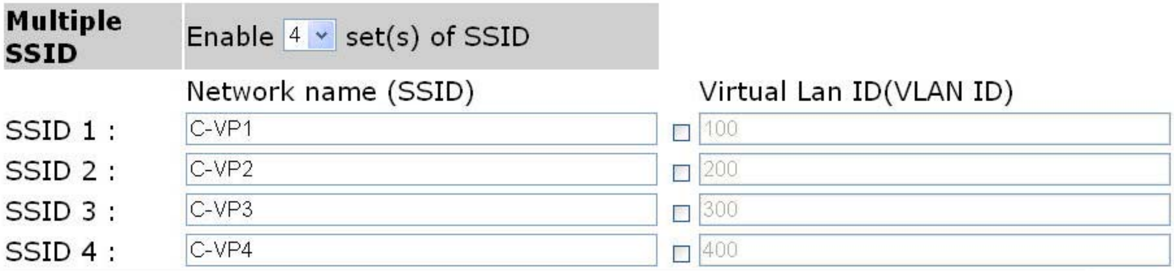
If there is RF interference, you may want to reduce the **Data rate** for more reliable wireless transmission. In most cases, leave the setting to **Auto**.

The transmit power of the RF module of the IEEE 802.11b/g can be adjusted so that the RF coverage of the IEEE 802.11b/g can be changed.

3.5.1.2. Multiple SSID

If you want to configure the Guest and Internal networks on Virtual LAN (VLANs), the switch and DHCP server you are using must support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard.

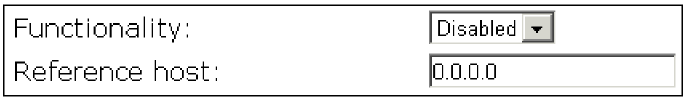
The **MSSID** numbers can setup for 1 to 4 sets. When you enable MSSID you can name each SSID. If you configure enable Guest access and configure Internal and Guest networks on VLANs, this field will be enabled. Provide a number between 1 and 4095 for the Internal VLAN. This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE802.1Q frames. The access point must be able to reach the DHCP server. Check with the Administrator regarding the VLAN and DHCP configurations.



Multiple SSID	Enable 4 set(s) of SSID		
	Network name (SSID)		Virtual Lan ID(VLAN ID)
SSID 1 :	C-VP1	□	100
SSID 2 :	C-VP2	□	200
SSID 3 :	C-VP3	□	300
SSID 4 :	C-VP4	□	400

Fig. 33: Basic MSSID communication settings

3.5.1.3. Link Integrity

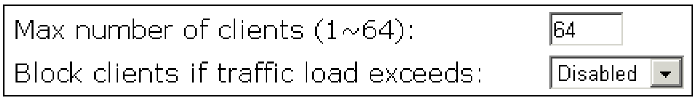


Functionality:	Disabled
Reference host:	0.0.0.0

Fig. 34: 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 IEEE 802.11b/g and no wireless client can associate with the IEEE 802.11b/g. The detection mechanism is based on pinging the IP address specified in **Reference host**.

3.5.1.4. Association Control

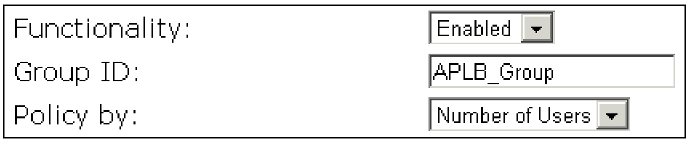


Max number of clients (1~64):	64
Block clients if traffic load exceeds:	Disabled

Fig. 35: 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 IEEE 802.11b/g. If traffic load of the IEEE 802.11b/g exceeds the load specified in the **Block clients if traffic load exceeds** setting, no more wireless client can associate with the IEEE 802.11b/g.

3.5.1.5. IEEE 802.11b/g Load Balancing



Functionality:	Enabled ▾
Group ID:	APLB_Group
Policy by:	Number of Users ▾

Fig. 36: IEEE 802.11b/g load balancing settings

Several IEEE 802.11b/g's 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 IEEE 802.11b/g 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 IEEE 802.11b/g that has the less traffic load in the group.

3.5.1.6. Wireless Distribution System

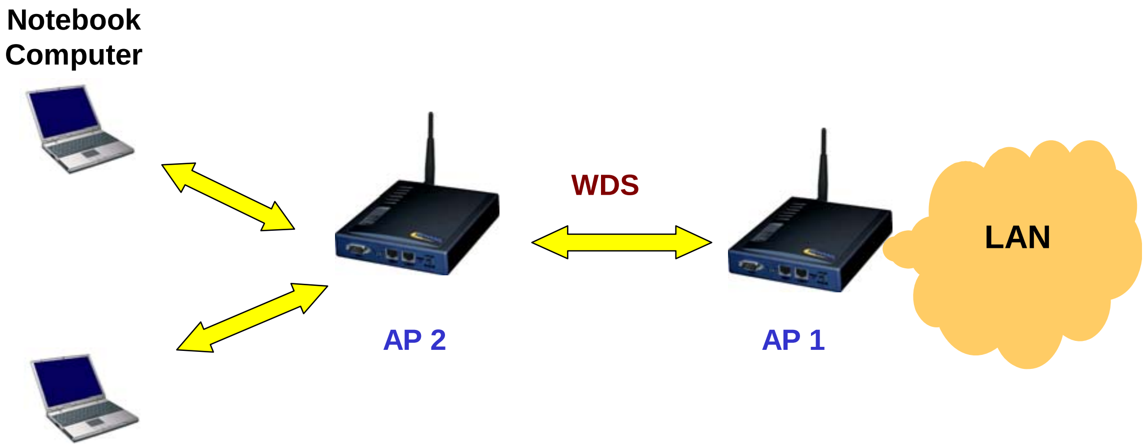


Fig. 37: Wireless Distribution System

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 37, AP 2 acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 plays a role of "AP repeater".

