

IEEE 802.11b/g Wireless Access Point/Bridge

User's Guide

Version: 1.4

Last Updated: 07/07/2009

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. Features	1
2. First-Time Installation and Configuration	4
2.1. Before you starting	4
2.2. Mounting the AP on a Wall	5
2.3. Preparing for Configuration	6
2.3.1. Connecting the Managing Computer and the AP	6
2.3.2. Changing the TCP/IP Settings of the Managing Computer	6
2.4. Configuring the AP	7
2.4.1. Entering the User Name and Password	7
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	10
2.4.5. Step 4: Reviewing and Applying Settings	11
2.5. Deploying the AP	11
2.6. Setting up Client Computers	13
2.6.1. Configuring IEEE 802.11g-Related Settings	13
2.6.2. Configuring TCP/IP-Related Settings	13
2.7. Confirming the Settings of the AP and Client Computers	13
2.7.1. Checking if the IEEE 802.11g-Related Settings Work	14
2.7.2. Checking if the TCP/IP-Related Settings Work	14
2.8. Using Web-Based Network Manager	15
2.8.1. Menu Structure	15
2.8.2. Save, Save & Restart, and Cancel Commands	16
2.8.3. Home and Refresh Commands	17
2.9. Viewing Status	17
2.9.1. Associated Wireless Clients	17
2.9.2. Current DHCP Mappings	18
2.9.3. System Log	18
2.9.4. Link Monitor	18
2.10. General Operations	19
2.10.1. Specifying Operational Mode	19
2.10.2. Changing Password	20
2.10.3. Managing Firmware	20
2.10.3.1. Upgrading Firmware by HTTP	20
2.10.3.2. Backing up and Restoring Configuration Settings by HTTP	21
2.10.3.3. Resetting Configuration to Factory Defaults	21
2.11. Configuring TCP/IP Related Settings	22
2.11.1. Addressing	22
2.11.2. DHCP Server	22
2.11.2.1. Basic	22
2.11.2.2. Static DHCP Mappings	23
2.12. Configuring IEEE 802.11b/g-Related Settings	23
2.12.1. Communication	23
2.12.1.1. Basic	23
2.12.1.2. Link Integrity	24
2.12.1.3. Association Control	24
2.12.1.4. AP Load Balancing	24
2.12.1.5. Wireless Distribution System	25
2.12.2. Security	27
2.12.2.1. Basic	28
2.12.2.2. MAC-Address-Based Access Control	30

2.12.3. IEEE 802.1x/RADIUS	31
2.13. Configuring Advanced Settings	32
2.13.1. Packet Filters	32
2.13.1.1. Ethernet Type Filters	32
2.13.1.2. IP Protocol Filters	33
2.13.1.3. TCP/UDP Port Filters	33
2.13.2. Management.....	34
2.13.2.1. UPnP	34
2.13.2.2. System Log	34
2.13.2.3. SNMP	35
Appendix A: Default Settings	36
Appendix B: Troubleshooting.....	37
B-1: Wireless Settings Problems	37
B-2: TCP/IP Settings Problems	38
B-3: Unknown Problems	39

1. Introduction

The IEEE 802.11b/g (900MHz) wireless access point (AP) enables IEEE 802.11b/g (900MHz) client computers to access the resources on the Ethernet network. With the sleek Web-based user interface, a network administrator can easily and clearly manage the AP. Following sections describe the installation steps, the configuration steps, and the explanation of Web management for the users to meet their needs.

1.1. Features

- **IEEE 802.11b/g**
 - **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/128-bit and 152-bit WEP (Wired Equivalent Privacy).** For authentication and data encryption.
 - **Enabling/disabling SSID broadcasts.** When the AP 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 AP 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 AP 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 AP 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 AP supports the WPA standard proposed by the Wi-Fi Alliance (<http://www.wi-fi.org>). Both WPA-PSK (Pre-Shared Key) mode and full WPA mode are supported. WPA is composed of TKIP (Temporal Key Integrity Protocol) and IEEE 802.1x and serves as a successor to WEP for better WLAN security.
 - **Repeater.** When the AP is in AP/Bridge mode, it can communicate with other APs or wireless bridges via WDS (Wireless Distribution System). Therefore, an AP can wirelessly

forward packets from wireless clients to another AP, and then the later AP forwards the packets to the Ethernet network.

- **Wireless client isolation.** When the AP 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 APs can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the APs. This function is available when the AP is in AP/Bridge mode.
- **Transmit power control.** Transmit power of the AP's RF module can be adjusted to change RF coverage of the AP.
- **Link integrity.** When the AP 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 AP and no wireless client can associate with it.
- **Association control.** When the AP is in AP/Bridge mode, it can be configured to deny association requests when it has served too many wireless clients or traffic load is too heavy.
- **Associated wireless clients status.** When the AP is in AP/Bridge mode, it can show the status of all wireless clients that are associated with the AP.
- **Detachable antennas.** The factory-mounted antennas can be replaced with high-gain antennas for different purposes.
- **DHCP client.** The AP can automatically obtain an IP address from a DHCP server.
- **DHCP server.** The AP 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 AP provides Layer 2, Layer 3, and Layer 4 filtering capabilities.
- **Firmware Tools**
 - **Firmware upgrade.** The AP can be upgraded by HTTP (Hepertext Transfer Protocol).
 - **Configuration backup.** The configuration settings of the AP can be backed up to a file via [HTTP](#) for later restoring.
 - **Configuration reset.** Resetting the configuration settings to factory-default values.
- **Management**
 - **Web-based Network Manager** for configuring and monitoring the AP via a Web browser. The management protocol is HTTP (Hepertext Transfer Protocol)-based.

- **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, and Private Enterprise MIB are supported.
- **UPnP.** The AP responds to UPnP discovery messages so that a Windows XP user can locate the AP in My Network Places and use a Web browser to configure it.
- **System log.** For system operational status monitoring.
 - ◆ **Local log.** System events are logged to the on-board RAM of the AP and can be viewed using a Web browser.
 - ◆ **Remote log by SNMP trap.** Systems events are sent in the form of SNMP traps to a remote SNMP management server.
- **Power over Ethernet (optional).** Supplying power to an AP over an Ethernet cable using PowerDsine (<http://www.powerdsine.com>) technology (IEEE 802.3af compliant in the future). This feature facilitates large-scale wireless LAN deployment.
- **Hardware Watchdog Timer.** If the firmware gets stuck in an invalid state, the hardware watchdog timer will detect this situation and restart the AP. This way, the AP can provide continuous services.

2. First-Time Installation and Configuration

2.1. Before you starting

After unpacking the package, make sure the following items are present and in good condition.

