

Wireless Internet Access Server Appliance

User's Guide

Version: 2.4

Last Updated: 09/026/2002

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 radiate 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, 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

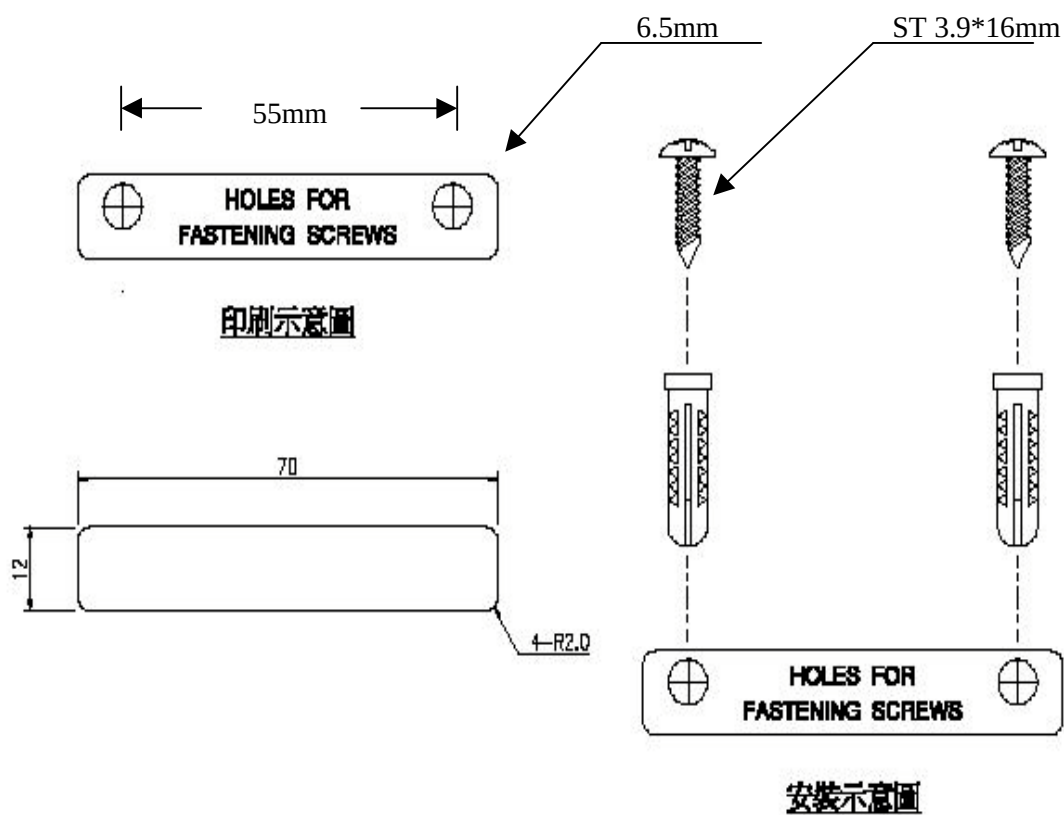
The ETSI version of this device is intended for home and office use in Austria, France (with Frequency channel restrictions). Germany , Italy ,Spain ,The Netherlands, United Kingdom.

Potential restrictive use

France: Only channels 10,11,12 ,and 13

Mounting instruction

1. Stick the accessorial sticker for wall-mounting on the wall.
2. Use a $\phi 6.5\text{mm}$ drill to drill a 25mm-deep hole at each of the cross marks.
3. Plug in an accessorial plastic conical anchor in each hole.
4. Screw an accessorial screw in each plastic conical anchor for a proper depth so that the wireless AP can be hung on the screws.
5. Hang the wireless AP on the screws.



Power Selection.

The AP can be powered by the supplied power adapter or POE (Power over Ethernet). The AP automatically selects the suitable one depending on the user's decision.

To power the AP 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.

Power Supply Selection Instruction - This product intended to be supplied by a Listed Power Unit, marked "Class 2" or "LPS" and output rated 5 V 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 an active Ethernet switch which can supply power over Ethernet.
2. Plug the other connector of the Ethernet cable to the **LAN / Config** port of the AP.