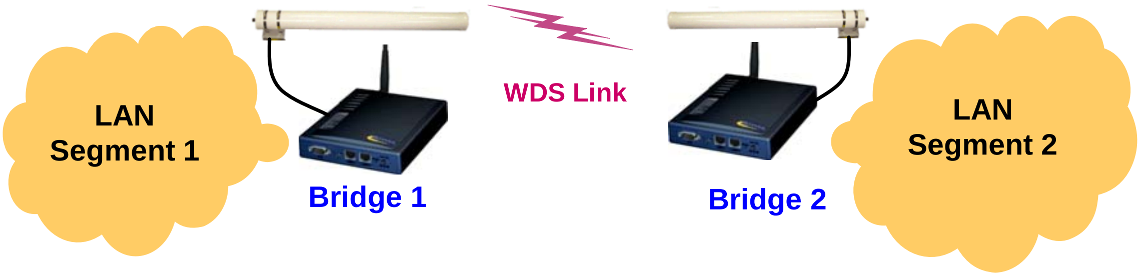
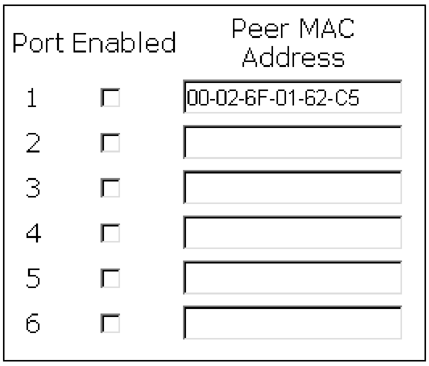


Fig. 38: LAN-to-LAN bridging

By WDS, two or more LAN segments can be connected wirelessly. As illustrated in Fig. 38, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the IEEE 802.11b/g is WDS-enabled, it can be used as a wireless bridge.

NOTE: A IEEE 802.11b/g can have up to *6* WDS links to other APs or wireless bridges.



Port	Enabled	Peer MAC Address
1	□	00-02-6F-01-62-C5
2	□	
3	□	
4	□	
5	□	
6	□	

Fig. 39: Wireless Distribution System settings

To enable a WDS link:

1. Specify the MAC address of the IEEE 802.11b/g at the other end of the WDS link.

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

For example, assume you want two IEEE 802.11b/g's with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link between them. On IEEE 802.11b/g 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on AP 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 an IEEE 802.11b/g is connected to other peer IEEE 802.11b/g s or wireless bridges by WDS.

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.

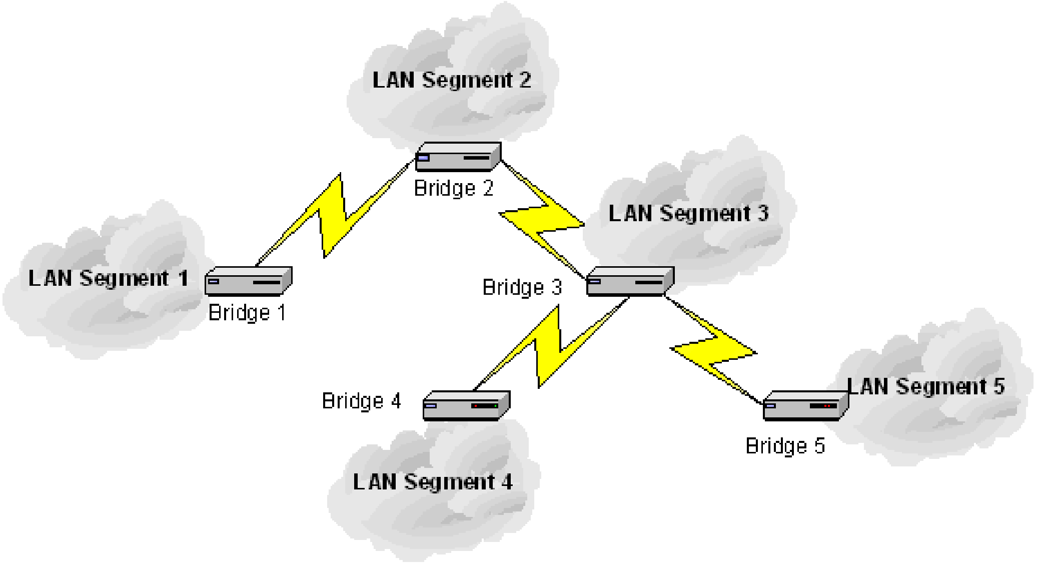


Fig. 40. Sample wireless bridge network topology.

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

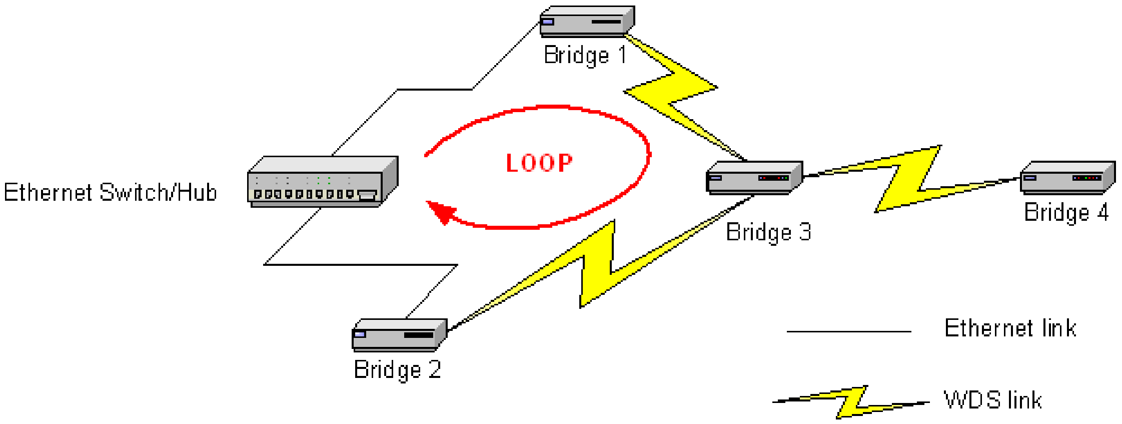


Fig. 41: Network topology containing a loop

If external high-gain *directional* antennas are used, it's difficult to align the antennas when the distance between the bridges is long.