1. IWE1700-Ag × 1pcs
2. 1.2M 10/100Base-T/TX Ethernet Cable × 1pcs
3. Wall-Mounting Kit × 1pcs (include Wall Mount #1 and #2)
4. User's Guide CD × 1pcs



Fig. 1. IWE1700 Full Package

Accessories (OPTIONAL):

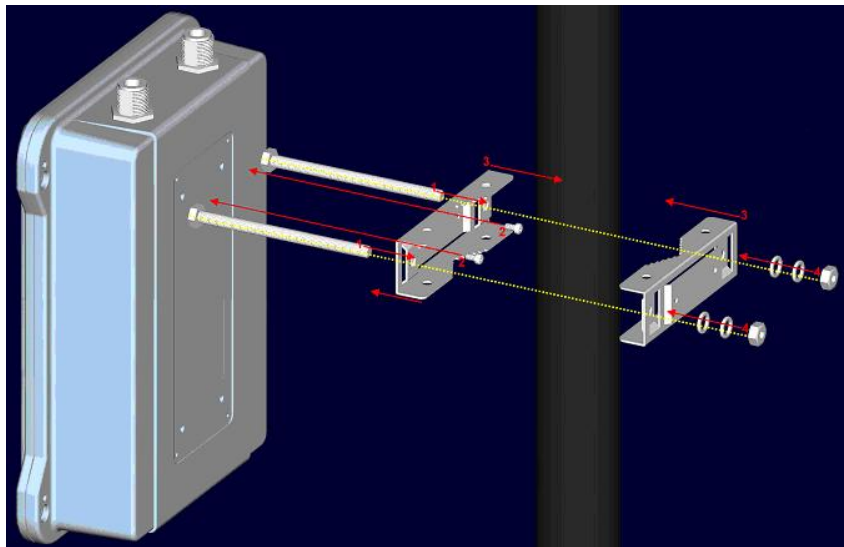
1. Power Injector × 1pcs
2. AC Power Cord × 1pcs
3. 25M Waterproof 10/100Base-T/TX Ethernet Cable × 1pcs



2.2. Mounting the AP on a Wall

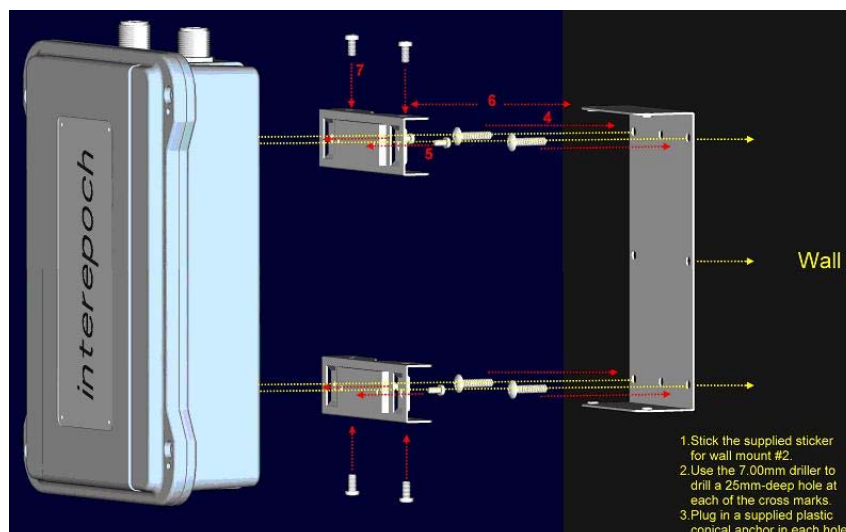
IWE with Wall Mount #1 Kit

1. Put the M6*90 screw into wall mount #1.
2. Fix the wall mount #1 to the bottom of IWE1700 by using M4*80 screw.
3. After finish step 2, put the IWE1700 to the pole with the wall mount #1 using M6*90 screw.
4. Use M6 screw set, including spring washer and nuts, to finish the installation.



IWE1700 with Wall Mount #2 Kit

1. Stick the supplied sticker for wall mount #2.
2. Use the 7.00mm driller to drill a 25mm-deep hole at each of the cross marks.
3. Plug in a supplied plastic conical anchor in each hole.
4. Screw a supplied ST3.9*20 screw in each plastic conical anchor for a proper depth so that the wireless AP can be hung on the screws.
5. Fix two wall mounts #1 to the bottom of IWE1700 by using two M4*80 screws.
6. After fix wall mount #1 and #2, please see the diagram to align wall mount #1 and #2.
7. Fix the wall mount #1 and #2 together using M4*80 screw to complete installation.



2.3. Preparing for Configuration

For you to configure an AP, 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 an AP, 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, you have to 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 AP 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 AP for first-time configuration, you have two choices as illustrated in Fig. 2.

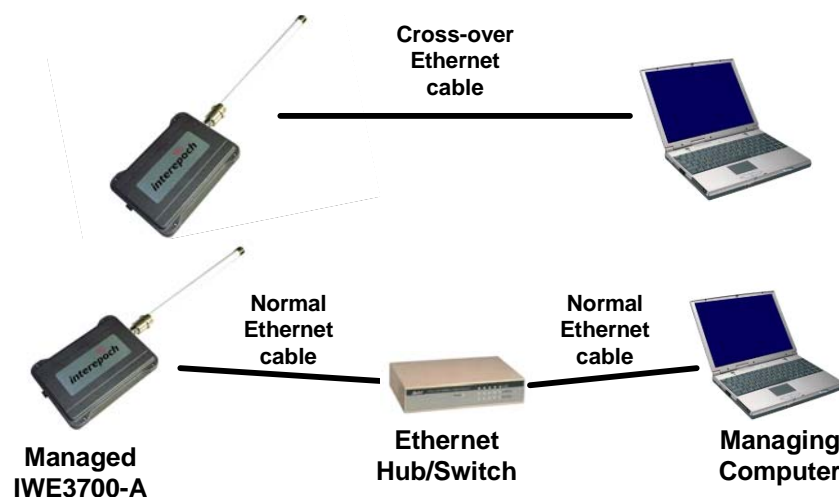


Fig. 2. Connecting a managing computer and an AP via Ethernet.

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

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

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

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

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

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

2.4. Configuring the 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* start page.

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

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.

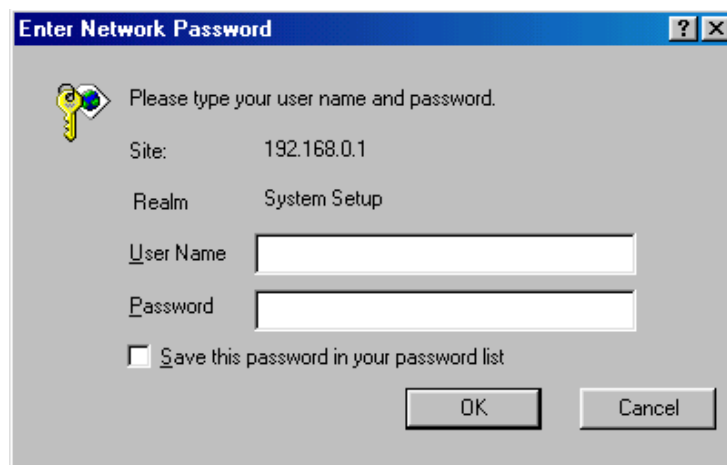


Fig. 3. Entering the user name and password.