Table of Contents

Power Selection	iv
1. Introduction	1
1.1. Overview	1
1.2. Features	1
2. First-Time Installation and Configuration	2
2.1. Preparing for Configuration	2
2.1.1. Connecting the Managing Computer and the AP	3
2.1.2. Changing the TCP/IP Settings of the Managing Computer	3
2.2. Configuring the AP	3
2.2.1. Entering the User Name and Password	4
2.2.2. Step 1: Configure TCP/IP Settings	5
2.2.3. Step 2: Configure IEEE 802.11 Settings	6
2.2.4. Step 3: Review and Apply Settings	6
2.3. Deploying the AP	7
2.4. Setting up Client Computers	7
2.4.1. Configuring IEEE 802.11b-Related Settings	7
2.4.2. Configuring TCP/IP-Related Settings	7
2.5. Confirming the Settings of the AP and Client Computers	8
2.5.1. Checking if the IEEE 802.11b-Related Settings Work	8
2.5.2. Checking if the TCP/IP-Related Settings Work	8
3. Using Web-Based Network Manager	8
3.1. Overview	9
3.2. General Operations	11
3.2.1. Changing Password	11
3.2.2. Upgrading Firmware	11
3.3. Configuring TCP/IP Related Settings	13
3.3.1. Addressing	13
3.4. Configuring IEEE 802.11b-Related Settings	13
3.4.1. Communication	13
3.4.2. Security	14
3.4.3. IEEE 802.1x/RADIUS (Advanced Model)	15
3.5. Configuring Advanced Settings	17
3.5.1. Management	17
A-1: Default Settings	18
A-2: LED Definitions	18
Appendix B: Troubleshooting	19
B-1: Wireless Settings Problems	19
B-2: TCP/IP Settings Problems	20
B-3: Unknown Problems	21

1. Introduction

1.1. Overview

The wireless access point (AP) enables IEEE 802.11b client computers to access the resources on the Ethernet network. The *Pro* and *Advanced* models are bundled with the Windows-based management software—Wireless Network Manager—for multiple AP management. The *Advanced* model supports IEEE 802.1x and RADIUS (Remote Authentication Dial-In User Service) for user-based authentication and dynamic encryption key distribution, thus it is suitable for enterprises that need strong data security and WISPs (Wireless Internet Service Providers) that need accounting and billing support.

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

1.2. Features

- **Configuration Reset.** Resetting the configuration settings to factory-set values.
- **IEEE 802.11b**
 - **Access point.** Bridging packets between the wireless IEEE 802.11b network interface and the wired Ethernet LAN interface.
 - **64-bit and 128-bit WEP (Wired Equivalent Privacy).** For authentication and data encryption.
 - **Enabling/disabling SSID broadcasts.** The user 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.** Blocking unauthorized wireless client computers based on MAC (Media Access Control) addresses.
 - **IEEE 802.1x/RADIUS (*Advanced* model).** User authentication and dynamic encryption key distribution can be achieved by IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service).
 - **Replaceable antennas (optional).** The factory-mounted antennas can be replaced with high-gain antennas for different purposes.
- **Management**
 - **Windows-based Wireless Network Manager (*Pro* and *Advanced* models)** for configuring, monitoring, and diagnosing the local computer and neighboring APs. The management protocol is MAC-based.
 - **Web-based Network Manager** for configuring and monitoring APs. The management

protocol is HTTP (HyperText Transfer Protocol)-based.

- **UPnP.** The AP responds to UPnP discovery messages so that a Windows XP user can locate the AP in the Network Neighborhood and use a Web browser to configure it.
- **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x (*Advanced* model), and InterEpoch Enterprise MIB are supported.
- **Power over Ethernet (optional).** Supplying power to an AP over an Ethernet cable (IEEE 802.3af compliant). 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. Accordingly, the AP can provide continuous services.

2. First-Time Installation and Configuration

If the AP supports PoE (Power over Ethernet), you can use an Ethernet switch hub that can supply power over Ethernet cables to power the AP.

2.1. Preparing for Configuration

For the user (or administrator) 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 **Pref-erences...**, 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, we 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 sub-net.**

2.1.1. Connecting the Managing Computer and the AP

To connect the Ethernet managing computer and the managed AP for first-time configuration, the user has two choices as illustrated in Fig. 1.