To adjust the alignments of a pair of bridges' directional antennas:

7. Connect each bridge to a computer via Ethernet.
8. Configure the date rate of each bridge to the lowest value, 1Mbps.
9. Fix the alignment of the antenna on one side.
10. Adjust the alignment of the antenna on other side by using response time information obtained from PINGing (run PING.exe) the "fixed-side" computer.
11. Fine-tune the alignment of the antenna until you get a best response time.

12. 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, 11Mbps, because of the distance and the gain of the antennas.

Fig. 42 illustrates the idea.

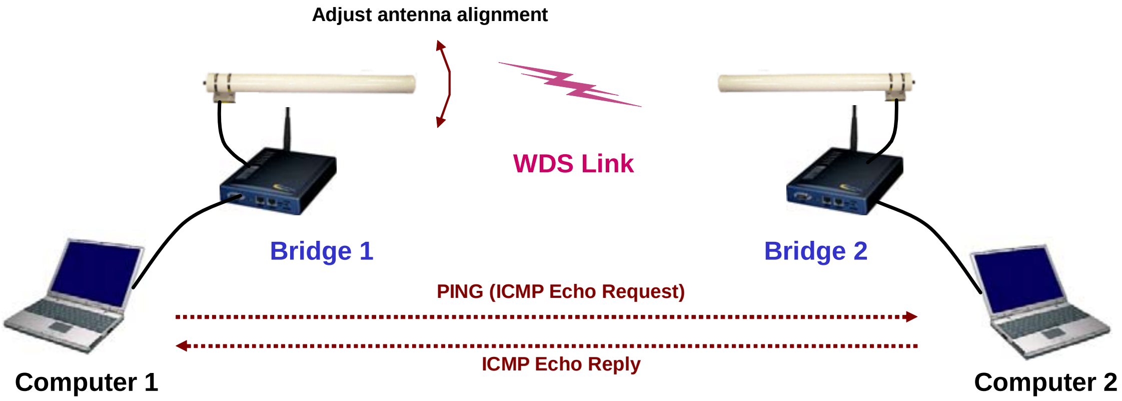
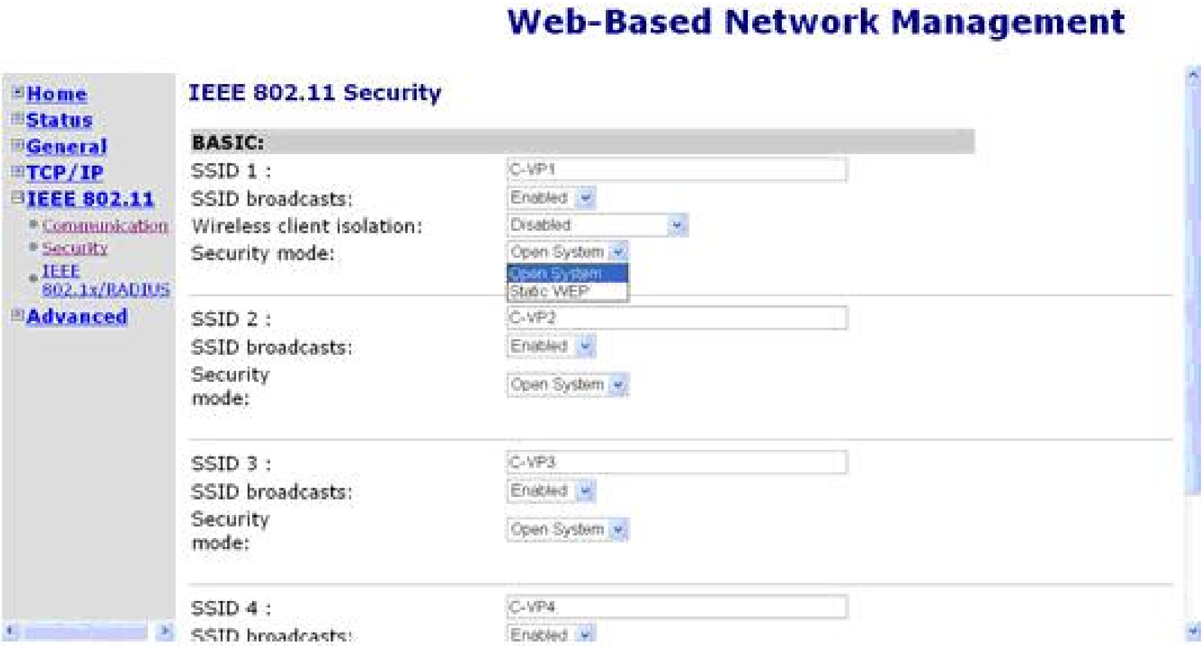


Fig. 42: Adjusting alignments of external directional antennas

3.5.2. Security

IEEE 802.11g security settings include **SSID broadcasts**, **Wireless client isolation**, **Security mode**, **IEEE 802.11 Authentication algorithm**, **WEP keys**, **MAC-Address-Based Access Control**.