NOTE: It is strongly recommended that the password be changed to other value for security reasons. On the start page, click the **General, Password** link to change the value of the password (see Section 2.10.2 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.

Web-Based Network Management

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

Bridge/AP Settings and Info	
Model:	AP adv
BIOS/Firmware version:	S91-01-0612/9.0.0.001
Release Date (MM/DD/YYYY):	03/20/2008
Operational Mode:	Access Point
MAC address:	00:09:92:10:00:0B
System up time (hr:min:sec):	0:01:04
TCP/IP Settings	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Default gateway:	192.168.0.254
IEEE802.1D (STP):	Disabled
Wireless LAN 1 Settings	
RF type:	11B/G Mixed
Channel number:	4
Network name (SSID):	wireless
Data rate:	auto
Security mode:	Open System
SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
MAC-address-based access control:	Disabled
Wi-Fi Multimedia(WMM) Functionality:	Disabled
Link integrity:	Disabled
Reference host:	0.0.0.0
Number of WLAN1 WDS links:	0
DHCP Server Settings	
DHCP server is disabled.	
Advanced Settings	
Web-based management port:	80
SNMP:	Enabled
UPNP:	Enabled
Ack Timeout	
Distance:	5000 meters

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 modes 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 AP supports 2 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 AP 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 APs. 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:

Table 1. Operational modes vs. wireless link types.

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

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 2.12.1.5 for more information). To establish a *dynamic* bridge link between an AP and an AP Client, both devices have to be configured with the same SSID and WEP settings. The AP Client automatically scans for any AP that is using the matched SSID and establishes a bridge link with the scanned AP.

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 AP 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

Basic	
RF type:	11B/G Mixed ▾
Channel number:	4 (907 MHz) ▾
SSID:	wireless
Data rate:	Auto ▾
Transmit Power (dBm) :	High ▾

Fig. 7. IEEE 802.11g communication settings.

Go to the **IEEE 802.11 / Communication** to configure IEEE 802.11b/g-related communication settings, including **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 AP 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

Restart **Cancel** The settings have been changed. Click **Restart** to restart the device for the settings to take effect.

Bridge/AP Settings and Info	
Model:	AP adv
BIOS/Firmware version:	S91-01-0612/9.0.0.004
Release Date:	2009/6/5
Operational Mode:	Access Point
MAC address:	00:15:61:10:0A:43
System up time (day:hr:min:sec):	0:0:01:34
TCP/IP Settings	
IP address:	192.168.0.168
Subnet mask:	255.255.255.0
Default gateway:	192.168.0.254
DNS:	168.95.1.1
IEEE802.1D (STP):	Enabled
Wireless LAN 1 Settings "AP/MSSID"	
RF type:	11B/G Mixed
Channel number:	6
Network name (SSID):	wireless66
Data rate:	auto
Transmit Power:	High
DTIM:	3
Security mode:	Open System
SSID broadcasts:	Enabled

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 AP for the new settings to take effect.

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

2.5. Deploying the AP

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

If you are configuring a pair of the APs 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 data 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, 54Mbps, because of the distance and the gain of the antennas.

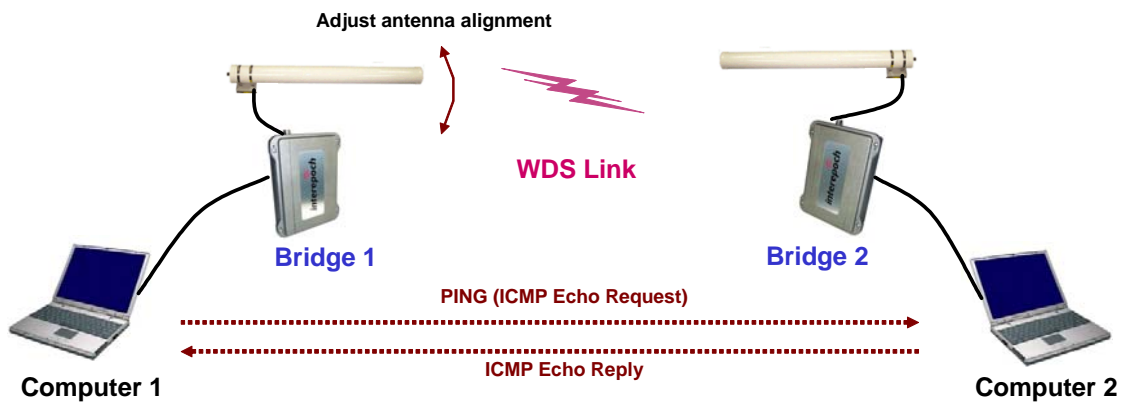


Fig. 9. Adjusting alignments of external directional antennas.

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

TIP: If you are doing *dynamic* bridging, you can use the Link Monitor feature on the AP Client side to help you align the directional antennas. Refer to Section 2.9.4 for more information.

Current Linking Status

Not Connected

Signal Strength			
Signal(dBm)	Noise(dBm)	SNR	Strength (%)
-95	-96	0	0%

Detect.. ■■■

Home
Refresh

Fig. 10. Link monitor.

2.6. Setting up Client Computers

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

2.6.1. Configuring IEEE 802.11g-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 AP.

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 AP must be identical. Or, in case the **SSID broadcasts** capability of the AP is enabled (by default), the SSID of the wireless client computer could be set to “any”.

NOTE: Both the wireless client computer and the AP must have the same WEP settings for them to communicate with each other.

NOTE: For better wireless security, IEEE 802.1x capability of the AP 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 AP 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 AP and Client Computers

After you have completed deploying the AP and setting up client computers, you have to make sure the settings you have made are correct.

2.7.1. Checking if the IEEE 802.11g-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 AP.

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 AP 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.

2.8. Using Web-Based Network Manager

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

Bridge/AP Settings and Info	
Model:	AP adv
BIOS/Firmware version:	S91-01-0612/9.0.0.004
Release Date:	2009/6/5
Operational Mode:	Access Point
MAC address:	00:15:61:10:0A:43
System up time (day:hr:min:sec):	0:0:04:50

TCP/IP Settings	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Default gateway:	192.168.0.254
DNS:	168.95.1.1
IEEE802.1D (STP):	Enabled

Wireless LAN 1 Settings "AP/MSSID"	
RF type:	11B/G Mixed
Channel number:	4
Network name (SSID):	wireless
Data rate:	auto
Transmit Power:	High
DTIM:	3
Security mode:	Open System
SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
MAC-address-based access control:	Disabled
Wi-Fi Multimedia(WMM) Functionality:	Disabled
Distance:	5000
Active MSSID Number:	0
Number of WLAN1 WDS links:	0

Wireless Miscellaneous	
Link integrity:	Disabled
Reference host:	0.0.0.0
Max number of clients:	64
Block clients if traffic load exceeds:	Disabled
AP Load Balancing Functionality :	Disabled

DHCP Server Settings	
DHCP server is disabled.	