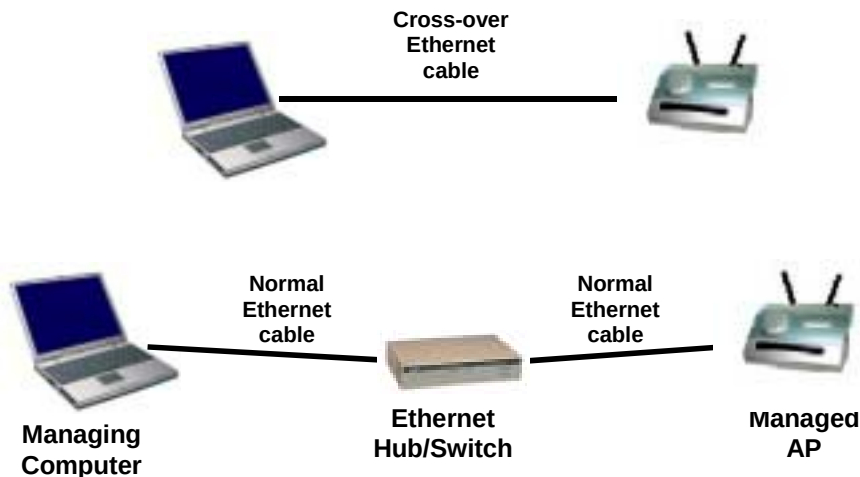


Fig. 1. Connecting a managing computer and an AP via Ethernet.

The user can use either a *cross-over* Ethernet cable (we have included one 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.

2.1.2. 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.

2.2. 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.

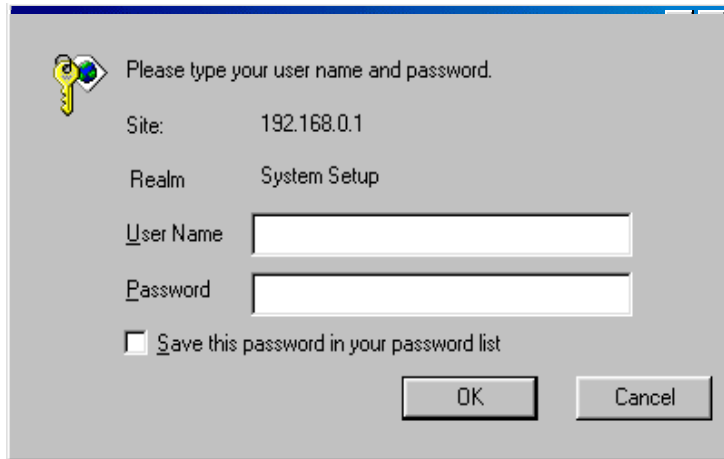
NOTE: If you are using the browser, *Opera* (from Opera Software), to configure an AP, click the menu item **File**, click **Preferences...**, click **File types**, and edit the MIME type, **text/html**, to add a file extension ".sht" so that Opera can work properly with the Web management pages of the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

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.

2.2.1. Entering the User Name and Password

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



Please type your user name and password.

Site: 192.168.0.1

Realm: System Setup

User Name:

Password:

☐ Save this password in your password list

OK Cancel

Fig. 2. Entering the user name and password.

NOTE: It is strongly recommended that the password be changed to other value for security reasons. On the start page, click the **General****Password** link to change the value of the password (see Section 3.2.1 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.

Access Point Settings and Info	
Model	AP Adv
BIOS/Firmware Version	APXS v1.20/1.4.1.2535
MAC Address (BSSID)	00-02-6F-01-62-C5
System Up Time (hr:min:sec)	0:04:12
TCP/IP Settings	LAN Interface - IP address: 192.168.0.1 - Subnet mask: 255.255.255.0 - Default gateway: 0.0.0.0
Wireless Settings	- Regulatory domain: FCC (U.S.) - Channel number: 11 - Transmission power: High - Network name (SSID): wireless - Security mode: Open System - SSID broadcasts: Enabled - MAC-address-based access control: Disabled
	Management UDP: Enabled

Fig. 3. The Start page.

2.2.2. Step 1: Configure TCP/IP Settings

Method of obtaining an IP address:	Set manually
IP address:	192.168.168.98
Subnet mask:	255.255.255.0
Default gateway:	192.168.168.1
Host name:	ap
Domain (DNS suffix):	

Fig. 4. 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.

2.2.3. Step 2: Configure IEEE 802.11 Settings

Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	EAPTLS
Transmission power:	High

Fig. 5. 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 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.

2.2.4. Step 3: Review and Apply Settings

[Restart](#) [Cancel](#)

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	APXS v1.20/1.4.1.2535
MAC Address (BSSID)	00-02-6F-01-62-C5
System Up Time (hr:min:sec)	2:41:32
TCP/IP Settings	LAN Interface • IP address: 192.168.0.1 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
Wireless Settings	• Regulatory domain: FCC (U.S.) • Channel number: 11 • Transmission power: High • Network name (SSID): wireless1

Fig. 6. 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.

2.3. Deploying the AP

After the settings have been configured, deploy the AP to the field application environment. Connect Ethernet client computers to the Ethernet switch ports of the AP.