IEEE 802.11 Security

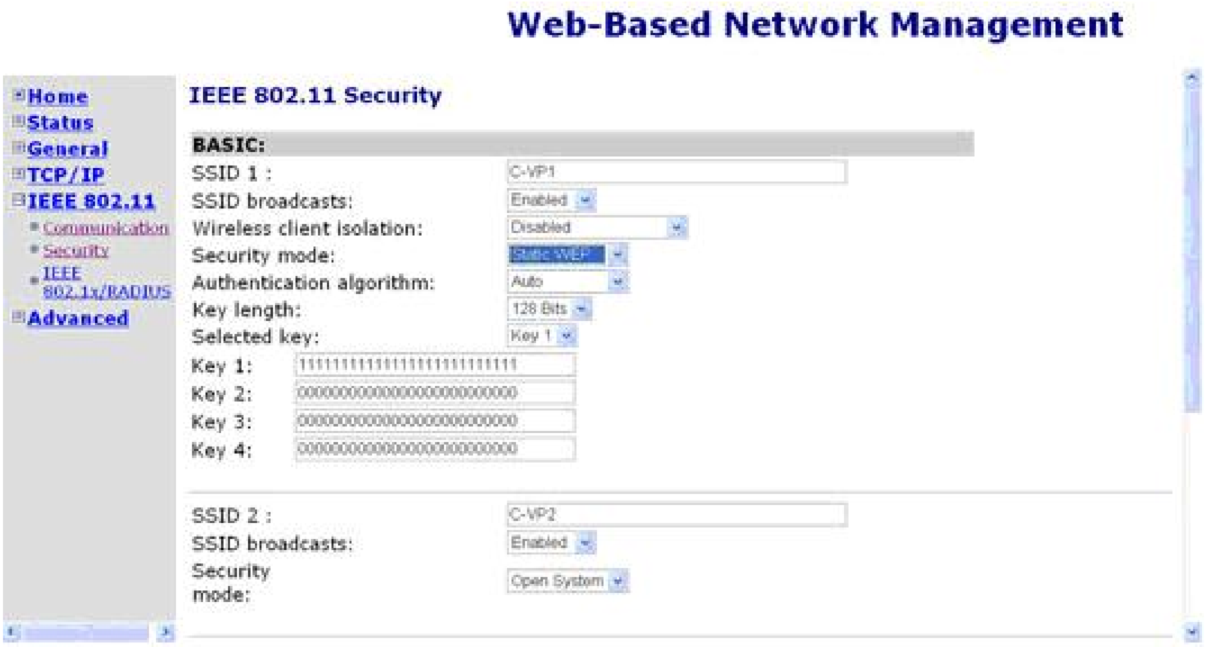
BASIC:

SSID 1 : C-VP1
SSID broadcasts: Enabled
Wireless client isolation: Disabled
Security mode: Open System

SSID 2 : C-VP2
SSID broadcasts: Enabled
Security mode: Open System

SSID 3 : C-VP3
SSID broadcasts: Enabled
Security mode: Open System

SSID 4 : C-VP4
SSID broadcasts: Enabled



IEEE 802.11 Security

BASIC:

SSID 1 :	C-VP1
SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
Security mode:	Static WEP
Authentication algorithm:	Auto
Key length:	128 Bits
Selected key:	Key 1
Key 1:	11111111111111111111111111
Key 2:	00000000000000000000000000
Key 3:	00000000000000000000000000
Key 4:	00000000000000000000000000
SSID 2 :	C-VP2
SSID broadcasts:	Enabled
Security mode:	Open System

SSID 1~4 The network names that you name each SSID in the previous page

SSID Broadcasts Enable or Disable SSID broadcast.
Enabling this feature broadcasts the SSID across the network.

Wireless client isolation When the IEEE 802.11b/g is in AP/Bridge mode, wireless-to-wireless traffic 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.

Security mode The Security options for the primary SSID (SSID1) are up to 9 security modes depending on AP model variations:

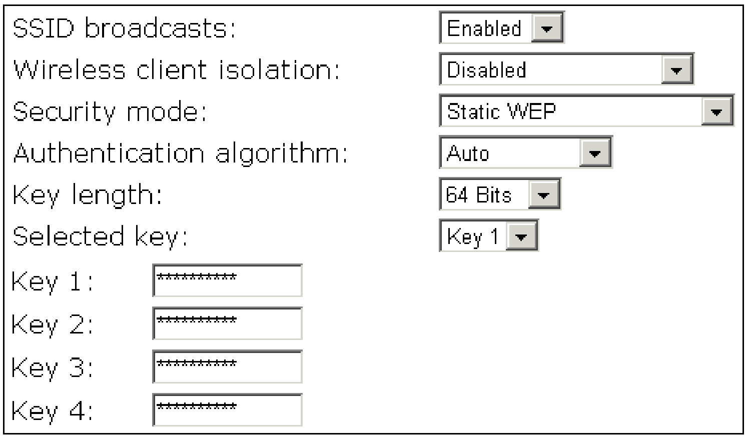
Open System. No authentication, no data encryption.

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

Key length Select 64-, 128-bits

Selected key Select the 1st through the 4th key to be the active key. Enter the key that you need here.

3.5.2.1. Basic



SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
Security mode:	Static WEP
Authentication algorithm:	Auto
Key length:	64 Bits
Selected key:	Key 1
Key 1:	**********
Key 2:	**********
Key 3:	**********
Key 4:	**********

Fig. 43: Basic 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 IEEE 802.11b/g 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 IEEE 802.11b/g’s 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 IEEE 802.11b/g 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 IEEE 802.11b/g’s in the same IP subnet is blocked. The behaviors are illustrated in the following figures.

