

Wireless Broadband Router IWE1200A

Quick Installation Guide

Version: 1.05

Last Updated: 09/12/2001

Instruction Manual

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.

FCC RF Radiation Exposure Statement:

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

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

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.

Table of Contents

1. Introduction	1
1.1. Overview	1
1.2. Features	1
2. Inserting the Accompanying PCMCIA WLAN Card (IWE1200A-1).....	2
3. Preparing for Configuration	3
3.1. Connecting the Managing Computer and the Broadband Router.....	3
3.2. Changing the TCP/IP Settings of the Managing Computer	3
4. Changing the Configuration of the Broadband Router	4
4.1. Entering the User Name and Password.....	4
4.2. Selecting an Operational Mode	5
4.3. Changing the TCP/IP-Related Settings.....	6
4.4. Changing the IEEE 802.11b-Related Settings	12
4.5. Changing the DHCP Server Settings.....	13
4.6. Applying the New Settings.....	13
5. Deploying the Broadband Router.....	14
5.1. Connecting the Broadband Router to Ethernet Client Computers	14
5.2. Connecting the Broadband Router to a Modem.....	15
6. Setting up Client Computers.....	15
6.1. Changing IEEE 802.11b-Related Settings	15
6.2. Changing TCP/IP-Related Settings	15
7. Confirming the Settings of the Broadband Router and Client Computers.....	16
7.1. Checking if the IEEE 802.11b-Related Settings Work.....	16
7.2. Checking if the TCP/IP-Related Settings Work	16
8. Installing the Print Client Components.....	17
Appendix A.....	18
A-1: Default Settings	18
A-2: LED Status	19
Appendix B: Using Web-Based Network Manager.....	19
B-1: Overview.....	19
B-2: Start Page.....	19
B-3: Changing Configuration	20
B-4: Changing Passwords	21
B-5: Upgrading Firmware	21
Appendix C: Troubleshooting	22
C-1: Wireless Settings Problems.....	22
C-2: TCP/IP Settings Problems	23
C-3: Unknown Problems.....	24

1. Introduction

1.1. Overview

The wireless broadband brouter (bridge and router) enables IEEE 802.11b and Ethernet client computers to share an Internet connection provided by an Internet service provider (ISP). The Internet connection can be DSL, cable, V.90, or ISDN-based. In addition, it also serves as a wireless access point, so that the wireless client computers and the Ethernet client computers can reach one another.

Since the wireless broadband brouter provides rich TCP/IP and WLAN (Wireless Local Area Network) functionality, a basic understanding of the inner workings of TCP/IP and IEEE 802.11b is necessary. Essential TCP/IP concepts include IP addressing, IP routing, IP name resolution, DHCP (Dynamic Host Configuration Protocol), and PPP (Point-to-Point Protocol). Essential IEEE 802.11b concepts include channel numbers and WEP (Wired Equivalent Privacy).

In this quick installation guide, we first describe how to prepare a *managing computer* on which the user (or administrator) uses a Web browser (Microsoft Internet Explorer recommended) to change the configuration settings of a wireless broadband brouter. Next, we explain the steps to change the settings using the *Web-Based Network Manager*. And then, we present the procedures to make sure that the new settings work correctly. Finally, we describe how to install the *print client* components on a client computer for the printer sharing functionality. In the remainder of this guide, a wireless broadband brouter is often referred to as a WIASA (*Wireless Internet Access Server Appliance*) for short.

1.2. Features

- **Self-Test.** The wireless broadband brouter can diagnose hardware problems by itself at start-up time.
- **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 Wi-Link broadband brouter 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.
- **Internet Connection Sharing**
 - **DNS proxy.** The wireless broadband brouter can forward DNS (Domain Name System) requests from client computers to DNS servers on the Internet. And DNS responses from

the DNS servers can be forwarded back to the client computers.

- **DHCP server.** The wireless broadband router can automatically assign IP addresses to client computers by DHCP (Dynamic Host Configuration Protocol).
- **NAT server.** Client computers can share a public IP address provided by an ISP (Internet Service Provider) by NAT (Network Address Translation). And our NAT server functionality supports the following:
 - ◆ **Virtual server.** Exposing servers on the intranet to the Internet.
 - ◆ **PPTP, IPsec, and L2TP tunneling.** Passing VPN (Virtual Private Network) packets through the intranet-Internet boundary. PPTP means Point-to-Point Tunneling Protocol, IPsec means IP Security, and L2TP means Layer 2 Tunneling Protocol.
 - ◆ **DMZ (DeMilitarized Zone).** All non-recognized IP packets from the Internet can be forwarded to a specific computer on the intranet.
- **DSL/Cable Modem Support.** Supporting dynamic IP address assignment by PPPoE (Point-to-Point Protocol over Ethernet) or DHCP and static IP address assignment.
- **V.90/ISDN Modem Support.** Supporting PPP (Point-to-Point Protocol) dial-up networking over RS232.
- **Auto-dial.** When the wireless broadband router detects outgoing packets to the Internet, it dials up to the ISP automatically. This functionality applies to PPP and PPPoE.
- **Printer Sharing.** The wireless broadband router can serve as a print server for Windows 9x/2000 client computers.
- **4-Port Ethernet Switch.** The wireless broadband router provides a 4-port Ethernet switch so that a stand-alone Ethernet hub/switch is not necessary for connecting Ethernet client computers to the router.
- **Firmware Upgrade.** The firmware of wireless broadband routers can be upgraded, so that more features can be added in the future. One of the planned features is the support for *IEEE 802.1x port-based access control*.
- **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).
- **Management**
 - Web-based Network Manager for configuring and monitoring wireless broadband routers. The management protocol is HTTP (HyperText Transfer Protocol)-based.

2. Inserting the Accompanying PCMCIA WLAN Card (IWE1200A-1)

The wireless interface of a WIASA (IWE1200A-1) is a WLAN PCMCIA card inserted into the PCMCIA socket labeled **Wireless LAN Card**. Since a WIASA and its accompanying WLAN PCMCIA card are placed separately within a package, the user has to insert the PCMCIA card to the socket of the WIASA after they are taken out of the package. And then, plug the connector of the power adapter to the power jack of the WIASA to power it on.

NOTE: Unless a WIASA is to be packed and moved to a distant place, don't pluck out the PCMCIA card from the socket.