Advanced Settings	
Web-based management port:	80
SNMP:	Enabled
UPNP:	Enabled

Fig. 11. The Start page.

2.8.1. 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 AP 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 AP—*AP/Bridge* or *AP Client*.
 - **Password.** For gaining rights to change the settings of the AP.
 - **Firmware Tools.** For upgrading the firmware of the AP, backing up and restoring configuration, and configuration reset settings of the AP.
- **TCP/IP.** TCP/IP-related settings.
 - **Addressing.** IP address settings for the AP to work with TCP/IP.
 - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the AP.
- **IEEE 802.11.** IEEE 802.11g-related settings.
 - **Communication.** Basic settings for the IEEE 802.11g interface of the AP 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 AP.
 - **Packet Filters.** Ethernet Type Filters, IP Protocol Filters, and TCP/UDP Port Filters settings.
 - **Management.** UPnP, System Log, and SNMP settings.

2.8.2. Save, Save & Restart, and Cancel Commands



Fig. 12. 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 AP and brings you back to the start page. Clicking **Save & Restart** stores the settings changes to the memory of the AP and restarts the AP 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 AP for the settings changes to take effect.

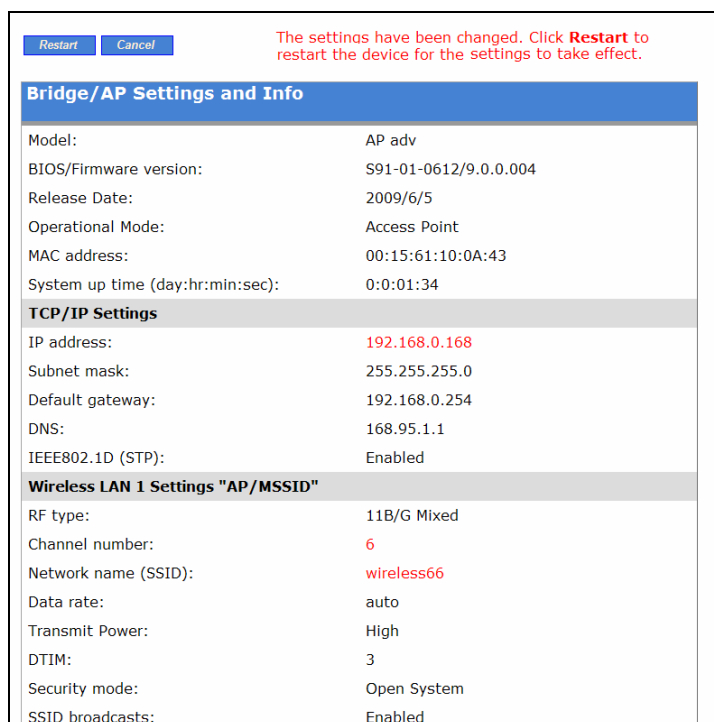


Fig. 13. Settings have been changed.

2.8.3. Home and Refresh Commands



Fig. 14. 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.

2.9. Viewing Status

2.9.1. Associated Wireless Clients

Associated Wireless Clients						
Wireless Clients Status						
No.	MAC Address	Tx Bytes	Rx Bytes	Rate	RSSI	Last Activity Time (secs)
1	00:0a:79:6b:1c:02	2939	10961	11 Mbps	1	22.12

Fig. 15. 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.

2.9.2. 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. 16. 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 2.11.2). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool specified by the **First allocateable IP address** and **Allocateable IP address count** settings on the **DHCP Server** configuration page.

2.9.3. System Log

Model:	AP adv
BIOS/Firmware version:	S91-01-0612/9.0.0.004
Operational Mode:	Access Point
Current time:	2009年6月6日 上午 11:47:38
<p>2009年6月6日 上午 11:46:43 SYSTEM START UP! 2009年6月6日 上午 11:46:43 Wireless LAN interface initializes success. 2009年6月6日 上午 11:46:43 Mac address --> 00:15:61:10:0A:43 2009年6月6日 上午 11:46:44 LAN IP address --> 192.168.0.1 2009年6月6日 上午 11:46:46 Wireless client:00:0a:79:6b:1c:02 associate</p>	

Fig. 17. System log.

System events are recorded in the memory of the AP. The logged information is useful for troubleshooting purposes. The system events are divided into several categories, and you can select which categories of events to log. See Section 2.13.2.2 for more information.

2.9.4. Link Monitor

Signal Strength			
Signal(dBm)	Noise(dBm)	SNR	Strength (%)
-95	-96	0	0%

Detect.. ■■■

[Home](#) [Refresh](#)

Fig. 18. Link monitor.

When the AP is in *AP Client* mode, you can use the Link Monitor status page to monitor the 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. Refer to Section 2.5 for more information about antenna alignment.

NOTE: The values are updated every 20 seconds.

2.10. General Operations

2.10.1. Specifying Operational Mode

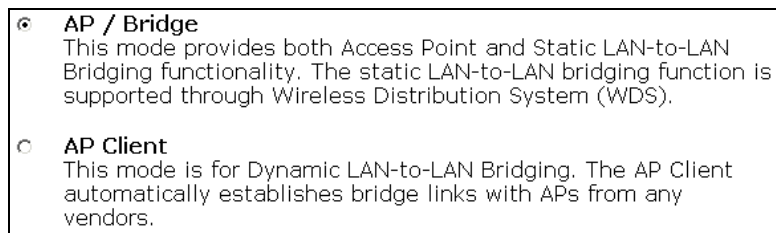


Fig. 19. Operational modes settings.

The AP supports 2 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 AP 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 APs. 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	

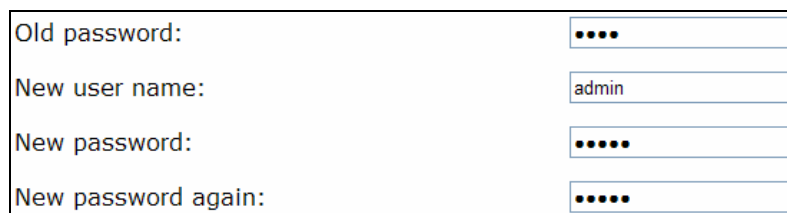
Table 2. Operational modes vs. wireless link types.

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 2.12.1.5 for more information). To establish a *dynamic* bridge link between an AP and an AP Client, both devices have to be configured with the same SSID and WEP settings. The AP Client automatically scans for any AP that is using the matched SSID and establishes a bridge link with the scanned AP.