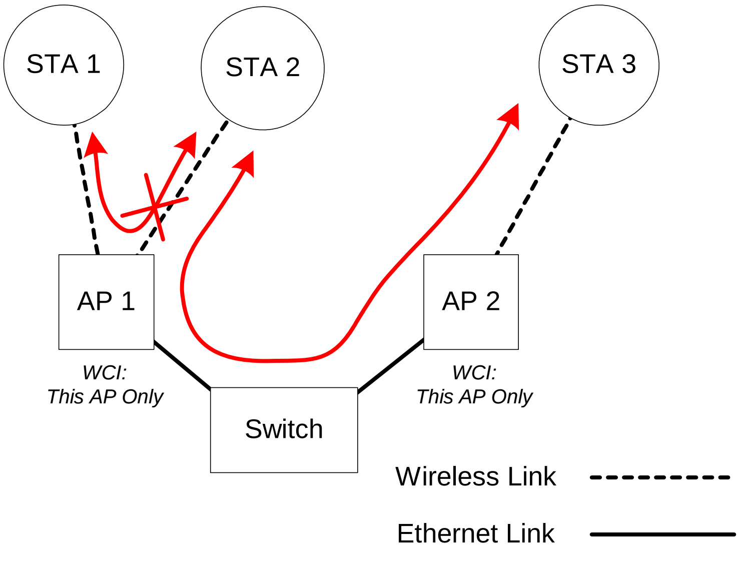


Fig. 44: Behavior of the “This AP Only” wireless client isolation option

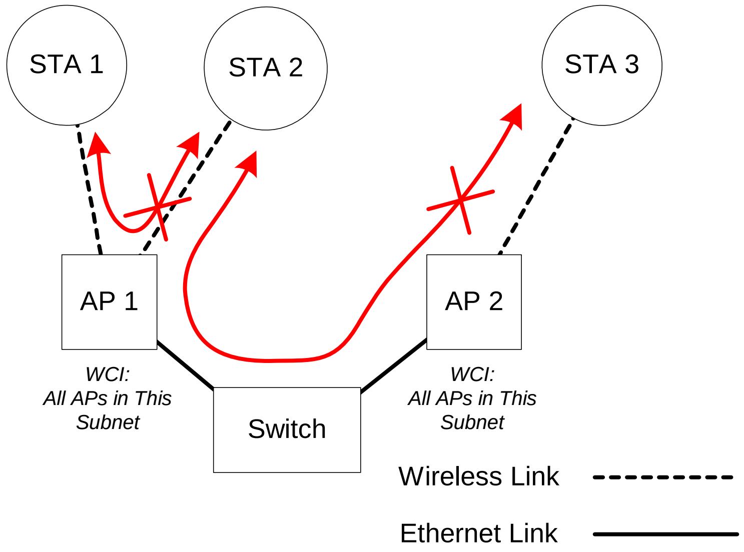


Fig. 45: Behavior of the “All APs on This Subnet” wireless client isolation option

As illustrated in Fig. 44 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. 45, 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 IEEE 802.11b/g is highly secured in this mode.

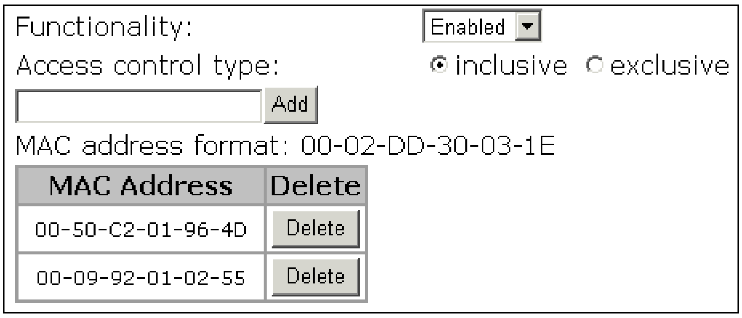
In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1x functionality is enabled. See Section 3.5.3 for more information about IEEE 802.1x and RADIUS.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, *Shared Key* authentication is used if WEP data encryption is enabled. In rare cases, *Open System* authentication may be used when WEP data encryption is enabled. The **Authentication algorithm** setting is provided for better compatibility with wireless clients with various WLAN network adapters. There are three options available, including *Open System*, *Shared Key*, and *Auto*.

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 IEEE 802.11b/g 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 IEEE 802.11b/g 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".

3.5.2.2. MAC-Address-Based Access Control



Functionality: Enabled

Access control type: ● inclusive ○ exclusive

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

MAC Address	Delete
00-50-C2-01-96-4D	Delete
00-09-92-01-02-55	Delete

Fig. 46: MAC-address-based access control settings

With **MAC-Address-Based Access Control**, you can specify the wireless client computers that are permitted or not permitted to associate with the IEEE 802.11b/g. When the table type is set to *inclusive*, entries in the table are permitted to associate with the IEEE 802.11b/g. When the table type is set to *exclusive*, entries in the table are not permitted to associate with the IEEE 802.11b/g.

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*.

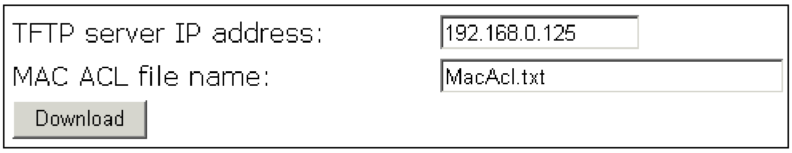
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Steps 3 for other wireless clients.

To delete an entry in the access control table:

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

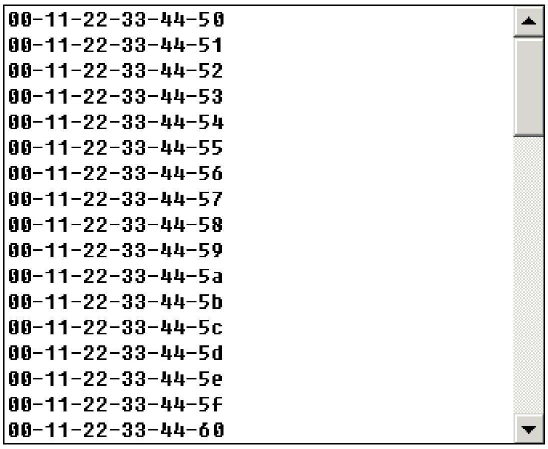
NOTE: The size of the access control table is 64.



TFTP server IP address: 192.168.0.125
MAC ACL file name: MacAcl.txt

Fig. 47: 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 IEEE 802.11b/g to download the MAC ACL (Access Control List) file from the TFTP server. Fig. 48 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. 48: 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**.

3.5.3. 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 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), 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.