2.4. Setting up Client Computers

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

2.4.1. 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 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 client must be in *infrastructure* mode, so that it can link to 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.

2.4.2. 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, the user 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.

2.5. 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.

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

To check if a wireless client computer can link to 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.

2.5.2. 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.

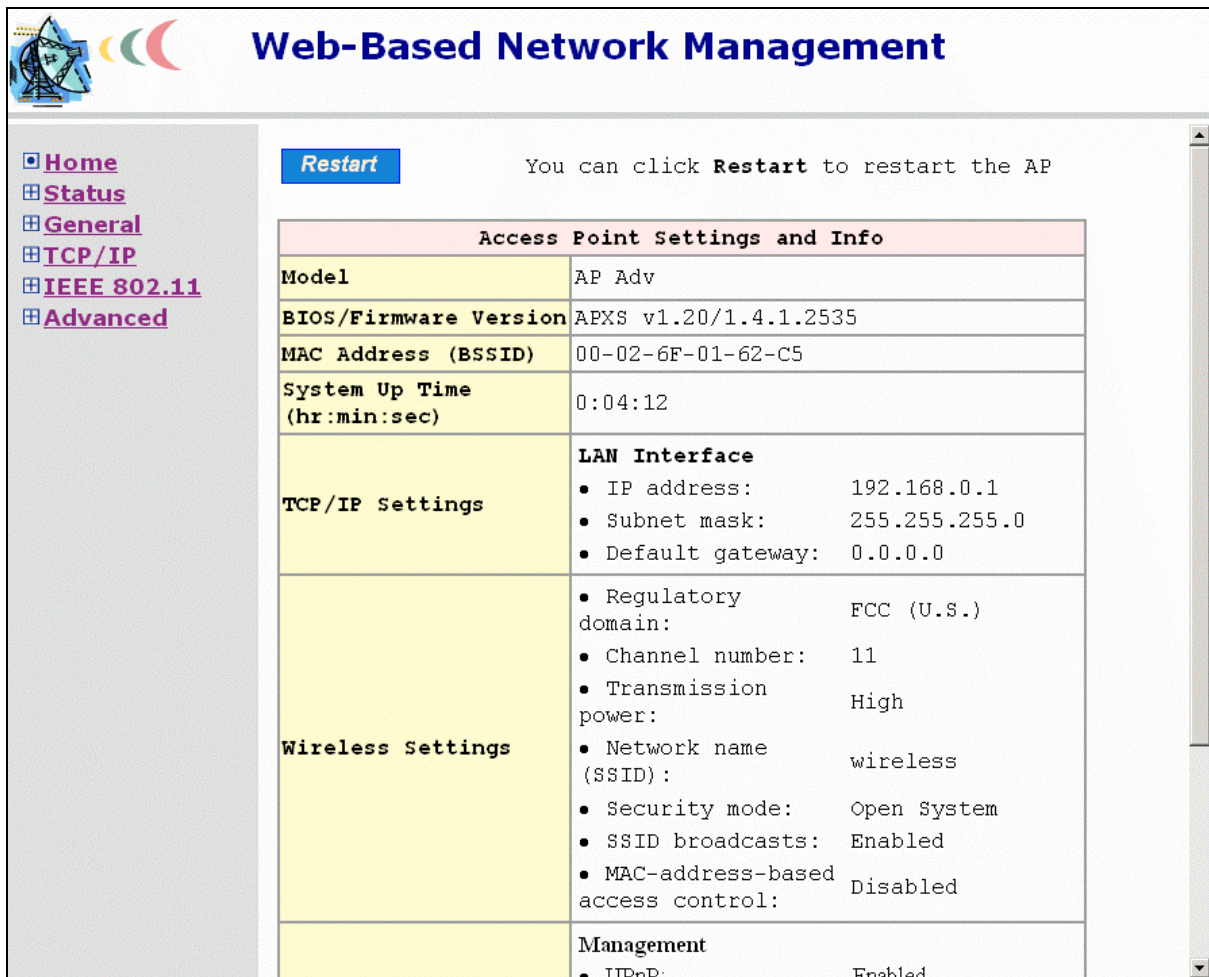
5. Type “**ping** *2nd_dns_server*”, where *2nd_dns_server* is a placeholder for the IP address of the secondary DNS server of the wireless client computer. Then press **Enter**.

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.