3. Preparing for Configuration

For the user (or administrator) to configure a WIASA, a *managing computer* with a Web browser (Microsoft Internet Explorer recommended) is needed. For first-time configuration of a WIASA, the managing computer should already have an Ethernet network interface card (NIC) installed. For maintenance-configuration of a deployed WIASA, either a wireless computer or a wired computer can be employed as the managing computer.

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 WIASA are in the same IP subnet**. By default (see Appendix A-1, "Default Settings"), the DHCP server functionality of a WIASA is enabled, so that if the managing computer is set to automatically obtain an IP address by DHCP, the condition can be satisfied easily.

3.1. Connecting the Managing Computer and the Broadband Router

Connect the Ethernet managing computer to anyone of the LAN switch ports of the managed WIASA with a normal Ethernet cable (see Fig. 1).

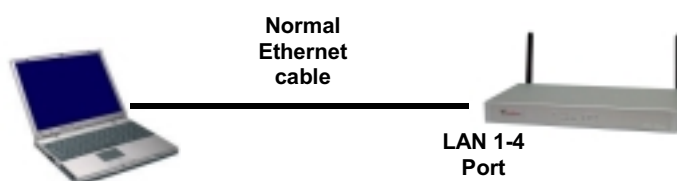


Fig. 1. Connecting a managing computer and a WIASA via Ethernet.

Since the DHCP server functionality is factory-set to be enabled, it's recommended that there are no other computers connected to the other Ethernet switch ports of the WIASA, so that the user can be 100-percent sure that the WIASA will be the DHCP server of the managing computer.

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 WIASA are in the same IP subnet. If the managing computer is originally set a static IP address, the user can either change the IP address to **192.168.0.xxx** (the default IP address of a WIASA is **192.168.0.1**) and the subnet mask to **255.255.255.0** or select an automatically-obtain-an-IP-address option.

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

If the computer is already set to obtain an IP address automatically, the user can use the Windows-provided tool, **WinIPCfg.exe** (on Windows 9x) or **IPConfig.exe** (on Windows 2000), to re-obtain an IP address from the WIASA. **WinIPCfg.exe** is a GUI program, and has command

buttons for releasing the current IP address and re-obtaining an IP address. **IPConfig.exe** is a command-line program, and the **/release** option releases the current IP address and the **/renew** option triggers the Windows DHCP client subsystem to re-obtain an IP address.

NOTE: By default, the first assignable IP address of the DHCP server on the WIASA is **192.168.0.2**.

4. Changing the Configuration of the Broadband Router

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

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

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.

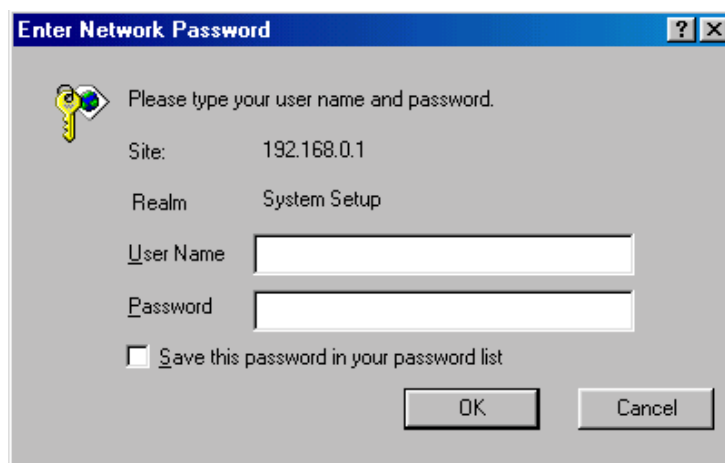


Fig. 2. Entering the user name and password.

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

TIP: The start page can be saved or printed within the Web browser for future reference.

On the start page, click the **Change Configuration** link to change the configuration of the WIASA. (See Appendix B, “Using Web-Based Network Manager” for more information about the Web management pages.)