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 AP 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.

2.10.2. Changing Password



A screenshot of a web form for changing the password. It contains four input fields: 'Old password:' with four dots, 'New user name:' with the text 'admin', 'New password:' with four dots, and 'New password again:' with four dots.

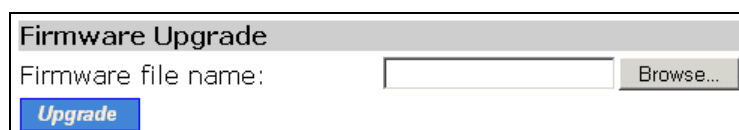
Fig. 20. Password.

On this page, you can change the user name and password for the right to modify the configuration of the bridge. The new password must be typed twice for confirmation.

2.10.3. Managing Firmware

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

2.10.3.1. Upgrading Firmware by HTTP



A screenshot of a web form titled 'Firmware Upgrade'. It has a text input field for 'Firmware file name:' followed by a 'Browse...' button. Below the input field is a blue 'Upgrade' button.

Fig. 21. Firmware upgrade by HTTP.

To upgrade firmware of the AP 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.

2.10.3.2. Backing up and Restoring Configuration Settings by HTTP

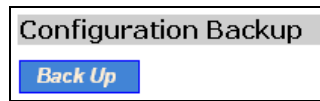


Fig. 22. Firmware backup by HTTP.

To back up configuration of the AP 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 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". 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.

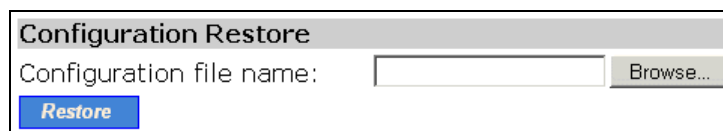


Fig. 23. Configuration restore by HTTP.

To restore configuration of the AP 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 AP.

2.10.3.3. Resetting Configuration to Factory Defaults

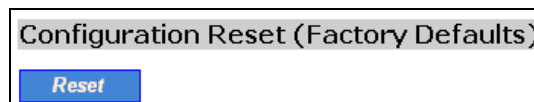


Fig. 24. Configuration reset.

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.

2.11. Configuring TCP/IP Related Settings

2.11.1. Addressing

Method of obtaining an IP address:	Set Manually
IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Default gateway:	192.168.0.254
Host name:	test
Domain (DNS suffix):	domain.com
IEEE802.1D (Spanning Tree Protocol):	Disabled

Fig. 25. TCP/IP settings.

The IP address of the AP 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 AP.

2.11.2. DHCP Server

2.11.2.1. 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:	192.168.0.10
First allocatable IP address:	192.168.0.100
Allocatable IP address count:	100
Lease time (Hours):	24

Fig. 26. Basic DHCP server settings.

The AP 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 allocatable 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 AP.

NOTE: By default the DHCP server function is disabled.

2.11.2.2. Static DHCP Mappings

Enabled	Desc.	MAC Address	IP Address
<input type="checkbox"/>	David	00:09:92:11:a1:be	192.168.0.5
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Fig. 27. 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.

2.12. Configuring IEEE 802.11b/g-Related Settings

2.12.1. Communication

2.12.1.1. Basic

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

RF type:	11B/G Mixed
Channel number:	4
Network name (SSID):	wireless
Data rate:	auto
Transmit Power:	High

Fig. 28. Basic IEEE 802.11b/g mixed communication settings.

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

The RF type of the WLAN interface can be configured to work in IEEE 802.11 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 AP 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 AP can be adjusted so that the RF coverage of the AP can be changed.

2.12.1.2. Link Integrity

Functionality:	Disabled ▾
Reference host:	0.0.0.0

Fig. 29. Link integrity settings.

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

2.12.1.3. Association Control

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

Fig. 30. Association control settings.

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

2.12.1.4. AP Load Balancing

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

Fig. 31. AP load balancing settings.

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

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

2.12.1.5. Wireless Distribution System

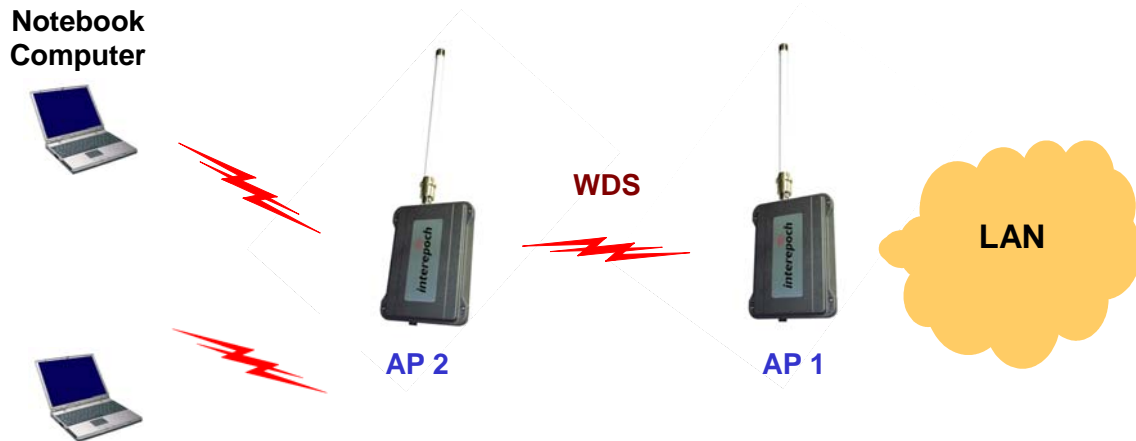


Fig. 32. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 32, 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. 33. LAN-to-LAN bridging.

By WDS, two or more LAN segments can be connected wirelessly. As illustrated in Fig. 33, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the AP is WDS-enabled, it can be used as a wireless bridge.

NOTE: An AP can have up to 6 WDS links to other APs or wireless bridges.

Port	Enabled	Peer MAC Address
1	<input type="checkbox"/>	00-02-6F-01-62-C5
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	

Fig. 34. Wireless Distribution System settings.

To enable a WDS link:

1. Specify the MAC address of the AP at the other end of the WDS link.
2. Select the corresponding **Enabled** check box.

For example, assume you want two APs with MAC addresses 00:02:65:01:62:C5 and 00:02:65:01:62:C6 to establish a WDS link between them. On AP 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 AP is connected to other peer APs 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.