3. Using Web-Based Network Manager

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

3.1. Overview



Web-Based Network Management

[Restart](#) You can click **Restart** to restart the AP

Access Point Settings and Info	
Model	AP Adv
BIOS/Firmware Version	APXS v1.20/1.4.1.2535
MAC Address (BSSID)	00-02-6F-01-62-C5
System Up Time (hr:min:sec)	0:04:12
TCP/IP Settings	LAN Interface • IP address: 192.168.0.1 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
Wireless Settings	• Regulatory domain: FCC (U.S.) • Channel number: 11 • Transmission power: High • Network name (SSID): wireless • Security mode: Open System • SSID broadcasts: Enabled • MAC-address-based access control: Disabled
	Management • UPnP: Enabled

Fig. 7. The Start page.

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

- **Home.** For going back to the start page.
- **General.** Global operations.
 - **Password.** For gaining right to change the settings of the AP.
 - **Firmware Upgrade.** For upgrading the firmware of the AP.
- **TCP/IP.** TCP/IP-related settings.
 - **Addressing.** IP addressing settings for the AP to work in the TCP/IP networking world.
- **IEEE 802.11.** IEEE 802.11b-related settings.
 - **Communications.** Basic settings for the IEEE 802.11b 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 (Advanced model).** 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.
- **Management.** UPnP and SNMP settings.



Fig. 8. Save, Save & Restart, and Cancel.

At the bottom of each page, 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 the user 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 the user back to the start page.

If the user clicks **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.

Restart
Cancel

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	APXS v1.20/1.4.1.2535
MAC Address (BSSID)	00-02-6F-01-62-C5
System Up Time (hr:min:sec)	2:41:32
TCP/IP Settings	LAN Interface - IP address: 192.168.0.1 - Subnet mask: 255.255.255.0 - Default gateway: 0.0.0.0
Wireless Settings	- Regulatory domain: FCC (U.S.) - Channel number: 11 - Transmission power: High - Network name (SSID): wireless1

Fig. 9. Settings have been changed.

3.2. General Operations

3.2.1. Changing Password

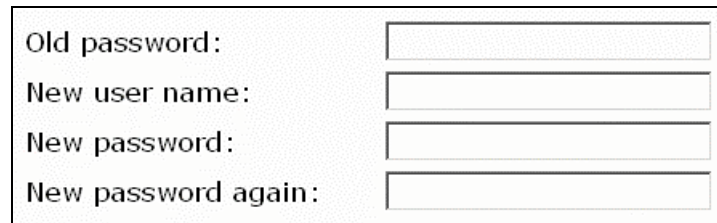
A web form for changing a password. It contains four labeled text input fields stacked vertically: 'Old password:', 'New user name:', 'New password:', and 'New password again:'. Each label is to the left of its corresponding input field.

Fig. 10. Password.

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

3.2.2. Upgrading Firmware

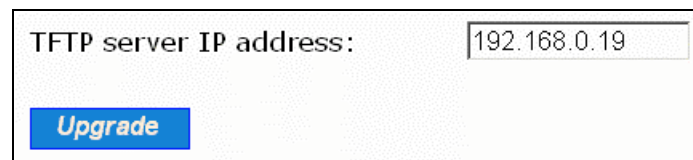
A web form for upgrading firmware. It features a label 'TFTP server IP address:' followed by a text input field containing the value '192.168.0.19'. Below the input field is a blue button with the text 'Upgrade' in white.

Fig. 11. Firmware Upgrade.

The AP can be triggered to download updated firmware from a specified TFTP server. On this page, the user specifies the IP address of the intended TFTP server, and then triggers the AP to begin downloading.

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.

To upgrade the firmware of AP:

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 the **LAN/Config** Ethernet port with a *crossover* Ethernet cable.
3. Configure the computer to **obtain an IP address automatically**.
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 Upgrade** hyperlink.
6. 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.
7. Trigger the firmware upgrade process by clicking **Upgrade**.