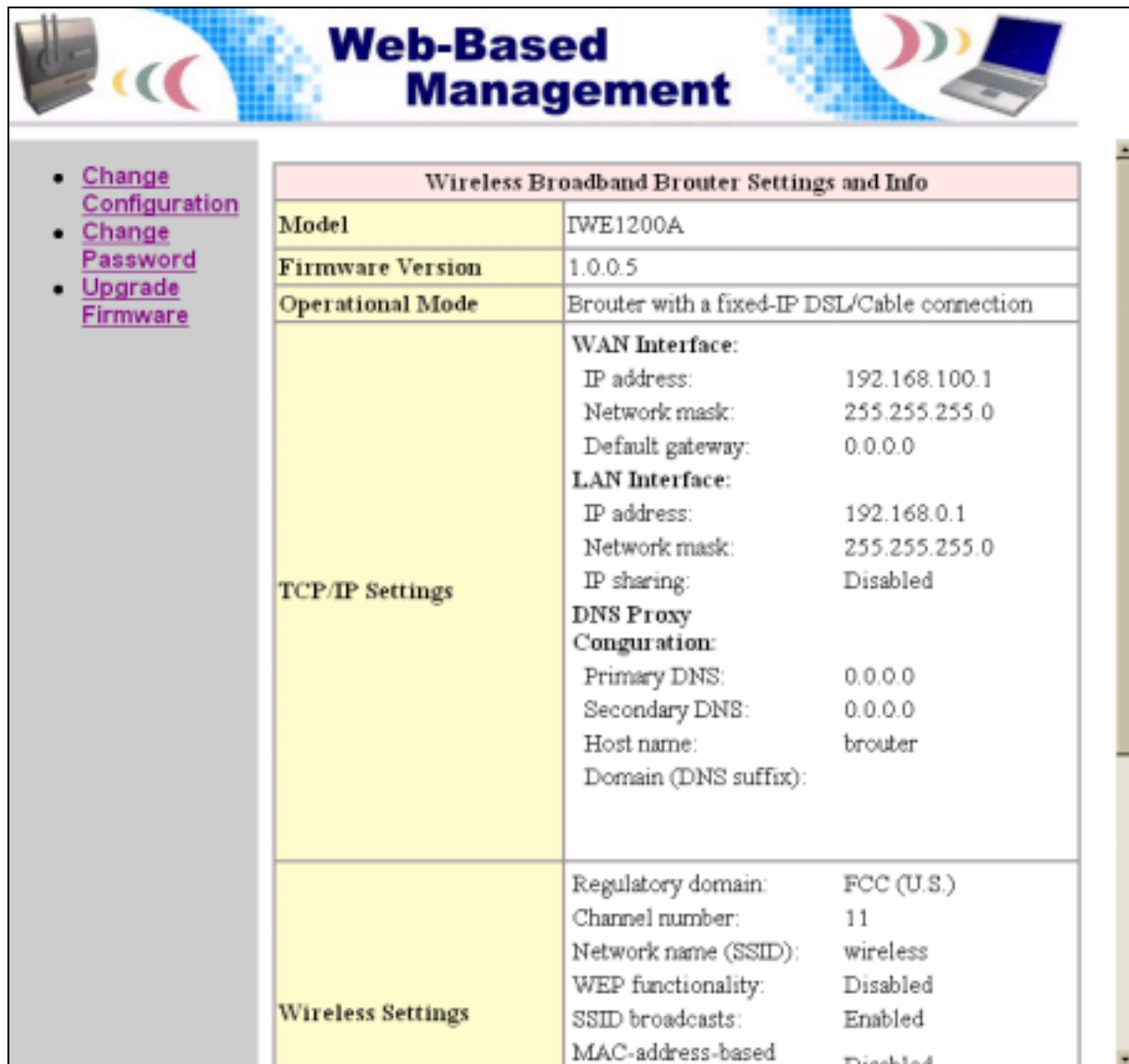


Fig. 3. The Start page.

The first page of the configuration wizard is a welcome page. This page gives a brief description of the configuration process. Click **Next** to continue. The configuration process is 5-step. We'll explain what to do step-by-step in the following subsections.

4.2. Selecting an Operational Mode

- If the WIASA is to be used simply as a wireless-to-Ethernet access point, select **Simple Access Point**. In this mode, the Ethernet WAN interface is disabled.
- If the WIASA is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by PPPoE, select **Brouter with a PPPoE-Based DSL/Cable Connection**. In this mode, the IP address settings for the LAN interfaces, PPPoE settings, and NAT settings can be changed on the following pages.
- If the WIASA is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by DHCP, select **Brouter with a DHCP-Based DSL/Cable Connection**. In this mode, the IP address settings for the LAN interfaces and NAT settings can be changed on the following pages.

- If the WIASA is to be used with a DSL or cable modem and the WAN IP address has to be manually set, select **Router with a Fixed-IP DSL/Cable Connection**. In this mode, the IP address settings for the LAN and the WAN interfaces as well as NAT settings can be changed on the following pages.
- If the WIASA is to be used with a V.90 or ISDN modem, select **Router with a Dial-up Connection**. In this mode, the IP address settings for the LAN interfaces, PPP settings, and NAT settings can be changed on the following pages.

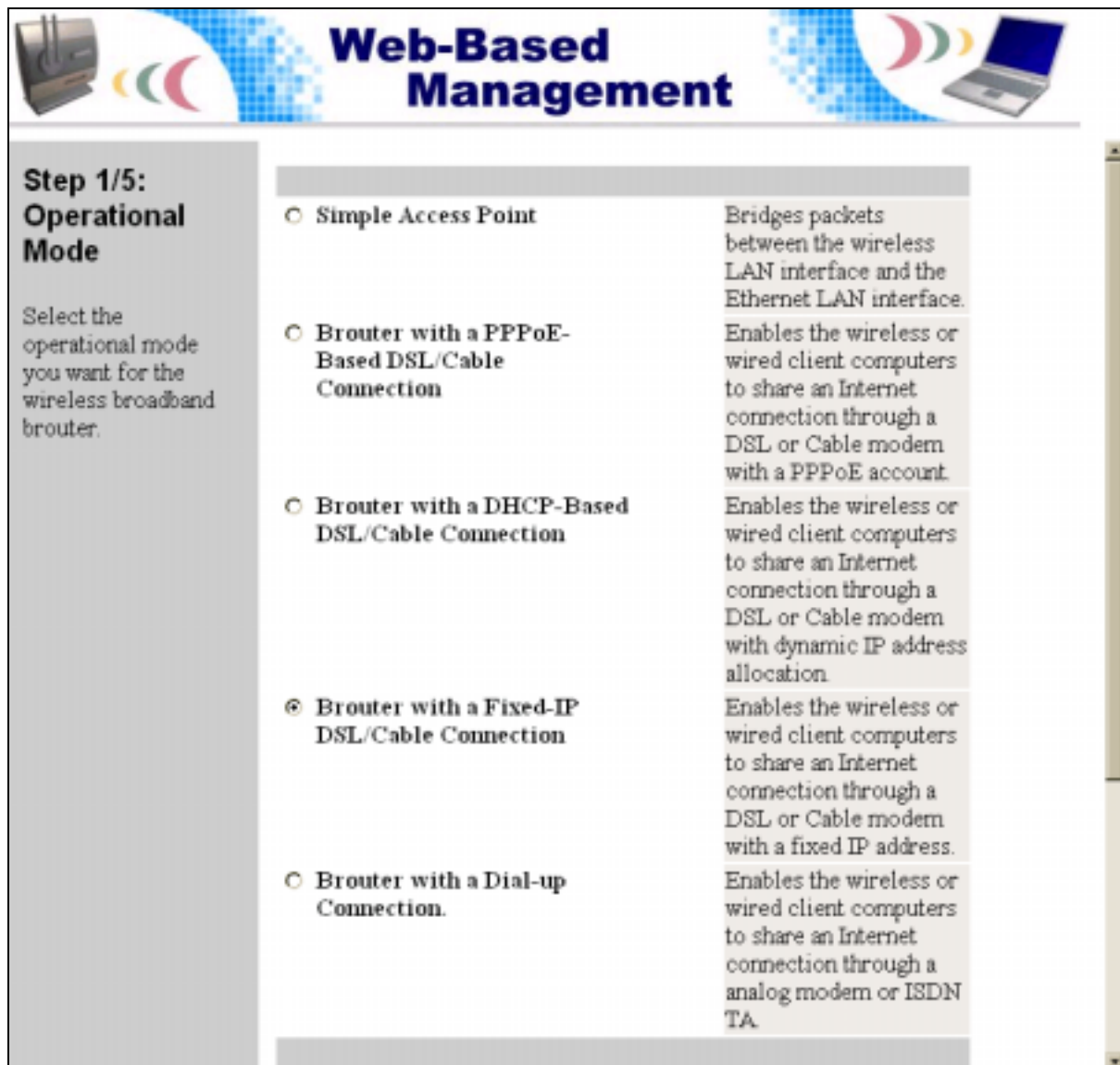


Fig. 4. Operational modes.