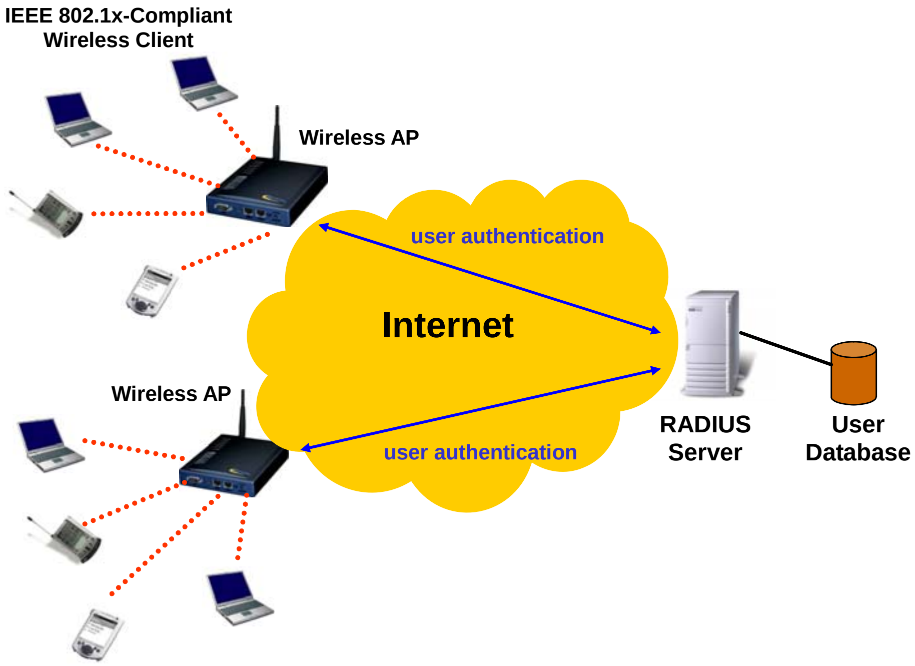
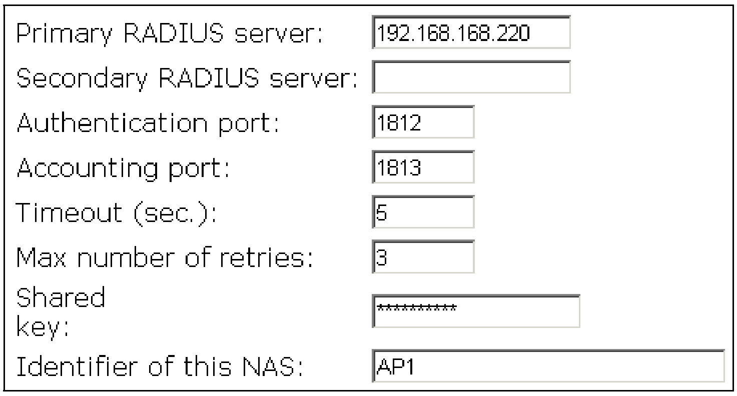


Fig. 49: IEEE 802.1x and RADIUS

An 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. You 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:	AP1

Fig. 50: IEEE 802.1x/RADIUS settings

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

3.6. Configuring Advanced Settings

3.6.1. Packet Filters

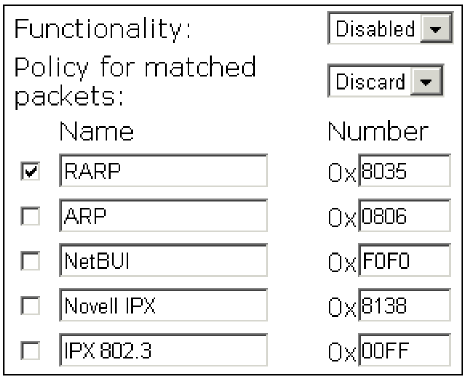
The IEEE 802.11b/g provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

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

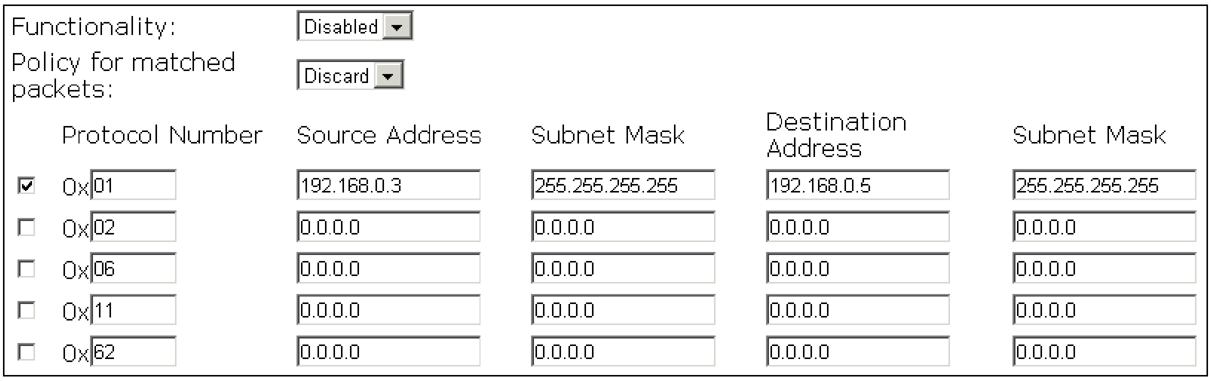
Policy for matched packets: Discard

	Name	Number
☑	RARP	0x 8035
□	ARP	0x 0806
□	NetBUI	0x F0F0
□	Novell IPX	0x 8138
□	IPX 802.3	0x 00FF