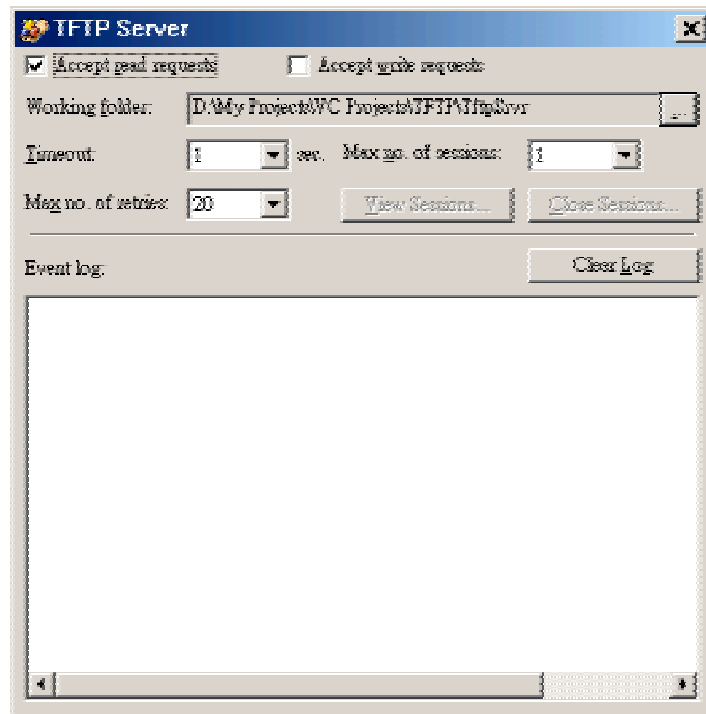


Fig. 12. TFTP Server.

TIP: It's more convenient to use the Firmware Upgrade Wizard of Wireless Network Manager to upgrade the firmware of an AP.

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: The LAN IP address of the AP 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 AP 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 AP unstartable. When this occurs, call for technical support.

3.3. Configuring TCP/IP Related Settings

3.3.1. Addressing

Method of obtaining an IP address:	Set manually
IP address:	192.168.168.98
Subnet mask:	255.255.255.0
Default gateway:	192.168.168.1
Host name:	ap
Domain (DNS suffix):	

Fig. 13. TCP/IP settings.

The IP address of the AP 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.

3.4. Configuring IEEE 802.11b-Related Settings

3.4.1. Communication

IEEE 802.11b-related communication settings include *Regulatory Domain*, *Channel Number*, and *Network Name (SSID)*.

Regulatory domain:	FCC (U.S.)
Channel number:	11
Network name (SSID):	EAPTLS
Transmission power:	High

Fig. 14. IEEE 802.11b communication settings.

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.

3.4.2. Security

SSID broadcasts: Enabled

Security mode: 802.1x EAP-MD5

MAC-Address-Based Access Control

Functionality: Disabled

Access control type: ☒ inclusive ☐ exclusive

☒ 00-50-C2-01-96-4D	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐

Fig. 15. IEEE 802.11b communication settings.

IEEE 802.11b security settings include *SSID Broadcasts*, *Security Mode*, *WEP Keys*, *MAC-Address-Based Access Control*.

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 connect to the AP.

There are 3 security modes for the *Standard* or *Pro* AP:

- **Open System.** No authentication, no data encryption.
- **64-bit WEP.** Authentication and data encryption based on 64-bit WEP (Wired Equivalent Privacy).
- **128-bit WEP.** Authentication and data encryption based on 128-bit WEP (Wired Equivalent Privacy), and 128-bit keys are used.

And there are 6 more security modes for the *Advanced* AP:

- **802.1x EAP-MD5.** The IEEE 802.1x functionality is enabled and the username/password-based EAP-MD5 authentication is used. No data encryption.
- **802.1x EAP-MD5 + 64-bit WEP.** The IEEE 802.1x functionality is enabled and the username/password-based EAP-MD5 authentication is used. Data encryption is achieved by 64-bit WEP.
- **802.1x EAP-MD5 + 128-bit WEP.** The IEEE 802.1x functionality is enabled and the username/password-based EAP-MD5 authentication is used. Data encryption is achieved by 128-bit WEP.

- **802.1x EAP-TLS; no encryption.** The IEEE 802.1x functionality is enabled and the digital certificate-based EAP-TLS user authentication. No data encryption is used.
- **802.1x EAP-TLS + 64-bit key.** The IEEE 802.1x functionality is enabled and the digital certificate-based EAP-TLS (Transport Layer Security) user authentication and data encryption is used. Session keys are 64-bit.
- **802.1x EAP-TLS + 128-bit key.** The IEEE 802.1x functionality is enabled and the digital certificate-based EAP-TLS user authentication and data encryption is used. Session keys are 128-bit.

See Section 3.4.3 for more information about IEEE 802.1x.

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

To deny wireless clients' access to the wireless network:

1. Set the **Access control type** to *exclusive*.
2. Specify the MAC address of a wireless client to be denied access.
3. Select the corresponding **Enabled** check box.
4. Repeat Steps 1 to 3 for other wireless clients.

To grant wireless clients' access to the wireless network:

1. Set the **Access control type** to *inclusive*.
2. Specify the MAC address of a wireless client to be granted access.
3. Select the corresponding **Enabled** check box.
4. Repeat Steps 1 to 3 for other wireless clients.