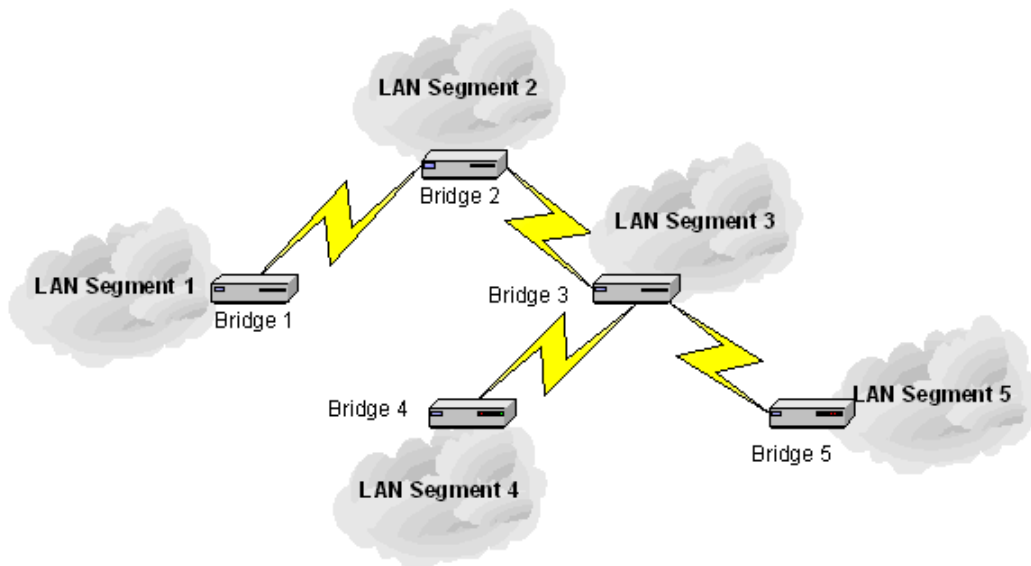
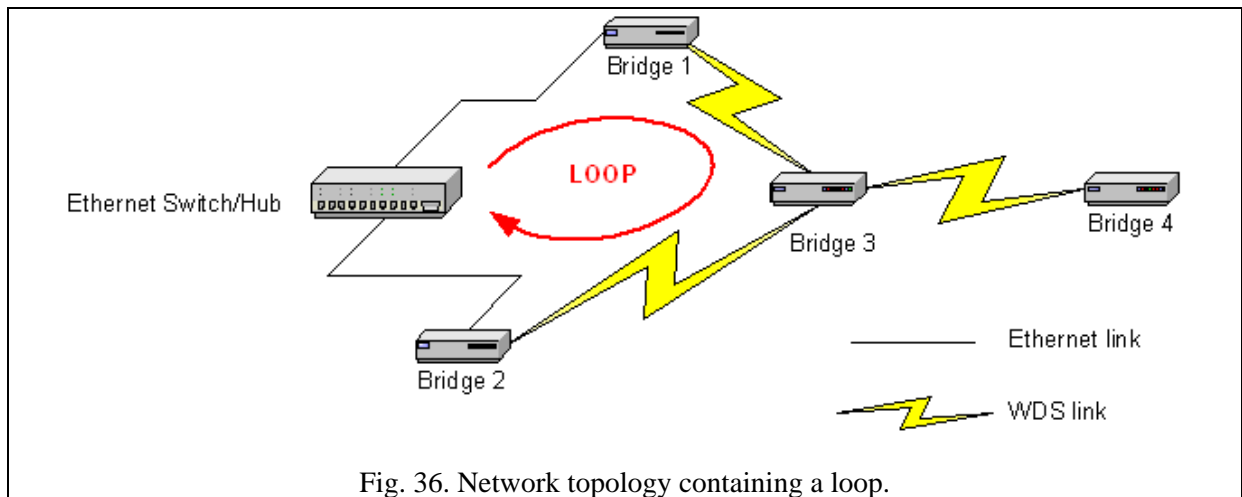


Fig. 35. Sample wireless bridge network topology.

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.



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 data 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. 37 illustrates the idea.

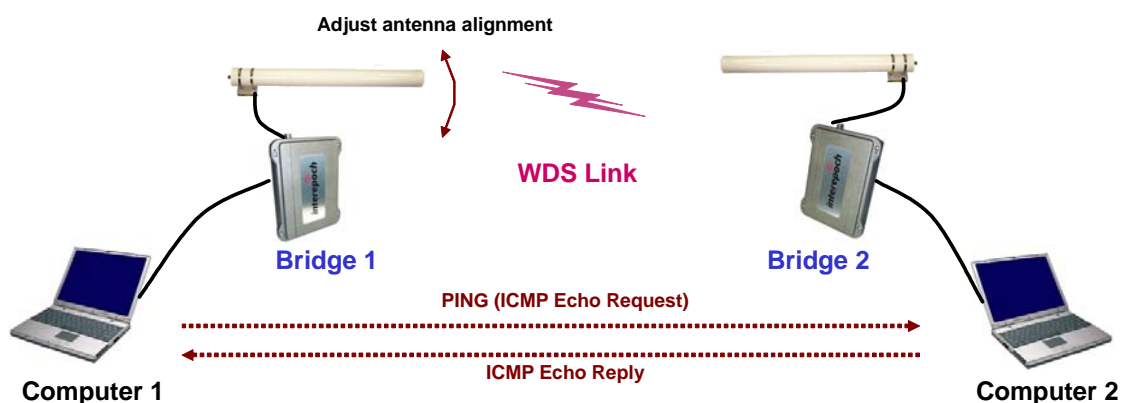


Fig. 37. Adjusting alignments of external directional antennas.

2.12.2. 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**.

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

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients (STAs) of this AP cannot see each other, and wireless-to-wireless traffic between the STAs is blocked. When the setting is set to **All APs in This Subnet**, traffic among wireless users of different APs in the same IP subnet is blocked. The behaviors are illustrated in the following figures.

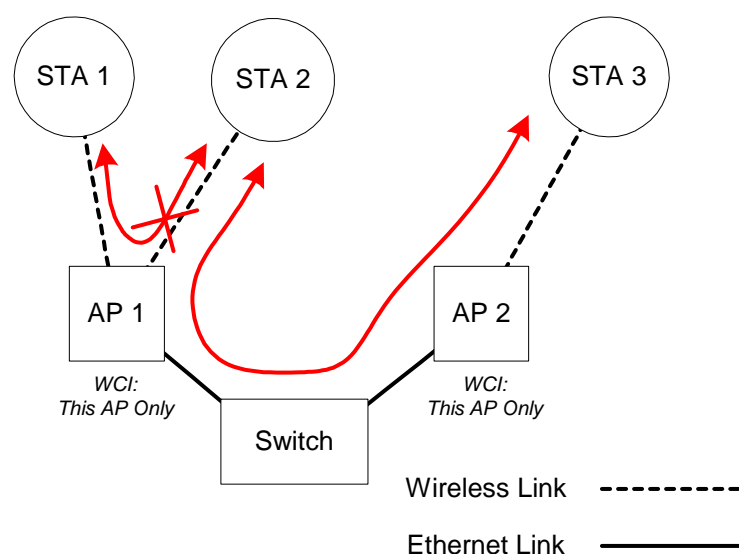


Fig. 39. Behavior of the "This AP Only" wireless client isolation option.