Fig. 51: 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

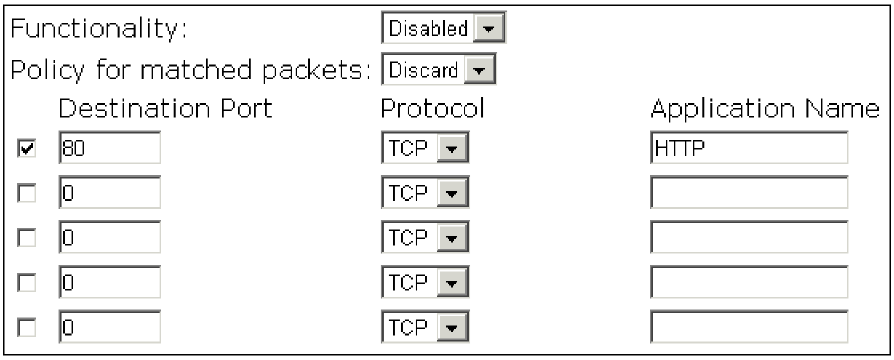
	Protocol Number	Source Address	Subnet Mask	Destination Address	Subnet Mask
☑	0x01	192.168.0.3	255.255.255.255	192.168.0.5	255.255.255.255
□	0x02	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
□	0x06	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
□	0x11	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
□	0x62	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Fig. 52: 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

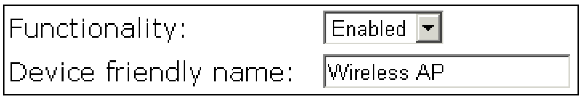
	Destination Port	Protocol	Application Name
☑	80	TCP	HTTP
□	0	TCP	
□	0	TCP	
□	0	TCP	
□	0	TCP	

Fig. 53: 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



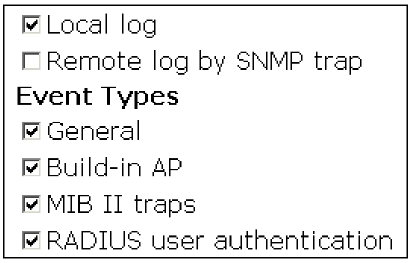
Functionality: Enabled

Device friendly name: Wireless AP

Fig. 54: 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 IEEE 802.11b/g in My Network Places of Windows XP. The IEEE 802.11b/g 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 IEEE 802.11b/g will launch the default Web browser for you to configure the AP.

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. 55: System log settings

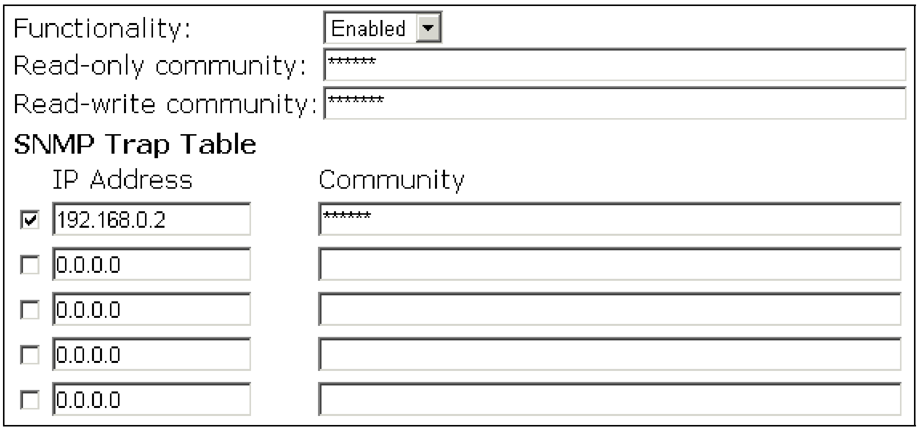
System events can be logged to the on-board RAM of the IEEE 802.11b/g (**Local log**) or sent to a remote computer on which an SNMP trap monitor program runs (**Remote log by SNMP trap**). See the next subsection for more information about SNMP trap settings.

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 IEEE 802.11b/g 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. 56: 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 **Default** (**SF-Reset**, or **Soft-Reset**) switch on the housing of a *powered-on* IEEE 802.11b/g to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
IEEE 802.11g	
Regulatory Domain	FCC (U.S.)
Channel Number	11
SSID	wireless
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	High
MAC Address	See the label on the accompanying PCMCIA card or the label on the housing of the AP.
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
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Wireless Client Isolation	Disabled
AP Load balancing	Disabled
Link Integrity	Disabled
Association Control	
Max Number of Clients	64
Block Clients if Traffic Load Exceeds	Disabled
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
DHCP Server	Disabled
Management	
UPnP	Enabled
System Log	Local Log
SNMP	Enabled
SNMP read community	public
SNMP write community	private
Telnet	Enabled

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the IEEE 802.11b/g is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the IEEE 802.11b/g.

- Make sure that the LED ALV of the IEEE 802.11b/g is blinking to indicate the IEEE 802.11b/g is working.

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

B-1: Wireless Settings Problems

- **The wireless client computer cannot associate with an IEEE 802.11b/g.**
  - Is the wireless client set in *infrastructure* mode?
    - Check the *operating mode* of the WLAN NIC.
  - Is the SSID of the WLAN NIC identical to that of the prospective AP?
    - Check the SSID setting of the WLAN NIC and of the IEEE 802.11b/g.
  - Is the WEP functionality of the prospective IEEE 802.11b/g enabled?
    - Make appropriate WEP settings of the client computer to match those of the IEEE 802.11b/g.
  - Is the prospective IEEE 802.11b/g within range of wireless communication?
    - Check the *signal strength* and *link quality* sensed by the WLAN NIC.