NOTE: The LAN interfaces include the IEEE 802.11b wireless LAN interface and the Ethernet LAN interfaces. These two interfaces share a LAN IP address.

4.3. Changing the TCP/IP-Related Settings

- If the WIASA was set to be in **Simple Access Point** mode, one IP address is needed. This 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.

Web-Based Management

Step 2/5: TCP/IP Settings

Set the IP address settings of this wireless broadband router as a *Simple Access Point*.

Method	Set manually
IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Default gateway:	0.0.0.0

<< Back Cancel Next >>

Fig. 5. TCP/IP settings for **Simple Access Point** mode.

- If the WIASA was set to be in **Router with a PPPoE-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet/wireless LAN interfaces and the other for the WAN interface. The IEEE 802.11b interface and the Ethernet LAN interface share the LAN IP address. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPPoE from the ISP. Consult your ISP for the correct *User Name*, *Password*, and *Service Name* settings.

NOTE: If the **Idle Disconnect Time** is set to 0, the PPPoE connection will not be disconnected.

Web-Based Management

Step 2/5: TCP/IP Settings

Set TCP/IP-related settings of the PPPoE-based Ethernet WAN interface and Ethernet/wireless LAN interfaces.

Ethernet WAN Interface

User name:

Password:

Password again:

Service name:

Idle disconnect time (min):

Host name:

Domain:

Ethernet/Wireless LAN Interfaces

IP address:

Subnet mask:

NAT: ☐

☐ DMZ host:

Virtual Server Mappings:

Server type	IP address
☐ FTP (port 21):	192.168.0.201
☐ IMAP (port 220):	
☐ SMTP (port 25):	
☐ POP3 (port 110):	
☐ TELNET (port 23):	

Fig. 6. TCP/IP settings for **Router with a PPPoE-Based DSL/Cable Connection** mode.

- If the WIASA was set to be in **Router with a DHCP-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet/wireless LAN interfaces and the other for the WAN interface. The IEEE 802.11b interface and the Ethernet LAN interface share the LAN IP address. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by DHCP from the ISP.

Web-Based Management

Step 2/5: TCP/IP Settings

Set the TCP/IP-related settings of the DHCP-based Ethernet WAN interface and Ethernet/wireless LAN interfaces.

Ethernet WAN Interface

Host name:

Domain (DNS suffix):

Ethernet Wireless LAN Interface

IP address:

Subnet mask:

NAT:

☐ DMZ host:

Virtual Server Mappings:

Server type	IP address
☐ FTP (port 21):	192.168.0.201
☐ IMAP (port 220):	
☐ SMTP (port 25):	
☐ POP3 (port 110):	
☐ TELNET (port 23):	
☐ HTTP (port 80):	

Fig. 7. TCP/IP settings for **Brouter with a DHCP-Based DSL/Cable Connection** mode.

- If the WIASA was set to be in **Brouter with a Fixed-IP DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet/wireless LAN interfaces and the other for the WAN interface. The IEEE 802.11b interface and the Ethernet LAN interface share the LAN IP address. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it must be manually set by the user. Consult your ISP for the correct *IP Address, Default Gateway, Subnet Mask, Primary DNS Server, and Secondary DNS Server* settings.

Web-Based Management

Step 2/5: TCP/IP Settings

Set the TCP/IP-related settings of the fixed-IP Ethernet WAN interface and Ethernet/wireless LAN interfaces.

Ethernet WAN Interface

Address Settings:

IP address:

Subnet mask:

Default gateway:

DNS Proxy:

Functionality:

DNS server 1:

DNS server 2:

Host name:

Domain:

Ethernet/Wireless LAN Interfaces

IP address:

Subnet mask:

NAT:

Functionality:

☐ DMZ host:

Virtual Server Mappings:

Server type	IP address
☐ FTP (port 21):	192.168.0.201
☐ IMAP (port 220):	
☐ POP3 (port 110):	

Fig. 8. TCP/IP settings for **Brouter with a Fixed-IP DSL/Cable Connection** mode.

- If the WIASA was set to be in **Brouter with a Dial-up Connection** mode, two IP addresses are needed—one for the Ethernet/wireless LAN interfaces and the other for the WAN interface. The IEEE 802.11b interface and the Ethernet LAN interface share the LAN IP address. The LAN IP address must be set manually to a private IP address, say **192.168.0.xxx**. The default IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPP from the ISP. Consult your ISP for the correct *User Name*, *Password*, and *Telephone Number* settings.

NOTE: If the **Idle Disconnect Time** is set to 0, the dial-up connection will not be disconnected.

Web-Based Management

Step 2/5: TCP/IP Settings

Set the TCP/IP-related settings of the dial-up networking interface and Ethernet/wireless interfaces.

Dial-Up WAN Interface

Telephone number:

User name:

Password:

Password again:

Idle disconnect time (min):

Host name:

Domain:

Ethernet/Wireless LAN Interface

IP address:

Subnet mask:

NAT: ☐

☐ DMZ host:

Virtual Server Mappings:

Server type	IP address
☐ FTP (port 21):	192.168.0.201
☐ IMAP (port 220):	
☐ SMTP (port 25):	
☐ POP3 (port 110):	
☐ TELNET (port 23):	
☐ HTTP (port 80):	

Fig. 9. TCP/IP settings for **Router with a Dial-up Connection** mode.

In addition to the IP-address-related settings for the WAN and LAN interfaces, you can also set NAT-related settings, including *virtual server*, on this page. The NAT server functionality can be enabled or disabled. Besides, you can expose internal servers on the intranet for public use.

To expose internal servers:

1. Select the corresponding check boxes for the kinds of servers you want to expose.
2. Specify the private IP addresses of the servers, and select the corresponding check boxes.

To specify the *DMZ host*:

- Enter the private IP address of the computer to be used as a DMZ host, and select the corresponding check box.