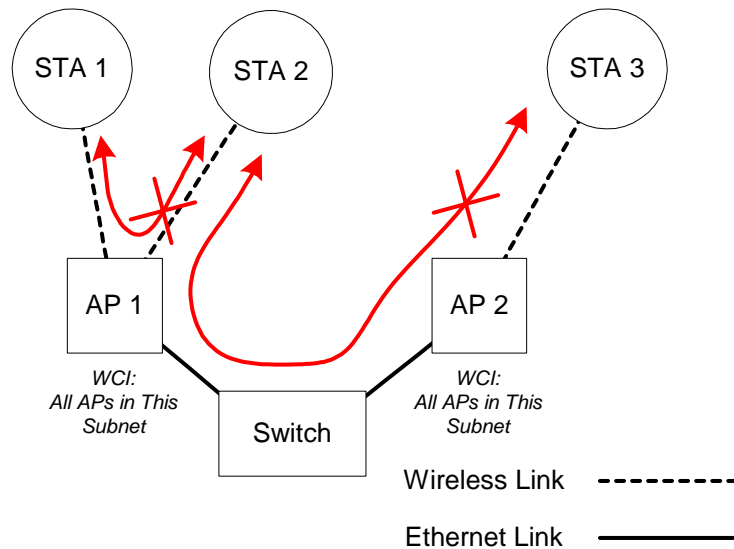


Fig. 40. Behavior of the “All APs on This Subnet” wireless client isolation option.

As illustrated in Fig. 39 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. 40, AP 1 and AP 2 communicates with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

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

- **Open System.** No authentication, no data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.
- **Static TKIP (WPA-PSK).** Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you have to specify the **Pre-shared key**, which will be used by the TKIP engine as a *master key* to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

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

- **IEEE 802.1x EAP without Encryption (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. No data encryption.
- **IEEE 802.1x EAP with Static WEP (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. Data encryption is achieved by static WEP.
- **IEEE 802.1x EAP with Dynamic WEP (EAP-TLS, EAP-TTLS, PEAP).** The IEEE 802.1x functionality is enabled and dynamic WEP key distribution authentication (EAP-TLS, EAP-TTLS, or PEAP) is used. Data encryption is achieved by dynamic WEP.
- **IEEE 802.1x EAP with Dynamic TKIP (WPA).** This is a full WPA mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The AP is highly secured in this mode.

In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1x functionality is enabled. See Section 2.12.3 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**, **128Bits** or **152 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

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

2.12.2.2. MAC-Address-Based Access Control

The screenshot shows a configuration window for MAC-address-based access control. At the top, 'Functionality' is set to 'Enabled' in a dropdown menu. Below it, 'Access control type' has two radio buttons: 'inclusive' (which is selected) and 'exclusive'. There is an empty text input field followed by an 'Add' button. Below this, the 'MAC address format' is set to '00-02-DD-30-03-1E'. A table with two columns, 'MAC Address' and 'Delete', contains two rows of data:

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

Fig. 41. 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 AP. When the table type is set to *inclusive*, entries in the table are permitted to associate with the AP. When the table type is set to *exclusive*, entries in the table are not permitted to associate with the AP.

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.

2.12.3. 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 2.12.2.1). 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.

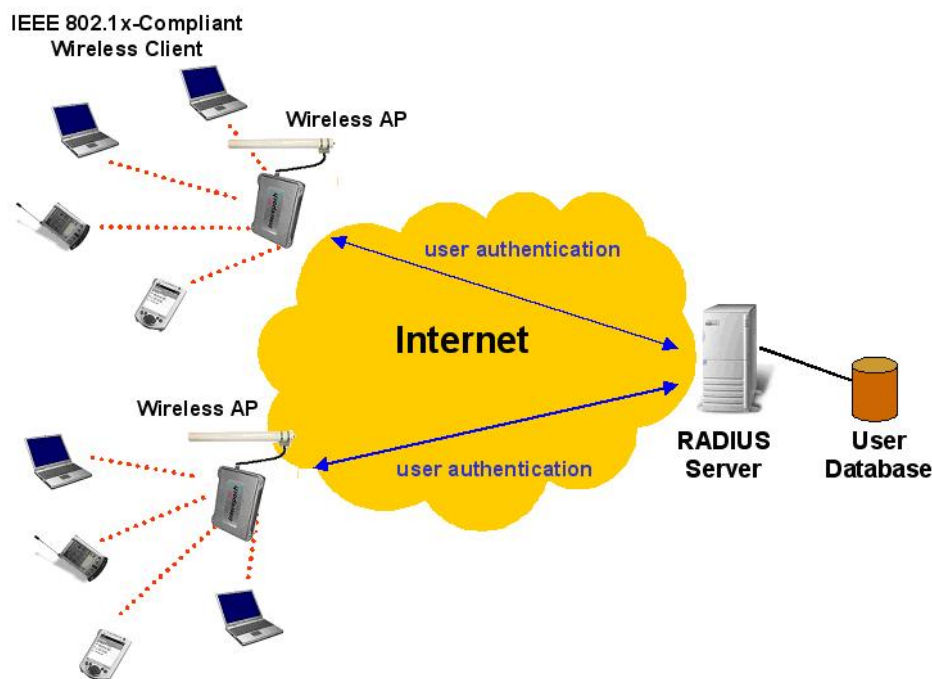


Fig. 42. IEEE 802.1x and RADIUS.

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. 43. 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.

2.13. Configuring Advanced Settings

2.13.1. Packet Filters

The AP 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.

2.13.1.1. Ethernet Type Filters

Functionality:	Disabled	
Policy for matched packets:	Discard	
	Name	Number
<input checked="" type="checkbox"/>	RARP	0x8035
<input type="checkbox"/>	ARP	0x0806
<input type="checkbox"/>	NetBUI	0xF0F0
<input type="checkbox"/>	Novell IPX	0x8138
<input type="checkbox"/>	IPX 802.3	0x00FF

Fig. 44. Ethernet type filters settings.

The *Ethernet type* field 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.

2.13.1.2. IP Protocol Filters

Functionality:	Disabled				
Policy for matched packets:	Discard				
	Protocol Number	Source Address	Subnet Mask	Destination Address	Subnet Mask
<input checked="" type="checkbox"/>	0x01	192.168.0.3	255.255.255.255	192.168.0.5	255.255.255.255
<input type="checkbox"/>	0x02	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/>	0x06	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/>	0x11	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/>	0x62	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Fig. 45. 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.