3.4.3. IEEE 802.1x/RADIUS (Advanced Model)

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 back-end RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the advanced wireless access point is controlled by the *security mode* (see Section 3.4.2). So far, the wireless access point supports two authentication mechanisms—EAP-MD5 (Message Digest version 5) and EAP-TLS (Transport Layer Security). If EAP-MD5 is used, the user has to give his or her *user name* and *password* for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's *digital certificate* that is stored in the com-

puter 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.

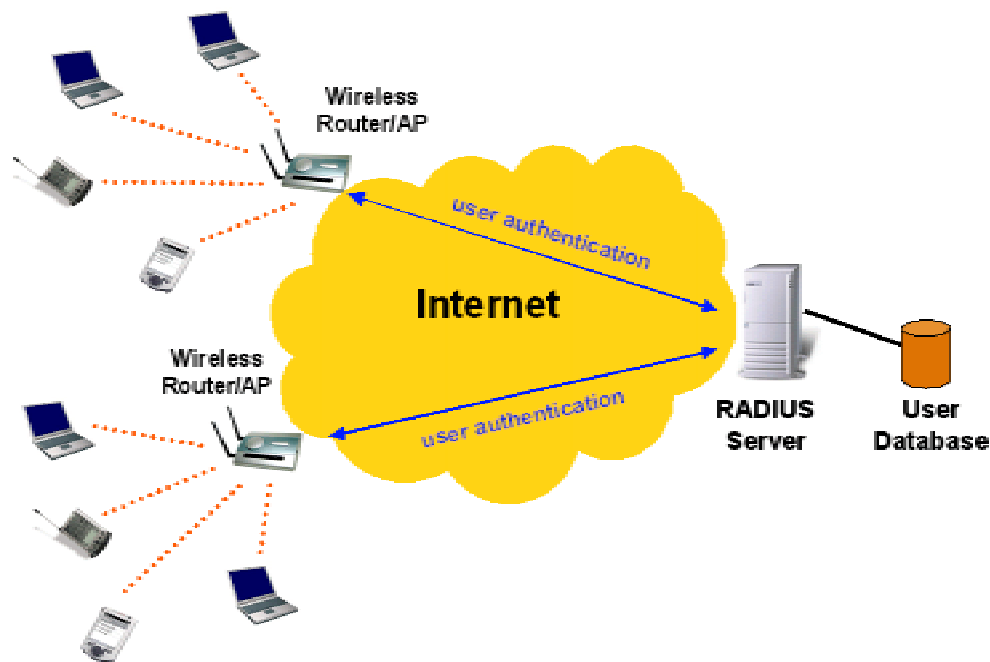


Fig. 16. IEEE 802.1x and RADIUS.

An *advanced* wireless access point supporting IEEE 802.1x can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the wireless access point will try to communicate with the secondary RADIUS server. The user can specify the length of time-out 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:	192.168.168.219
Secondary RADIUS server:	
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared key:	*****
Identifier of this NAS:	ap2

Fig. 17. IEEE 802.1x/RADIUS settings.

3.5. Configuring Advanced Settings

3.5.1. Management

3.5.1.1. SNMP

Functionality:	Enabled ▾
Read only community:	public
Read write community:	private
SNMP Trap table	
IP address	Community
☒ 192.168.0.2	public
☐ 0.0.0.0	
☐ 0.0.0.0	
☐ 0.0.0.0	
☐ 0.0.0.0	

Fig. 18. SNMP settings.

The SNMP (Simple Network Management Protocol) functionality can be disabled, and the user 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**.

3.5.1.2. UPnP

Functionality:	Enabled ▾
Friendly name:	

Fig. 19. 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, the user can see the AP in Network Neighborhood of Windows XP. The AP can be given a **friend name** that will be shown in Network Neighborhood. *Double-clicking* the icon in Network Neighborhood that stands for the AP will launch the default Web browser for the user to configure the AP.

A-1: 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-set values.

Setting Name	Default Value
Global	
User Name	root
Password	root
IEEE 802.11b	
Regulatory Domain	FCC (U.S.)
Channel Number	11
SSID	wireless
SSID Broadcasts	Enabled
Transmission Rate	11Mbps
Transmission 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
IEEE 802.1x/RADIUS	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
Management	
SNMP	Enabled
UPnP	Enabled

A-2: LED Definitions

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

- **ALV:** *Alive*. Blinks when the AP is working normally.
- **RF:** IEEE 802.11b interface
- **LAN:** Ethernet LAN interface
- **PWR:** Power

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 link to an access point.**
 - 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 access point or AP?
 - ◆ Check the SSID setting of the WLAN NIC and of the AP.
 - Is the WEP functionality of the prospective access point or AP enabled?
 - ◆ Make appropriate WEP settings of the client computer to match those of the access point or AP.
 - Is the prospective access point or AP within range of wireless communication?
 - ◆ Check the *signal strength* and *link quality* sensed by the WLAN NIC.