NOTE: A DMZ (*DeMilitarized Zone*) host receives all non-recognized TCP/IP packets from the NAT server on the WISA, therefore any kind of TCP/IP networking applications running on the host can seamlessly communicate with the Internet through NAT.

4.4. Changing the IEEE 802.11b-Related Settings

IEEE 802.11b-related settings include *Regulatory Domain*, *Channel Number*, *Network Name (SSID)*, *WEP Mode*, *WEP Keys*, *SSID Broadcasts*, *MAC-Address-Based Access Control*. The SSID of a wireless client computer and the SSID of the WIASA must be identical for them to communicate with each other.

For security reasons, it's highly recommended that the WEP functionality be enabled and the WEP keys are set adequately so that data transmitted over the wireless medium will be encrypted. Additionally, you can disable the SSID broadcasts functionality so that a wireless client computer with an "any" SSID cannot connect to the WIASA.

The screenshot shows a web-based management interface titled "Web-Based Management". On the left, a sidebar indicates "Step 3/5: Wireless Settings" and provides instructions: "Set the IEEE 802.11b-related settings of the wireless network interface of the wireless broadband router." The main content area is divided into sections: "Communication" with fields for "Regulatory domain" (FCC (U.S.)), "Channel number" (11), and "Network name(SSID)" (wireless); "Security" with "WEP" mode set to "Disabled"; "SSID broadcasts" set to "Enabled"; and "MAC-Address-Based Access Control" with "Functionality" set to "Disabled". Under "Access control type", the "inclusive" radio button is selected. A table lists MAC addresses, with the first entry "00-50-c2-01-96-4d" checked for inclusion.

Access control type: ☒ inclusive ☐ exclusive	
☒ 00-50-c2-01-96-4d	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐

Fig. 10. IEEE 802.11b-related settings.

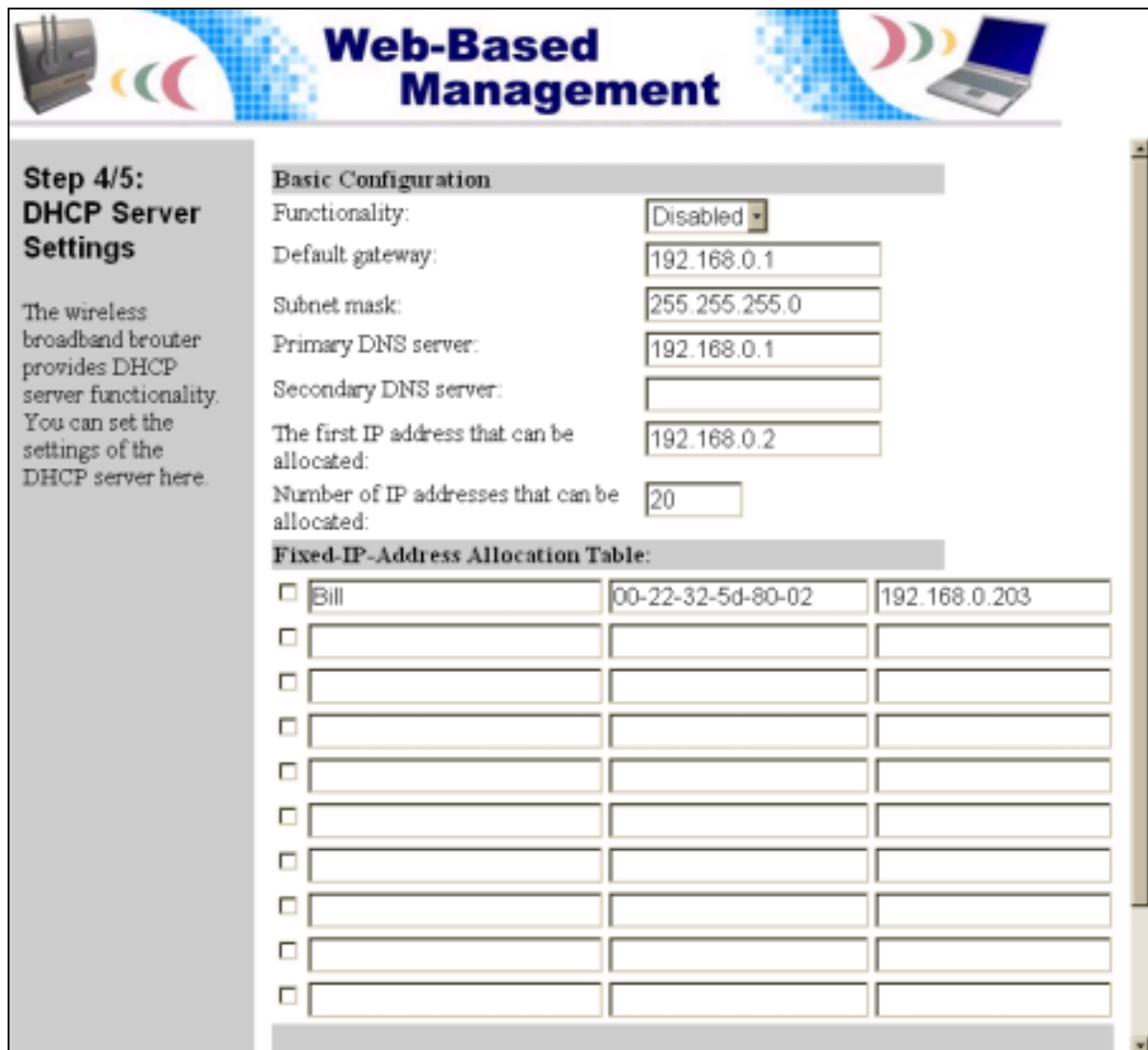
With MAC-Address-Based Access Control, you can specify the wireless client computers that are permitted or not permitted to connect to the WIASA. When the table type is set to **inclusive**, entries in the table are permitted to connect to the WIASA. When the table type is set to **exclusive**, entries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

4.5. Changing the DHCP Server Settings

The WIASA can automatically assign IP addresses to client computers by DHCP. On this 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.

In most cases, *Default Gateway* and *Primary DNS Server* should be set to the IP address of the WIASA's LAN interfaces (e.g., the default LAN IP address is **192.168.0.1**), and *Subnet Mask* is set to **255.255.255.0**.

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 WIASA.