B-2: TCP/IP Settings Problems

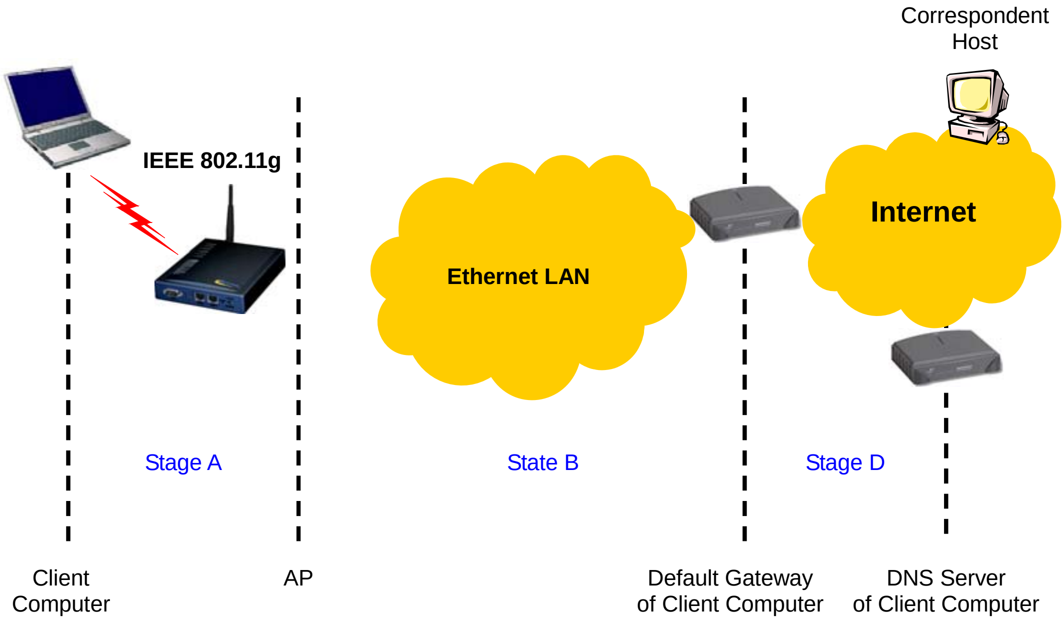


Fig. 57: Communication stages for a client to reach its correspondent host

For a wireless client computer to communicate with a correspondent host on the Internet by the host's domain name (e.g. http://www.wi-fi.com), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the AP, then the IEEE 802.11b/g relays this request to the default gateway of the client computer. Finally, this request is forwarded by the gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends further packets to this IP address.

As illustrated in Fig. 57, the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, **ping.exe**, can be employed to find out TCP/IP-related communication problems.

NOTE: If *two or more* NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the OS-provided command-line network tool, **route.exe**, to add or delete entries from the routing table. Or, use Windows-provided **Device Manager** to disable unnecessary NICs.

Solve the following problems in order:

- **The IEEE 802.11b/g does not respond to *ping* from the client computer.**
  - Are two or more NICs installed on the client computer?
    - Use the OS-provided command-line network tool, **route.exe**, to modify the contents of the routing table.
    - Use Windows-provided **Device Manager** to disable unnecessary NICs.
  - Is the underlying link (Ethernet or IEEE 802.11g) established?
    - Make sure the Ethernet link is OK.

    - ◆ Make sure the wireless settings of the wireless client computer and of the IEEE 802.11b/g match.

  - ■ Are the IP address of the *client computer* and the IP address of the *IEEE 802.11b/g* in the same IP subnet?

    - ◆ Use **WinIPCfg.exe** or **IPConfig.exe** to see the current IP address of the client computer. Make sure the IP address of the client computer and the IP address of the IEEE 802.11b/g are in the same IP subnet.

    - ◆ **TIP:** If you forget the current IP address of the AP, use Wireless Router/AP Browser to get the information (see Appendix B-3).

- ● **The default gateway of the client computer does not respond to *ping* from the client computer.**

  - ■ Solve the preceding problem first.

  - ■ Are the IP address of the *IEEE 802.11b/g* and the IP address of the *client computer* in the same IP subnet?

  - ■ If you cannot find any incorrect settings of the AP, the default gateway may be really down or there are other communication problems on the network backbone.

- ● **The DNS server(s) of the client computer do not respond to *ping* from the client computer.**

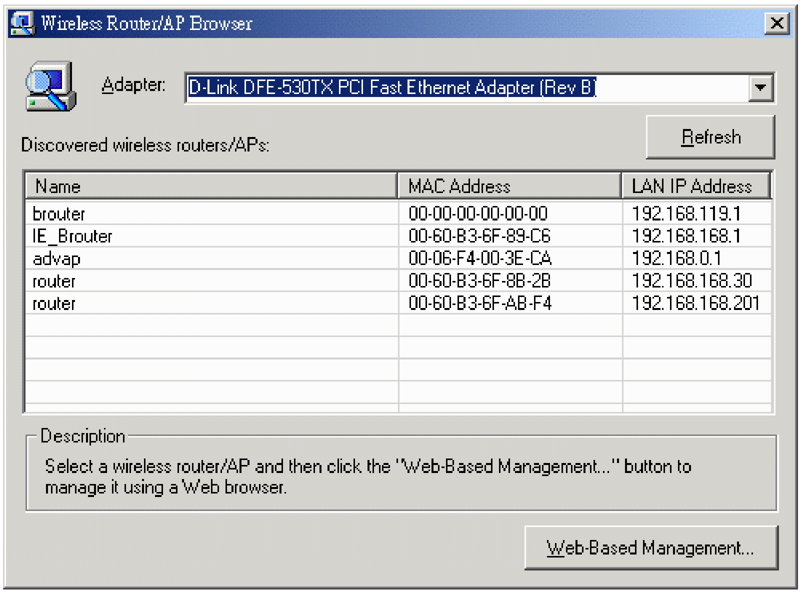
  - ■ Solve the preceding problems first.

  - ■ If you cannot find any incorrect settings of the AP, the default gateway of the IEEE 802.11b/g may be really down or there are other communication problems on the network backbone.

B-3: Unknown Problems

- ● **The IEEE 802.11b/g 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 APs 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. 58: Wireless Router/AP Browser

- **The IEEE 802.11b/g stops working and does not respond to Web management requests.**
  - The firmware of the IEEE 802.11b/g may be stuck in an incorrect state.
    - Unplug the power connector from the power jack, and then re-plug the connector to restart the AP.
    - Contact our technical support representatives to report this problem, so that the bugs can be static in future firmware versions.
  - If the IEEE 802.11b/g still does not work after restarting, there may be hardware component failures in the AP.
    - Contact our technical support representatives for repair.