B-2: TCP/IP Settings Problems

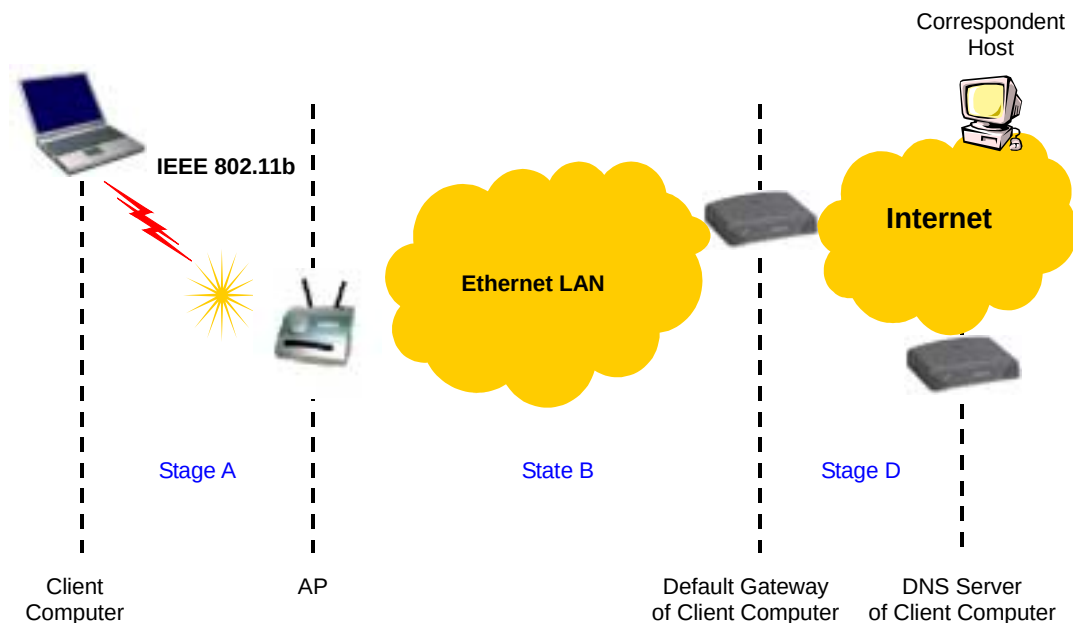


Fig. 20. Communication stages for a client to reach its correspondent host.

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. 20, 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 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 Device Manager** to disable unnecessary NICs.
 - Is the underlying link (Ethernet or IEEE 802.11b) 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 the Wireless Network Manager or Wireless Router/AP Browser to get the information (see Appendix C-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 (**WLBwrsr.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.

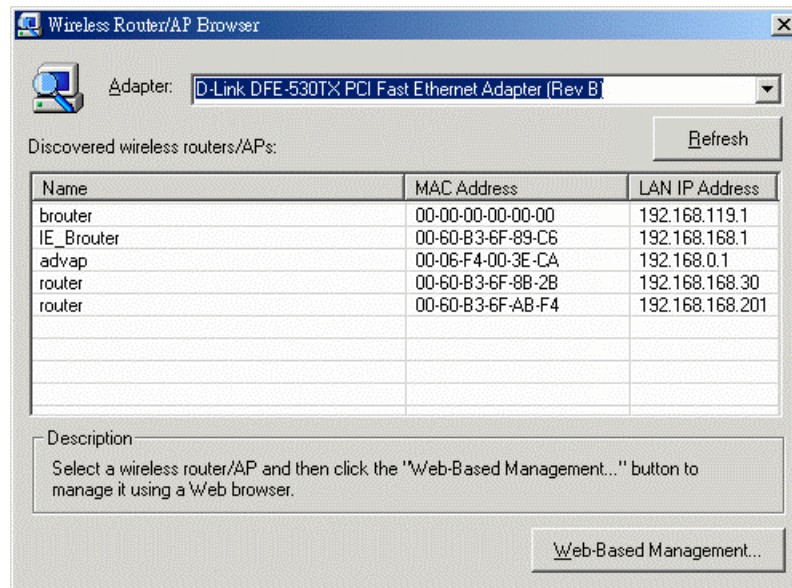


Fig. 21. Wireless Router/AP Browser.

- **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.