The screenshot shows a web-based management interface titled "Web-Based Management". On the left, a sidebar indicates "Step 4/5: DHCP Server Settings" and explains that the wireless broadband router provides DHCP server functionality. The main content area is titled "Basic Configuration" and contains several settings:

- Functionality: Disabled (dropdown menu)
- Default gateway: 192.168.0.1
- Subnet mask: 255.255.255.0
- Primary DNS server: 192.168.0.1
- Secondary DNS server: (empty field)
- The first IP address that can be allocated: 192.168.0.2
- Number of IP addresses that can be allocated: 20

Below these settings is a "Fixed-IP-Address Allocation Table" with 10 rows. Each row has a checkbox, a name field, a MAC address field, and an IP address field. The first row is pre-filled with "Bill", "00-22-32-5d-80-02", and "192.168.0.203".

	Name	MAC Address	IP Address
☐	Bill	00-22-32-5d-80-02	192.168.0.203
☐			
☐			
☐			
☐			
☐			
☐			
☐			
☐			
☐			

Fig. 11. DHCP server settings.

4.6. Applying the New Settings

On the final page, you can review all the settings you have made. Changes are highlighted in red. If

they are OK, click **Save & Restart** to apply the new settings. Or you can go back to previous pages to make modifications. Or you can click **Cancel** to leave the configuration process without any changes.

NOTE: About 12 seconds are needed for the WIASA to complete its restart process.



**Step 5/5:
Save & Restart**

Make sure that every item of all the settings is set correctly as you wish.

And then, click **Save & Restart** to save the configuration settings to the wireless broadband router and restart it for the new settings to take effect.

Wireless Broadband Router Settings and Info	
Model	IWE1200A
Firmware Version	1.0.0.5
Operational Mode	Simple Access Point
TCP/IP Settings	WAN Interface: The WAN interface is disabled LAN Interface: IP address: 192.168.0.1 Network mask: 255.255.255.0 Default gateway: 0.0.0.0
Wireless Settings	Regulatory domain: FCC (U.S.) Channel number: 11 Network name (SSID): wireless WEP functionality: Disabled SSID broadcasts: Enabled MAC-address-based access control: Disabled
DHCP Server Settings	DHCP server is disabled

<< Back
Cancel
Save & Restart

Fig. 12. Settings review.

5. Deploying the Broadband Router

After the settings are changed, deploy the WIASA to the field application environment. Connect Ethernet client computers to the Ethernet switch ports of the WIASA. If the WIASA was configured as a router, also connect a DSL, cable, V.90, or ISDN modem to the WIASA.

5.1. Connecting the Broadband Router to Ethernet Client Computers

To connect the WIASA with Ethernet client computers:

1. Plug one end of a *normal* (not *crossover*) Ethernet cable to a **LAN** Ethernet switch port of the WIASA, and the other end to the Ethernet jack of the Ethernet NIC of a client computer.
2. If necessary, use a normal Ethernet cable to connect the WIASA to another Ethernet switch/hub via the **UP-LINK** port.

5.2. Connecting the Broadband Router to a Modem

To connect the WIASA with a DSL or cable modem:

1. Plug one connector of a *cross-over* Ethernet cable to the Ethernet **WAN** jack of the WIASA.
2. Plug the other connector of this cable to the Ethernet jack of the DSL or cable mode. Refer to the user's manual of the modem if necessary.

To connect the WIASA with a V.90 or ISDN modem:

1. Plug one connector of a *normal* RS232 cable to the RS232 (**COM**) port of the WIASA.
2. Plug the other connector of this cable to the RS232 port of the V.90 or ISDN modem. Refer to the user's manual of the modem if necessary.

6. Setting up Client Computers

Before the client computers can use the services provided by the WIASA, their TCP/IP settings must be set adequately to match those of the WIASA. Furthermore, for wireless client computers, their IEEE 802.11b-related settings must also match those of the WIASA.

6.1. Changing 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 a WIASA.

To establish a wireless link to a WIASA:

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 a wireless access point or broadband router.

6.2. Changing 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 WIASA 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 WIASA, or select an automatically-obtain-an-IP-address option if the DHCP server functionality of the WIASA is enabled or there is already a DHCP server on the LAN.

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

If the computer is already set to obtain an IP address automatically, the user can use the Windows-provided tool, **WinIPCfg.exe** (on Windows 9x) or **IPConfig.exe** (on Windows 2000), to re-obtain an IP address from the WIASA. **WinIPCfg.exe** is a GUI program, and has command buttons for releasing the current IP address and re-obtaining an IP address. **IPConfig.exe** is a command-line program, and the **/release** option releases the current IP address and the **/renew** option triggers the Windows DHCP client subsystem to re-obtain an IP address.

7. Confirming the Settings of the Broadband Router and Client Computers

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

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

To check if a wireless client computer can link to the WIASA:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.
2. Check if the client computer is connected to an access point, and the access point is the WIASA.

If the check fails, see Appendix C-1, “Wireless Settings Problems” for troubleshooting.

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.
2. Type “**ping** *wiasa*”, where *wiasa* is a placeholder for the IP address of the WIASA. Replace it with your real IP address—for example, 192.168.0.1. Then press **Enter**.

If the WIASA responds, go to the next step; else, see Appendix C-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 client computer. Then press **Enter**.

NOTE: If the WIASA is set in *brouter* mode, the default gateway of the client computer should be the WIASA. You can skip this step in this case.

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

4. Type “**ping** *wiasa_1st_dns_server*”, where *wiasa_1st_dns_server* is a placeholder for the IP address of the primary DNS server of the WIASA. Then press **Enter**.

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

TIP: You can view the primary and secondary DNS servers of the WIASA on the start page of the Web-based Network Manager.

5. Type “**ping** *wiasa_2nd_dns_server*”, where *wiasa_2nd_dns_server* is a placeholder for the IP address of the secondary DNS server of the WIASA. Then press **Enter**.

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

8. Installing the Print Client Components

The print server components on the WIASA work in conjunction with the print client components on a client computer, and they communicate by TCP/IP. The print client components expose a virtual communication port on the client computer, so that, on the client computer, the driver of the printer must be configured to print to this virtual port. When an application on the client computer is printing, the print data is sent through the virtual port by the print client components to the WIASA. And then, the print data is directed to the printer, which is connected to the parallel port of the WIASA, by the print server components.