2.13.1.3. TCP/UDP Port Filters

Functionality:	Disabled		
Policy for matched packets:	Discard		
	Destination Port	Protocol	Application Name
<input checked="" type="checkbox"/>	80	TCP	HTTP
<input type="checkbox"/>	0	TCP	
<input type="checkbox"/>	0	TCP	
<input type="checkbox"/>	0	TCP	
<input type="checkbox"/>	0	TCP	

Fig. 46. 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**).

2.13.2. Management

2.13.2.1. UPnP

Functionality:	Enabled ▾
Device friendly name:	Wireless AP

Fig. 47. 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 AP in My Network Places of Windows XP. The AP 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 AP will launch the default Web browser for you to configure the AP.

2.13.2.2. System Log

<input checked="" type="checkbox"/> Local log
<input type="checkbox"/> Remote log by SNMP trap
Event Types
<input checked="" type="checkbox"/> General
<input checked="" type="checkbox"/> Build-in AP
<input checked="" type="checkbox"/> MIB II traps
<input checked="" type="checkbox"/> RADIUS user authentication

Fig. 48. System log settings.

System events can be logged to the on-board RAM of the AP (**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 AP via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (*disabled* by default).

2.13.2.3. SNMP

Functionality:	Enabled ▾
Read-only community:	*****
Read-write community:	*****
SNMP Trap Table	
IP Address	Community
<input checked="" type="checkbox"/> 192.168.0.2	*****
<input type="checkbox"/> 0.0.0.0	
<input type="checkbox"/> 0.0.0.0	
<input type="checkbox"/> 0.0.0.0	
<input type="checkbox"/> 0.0.0.0	

Fig. 49. 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* AP to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
IEEE 802.11b/g	
Channel Number	4
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

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the AP is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the AP.
- Make sure that the LED ALV of the AP is blinking to indicate the AP 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 AP.**
 - 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 AP.
 - Is the WEP functionality of the prospective AP enabled?
 - ◆ Make appropriate WEP settings of the client computer to match those of the AP.
 - Is the prospective AP within range of wireless communication?
 - ◆ Check the *signal strength* and *link quality* sensed by the WLAN NIC.

B-2: TCP/IP Settings Problems

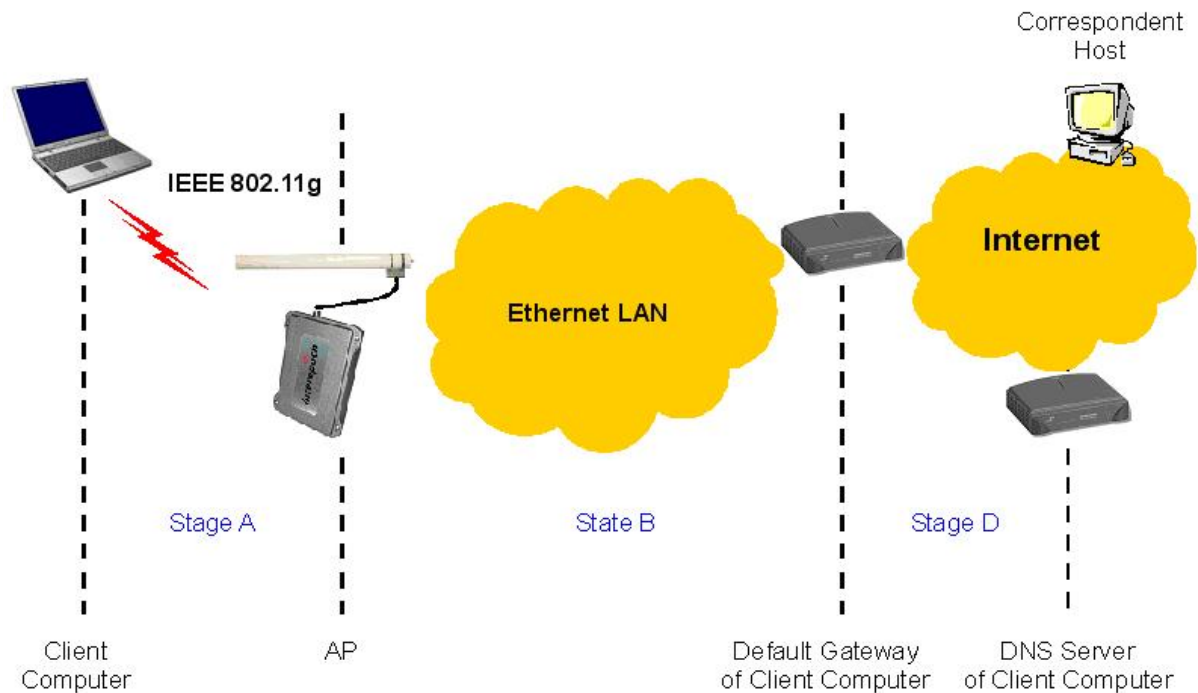


Fig. 50. Communication stages for a client to reach its correspondent host.

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 AP 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. 50, 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 AP 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 AP match.
- Are the IP address of the *client computer* and the IP address of the *AP* 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 AP 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 *AP* 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 AP may be really down or there are other communication problems on the network backbone.

B-3: Unknown Problems

- **The AP 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 (**WLBrsr.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.

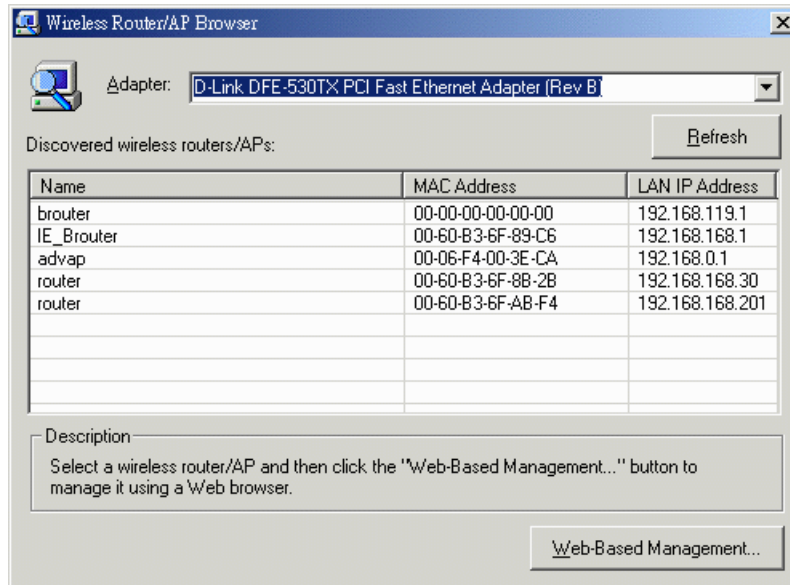


Fig. 51. Wireless Router/AP Browser.

- **The AP stops working and does not respond to Web management requests.**
 - The firmware of the AP 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 AP still does not work after restarting, there may be hardware component failures in the AP.
 - ◆ Contact our technical support representatives for repair.