To install the print client components on a client computer:

1. Connect the printer to the **Printer** port of the WIASA with a parallel cable.
2. Insert the Print Client setup disk into drive D: of the client computer, where "D:" is the name of the CD-ROM drive; substitute the real name of your CD-ROM drive for "D:" if necessary.
3. Run "**D:\PrntClnt\Setup.exe**" on the client computer.
4. Specify the IP address of the WIASA print server when prompted by the setup program.
5. Restart Windows as prompted by the setup program.
6. Add a new local printer using "**Start, Settings, Printers, Add Printer**" and select the WIASA Print Client port for the local printer within the Add New Printer Wizard.
7. Print a test page to check if the client computer can print to the printer that is connected to the WIASA.

Appendix A

A-1: Default Settings

TIP: Press the **Soft Reset** switch on the housing of a *powered-on* WIASA to reset the configuration settings to factory-set values.

Setting Name	Default Value
Global	
User Name	root
Password	root
Operational Mode	Brouter with a Fixed-IP DSL/Cable Connection
IEEE 802.11b	
Regulatory Domain	FCC (U.S.)
Channel Number	11
SSID	wireless
SSID Broadcasts	Enabled
Transmission Rate	11Mbps
MAC Address	See the label of the accompanying PCMCIA card
WEP Mode	Disabled
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
LAN Interface	
Method to Get an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
WAN Interface	
Type	Fixed-IP DSL/Cable
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Host Name	brouter
Domain (DNS suffix)	Not set
PPP	
User Name	username
Password	Not set
Telephone Number	Not set
PPPoE	
User Name	username
Password	Not set

Service Name	servicename
DHCP Server	
Functionality	Enabled
Default Gateway	192.168.0.1
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.0.1
Secondary DNS Server	0.0.0.0
First Allocatable IP Address	192.168.0.2
Number of Allocatable IP Addresses	20
NAT Server	
Functionality	Disabled
Virtual Server	Disabled
DMZ Host	Not set

A-2: LED Status

There are several LED indicators on the surface of a WIASA. They are defined as follows:

- **PWR:** *Power*
- **RF:** IEEE 802.11b interface
 - **LK:** *Link*. Light up when the IEEE 802.11b interface is initialized successfully.
 - **ACT:** *Active*. Light up when the IEEE 802.11b interface is transmitting or receiving data.
- **WAN:** Ethernet WAN interface
 - **TX:** *Transmitting*. Light up when the Ethernet WAN interface is transmitting data.
 - **RX:** *Receiving*. Light up when the Ethernet WAN interface is receiving data.
- **SS1-SS4:** Status 1 to 4 for status indication
- **100/10 1-4:** 10/100 Ethernet LAN switch ports
 - **LK:** *Link*. Light up when an Ethernet cable is connected firmly to this Ethernet port.
 - **ACT:** *Active*. Light up when this Ethernet port is transmitting or receiving data.

Appendix B: Using Web-Based Network Manager

B-1: Overview

Most of the time, a user (or administrator) just wants to know the current settings of a specific WIASA, rather than change its settings. As a result, the start page of the Web-based Network Manager shows *all* the current settings of the WIASA; hence the user does not have to jump here and there by clicking hyperlinks just to see the settings values. If the user really wishes to make changes to the settings, a Web-based configuration wizard can guide the user through the step-by-step configuration process. Therefore, the user can get his or her jobs done as soon as possible.

B-2: Start Page

The start page is divided into 3 panes. At the top is the banner. The bottom-left is the main menu with 5 menu items. Clicking a menu link bring to you to the page as described by the link name. And the current settings of the WIASA are shown in the bottom-right pane.

B-3: Changing Configuration

There are 6 pages for changing configuration. They are described as follows:

1. **Welcome.** This page gives a brief description of the configuration process.
2. **Operational Mode.** On this page, the user is required to select an operational mode for the WIASA. Currently, 5 modes are available:
 - **Simple Access Point.** In this mode, the Ethernet WAN interface is disabled. The WIASA acts as a bridge between the Ethernet LAN interface and the IEEE 802.11b wireless LAN interface.
 - **Router with a PPPoE-based DSL/Cable Connection.** In this mode, the WIASA assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by PPPoE from the ISP.
 - **Router with a DHCP-based DSL/Cable Connection.** In this mode, the WIASA assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by DHCP from the ISP.
 - **Router with a Fixed-IP DSL/Cable Connection.** In this mode, the WIASA assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface must be manually set by the user or administrator.
 - **Router with a Dial-up Connection.** In this mode, the WIASA assumes that a V.90 or ISDN modem is connected to its RS232 (COM) port. The client computers can therefore share this V.90/ISDN-based Internet connection by the NAT server functionality.
3. **TCP/IP Settings.** If the user selected the **Simple Access Point** mode on the previous page, this page enables the user to set the *IP Address*, *Subnet Mask*, and *Default Gateway*. If the user selected the **Router with a PPPoE-Based DSL/Cable Connection**, **Router with a DHCP-Based DSL/Cable Connection**, **Router with a Fixed-IP DSL/Cable Connection**, or **Router with a Dial-up Connection** mode, this page enables the user to set various settings regarding IP address, PPP, PPPoE, and NAT.
4. **Wireless Settings.** This page let the user set IEEE 802.11b-relevant settings, including *Regulatory Domain*, *Channel Number*, *Network Name (SSID)*, *WEP*, and *MAC-Address-Based Access Control*.
5. **DHCP Server Settings.** This page lets the user set the TCP/IP settings that will be disseminated to the client computers through the DHCP server functionality of the WIASA.
6. **Save and Restart.** On this page, all the settings are shown for the user's final confirmation. If the user is satisfied with the settings, he or she then clicks **Save & Restart** to save the settings to the WIASA and command it to restart for the new settings to take effect.

On the left side of each configuration page, there is a simple description of the purpose of each page. At the bottom of each page, there are command buttons for the user to go forward, go back, or cancel

the configuration process. Because of this wizard-like user interface, the user could always understand what he or she is doing with the configuration parameters.

B-4: Changing Passwords

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

B-5: Upgrading Firmware

The WIASA 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 WIASA to begin downloading.

Within the folder “TftpSrvr” 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.

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

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

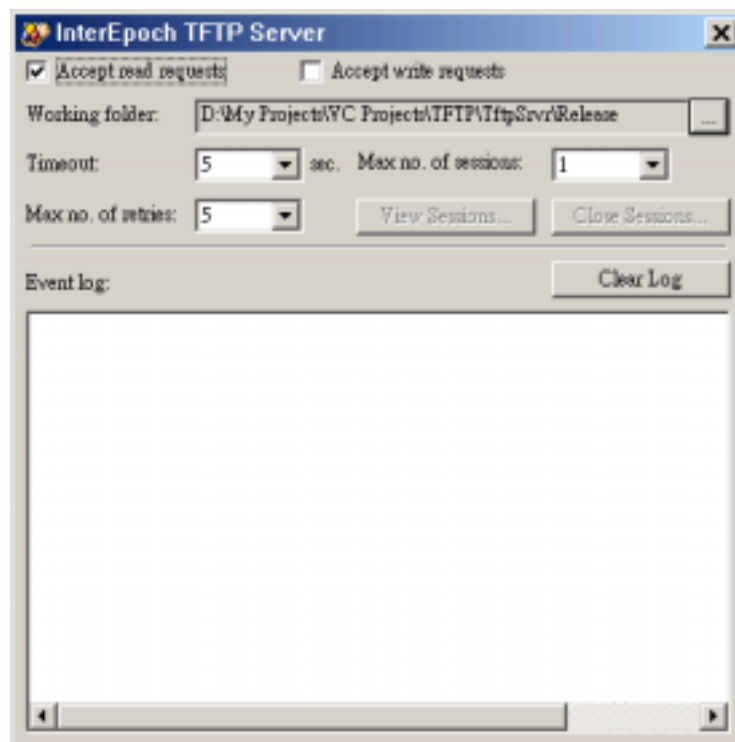


Fig. 13. InterEpoch TFTP Server.

Appendix C: Troubleshooting

Check the following first:

- Make sure that the power of the WIASA is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the WIASA.
- Make sure that the DSL, cable, V.90, or ISDN modem connected with the WIASA is powered on.
- Make sure that the LEDs on the surface of the WIASA do not indicate any errors.

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

C-2: TCP/IP Settings Problems

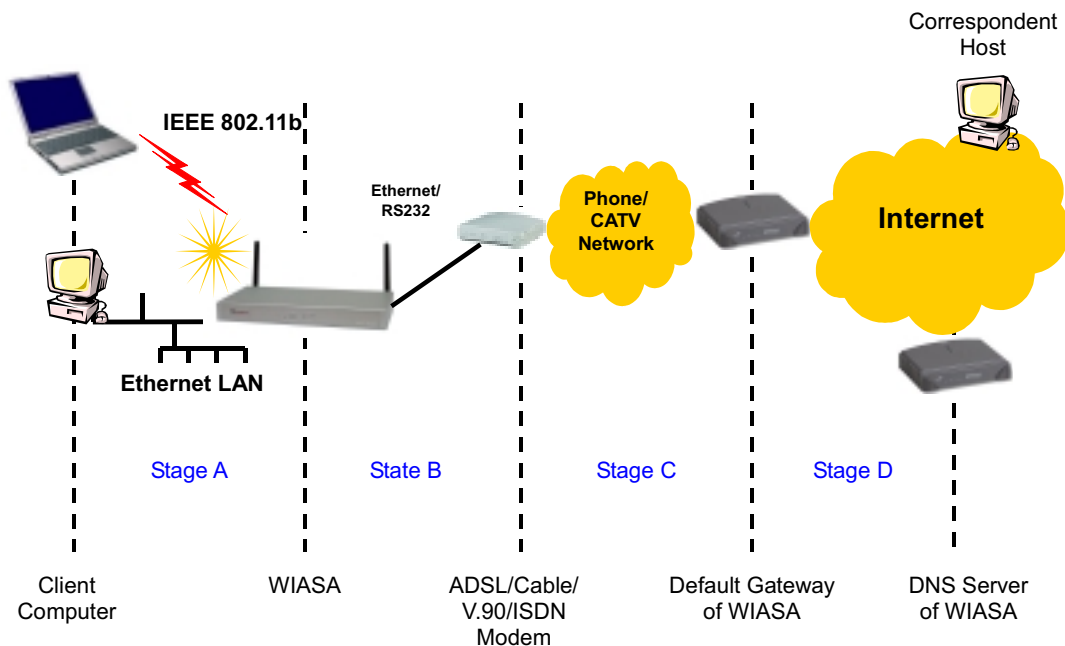


Fig. 14. Communication stages for a client to reach its correspondent host.

For a 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 WIASA, then the WIASA relays this request to the default gateway of the WIASA through a modem. 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. 14, 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 WIASA 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 the WIASA match.
- Are the IP address of the *client computer* and the IP address of the *WIASA* 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 matches that of the WIASA.
 - ◆ **TIP:** If you forget the current IP address of the WIASA and cannot remember it anyhow, the last resort may be pressing the **SF-Reset** (soft-reset) switch, while the WIASA is powered on, to restore the settings of the WIASA to factory-set values.
- **The default gateway of the WIASA does not respond to *ping* from the client computer.**
 - Solve the preceding problem first.
 - Is the modem working?
 - ◆ You may find out the answer by directly connecting the modem to a computer. Referring to the manual of the modem if necessary.
 - Are the IP address of the *WIASA* and the IP address of the *gateway* in the same IP subnet?
 - ◆ Find out the answer on the start page of the Web-Based Network Manager.
 - Is the NAT server functionality of the WIASA enabled?
 - ◆ Find out the answer on the start page of the Web-Based Network Manager.
 - If you cannot find any incorrect settings of the WIASA, the default gateway of the WIASA may be really down or there are other communication problems on the network backbone.
- **The DNS servers of the WIASA do not respond to *ping* from the client computer.**
 - Solve the preceding problems first.
 - If you cannot find any incorrect settings of the WIASA, the default gateway of the WIASA may be really down or there are other communication problems on the network backbone.

C-3: Unknown Problems

- **The WIASA stops working and does not respond to Web management requests.**
 - The firmware of the WIASA may be stuck in an incorrect state.
 - ◆ Unplug the power connector from the power jack, and then re-plug the connector to force the WIASA to restart.
 - ◆ Contact our technical support representatives to report this problem, so that the bugs

can be fixed in future firmware versions.

- If the WIASA still does not work after restarting, there may be hardware failures in the WIASA.
- ◆ Contact our technical support representatives for repairs.