



*PRZEDSIĘBIORSTWO HANDLOWE
EXPORT -IMPORT - HURT*

BIURO HANDLOWE WARSZAWA

*01-797 Warszawa
ul. Powązkowska 15
tel. 0-22 / 669 10 11
fax 0-22 / 669 11 60*

ATEL ELECTRONICS

*45-323 Opole
ul. Zielonogórska 3
tel. 0-77 / 455 60 76
fax 0-77 / 455 80 56
e-mail: cust@atel.com.pl
www.atel.com.pl*

.....
=K 9%%\$\$!F
....USER'S MANUAL

Wireless Broadband (Switch) Router

Pro/Advanced/Advanced+ User's Guide

Version: 2.12

Last Updated: 09/09/2003

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, (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 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.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.

Table of Contents

1. Introduction	1
1.1. Overview	1
1.2. Features.....	1
1.3. Feature Comparison	5
1.4. LED Definitions	5
2. First-Time Installation and Configuration	7
2.1. Inserting the Accompanying PCMCIA WLAN Card	7
2.2. Selecting a Power Supply Method.....	7
2.3. Mounting the Wireless Broadband Router on a Wall.....	7
2.4. Preparing for Configuration.....	8
2.4.1. Connecting the Managing Computer and the Wireless Broadband (Switch) Router.....	8
2.4.1.1. Router.....	8
2.4.1.2. Switch Router	9
2.4.2. Changing the TCP/IP Settings of the Managing Computer	9
2.5. Configuring the Wireless Broadband (Switch) Router	10
2.5.1. Entering the User Name and Password	10
2.5.2. ConfigWizard Step 1: Selecting an Operational Mode	12
2.5.3. ConfigWizard Step 2: Configuring TCP/IP Settings.....	12
2.5.3.1. Simple Access Point.....	12
2.5.3.2. Router with a PPPoE-Based DSL/Cable Connection.....	13
2.5.3.3. Router with a DHCP-Based DSL/Cable Connection	13
2.5.3.4. Router with a Static-IP DSL/Cable Connection	14
2.5.3.5. Router with a Dial-up Connection.....	15
2.5.4. ConfigWizard Step 3: Configuring IEEE 802.11 Settings	15
2.5.5. ConfigWizard Step 4: Reviewing and Applying Settings	16
2.6. Deploying the Wireless Broadband (Switch) Router.....	17
2.6.1. Connecting the Wireless Broadband (Switch) Router to Ethernet Client Computers	17
2.6.1.1. Router.....	17
2.6.1.2. Switch Router	17
2.6.2. Connecting the Wireless Broadband (Switch) Router to a Modem	17
2.7. Setting up Client Computers.....	18
2.7.1. Configuring IEEE 802.11b-Related Settings	18
2.7.2. Configuring TCP/IP-Related Settings.....	18
2.8. Confirming the Settings of the Wireless Broadband (Switch) Router and Client Computers	19
2.8.1. Checking if the IEEE 802.11b-Related Settings Work.....	19
2.8.2. Checking if the TCP/IP-Related Settings Work	19
2.9. Installing the Print Client Components (Switch Router).....	20
3. Using Web-Based Network Manager.....	21
3.1. Overview	21
3.1.1. Menu Structure	21
3.1.2. Save, Save & Restart, and Cancel Commands.....	22
3.1.3. Home and Refresh Commands	23
3.2. Viewing Status	23
3.2.1. Associated Wireless Clients	23
3.2.2. Current DHCP Mappings.....	24
3.2.3. System Log.....	24
3.3. General Operations	25
3.3.1. Specifying Operational Mode	25
3.3.2. Changing Password	26

3.3.3. Managing Firmware	26
3.3.3.1. Upgrading Firmware by HTTP	26
3.3.3.2. Backing up and Restoring Configuration Settings by HTTP	27
3.3.3.3. Upgrading Firmware by TFTP	27
3.3.3.4. Backing up and Restoring Configuration Settings by TFTP	29
3.3.3.5. Resetting Configuration to Factory Defaults	30
3.4. Configuring TCP/IP Related Settings	30
3.4.1. Addressing	30
3.4.1.1. Simple Access Point	31
3.4.1.2. Router with a PPPoE-Based DSL/Cable Connection	31
3.4.1.3. Router with a DHCP-Based DSL/Cable Connection	32
3.4.1.4. Router with a Static-IP DSL/Cable Connection	33
3.4.1.5. Router with a Dial-up Connection	34
3.4.2. DNS Proxy	34
3.4.2.1. Basic	35
3.4.2.2. Static DNS Mappings	35
3.4.3. NAT Server	35
3.4.3.1. Basic	35
3.4.3.2. Static NAT Mappings	36
3.4.3.3. Virtual Server Mappings	37
3.4.4. DHCP Server	38
3.4.4.1. Basic	38
3.4.4.2. Static DHCP Mappings	38
3.5. Configuring IEEE 802.11b-Related Settings	39
3.5.1. Communication	39
3.5.1.1. Basic	39
3.5.1.2. Link Integrity	39
3.5.1.3. Association Control	40
3.5.1.4. AP Load Balancing	40
3.5.1.5. Wireless Distribution System	41
3.5.2. Security	44
3.5.2.1. Basic	44
3.5.2.2. MAC-Address-Based Access Control	45
3.5.3. IEEE 802.1x/RADIUS	46
3.6. Configuring Advanced Settings	48
3.6.1. Filters and Firewall	48
3.6.1.1. Packet Filters	48
3.6.1.2. Firewall	49
3.6.1.3. URL Filters	49
3.6.2. Management	50
3.6.2.1. Remote Web-Based Management	50
3.6.2.2. UPnP	50
3.6.2.3. System Log	50
3.6.2.4. SNMP	51
Appendix A: Default Settings	52
Appendix B: Troubleshooting	54
B-1: Wireless Settings Problems	54
B-2: TCP/IP Settings Problems	55
B-3: Unknown Problems	57
Appendix C: Additional Information	58
C-1: Firmware Upgrade Using Xmodem Upgrade	58
C-2: Distances and Data Rates	59

1. Introduction

1.1. Overview

The wireless broadband (switch) 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.

There are 3 different model variations, *Pro*, *Advanced*, and *Advanced+*, which are classified in terms of features. The *Pro* edition provides the fewest features while the *Advanced+* edition provides the most. With the sleek Web-based user interface and Windows-based user interface (Wireless Network Manager), a network administrator can easily and clearly manage the wireless broadband (switch) router.

Since the wireless broadband (switch) router 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 Chapter 2, we describe the steps to install and configure a newly acquired wireless broadband (switch) router. Following the steps, the wireless broadband (switch) router can be quickly set up to work. In Chapter 3, detailed explanation of each Web management page is given for the user to understand how to fine-tune the settings of a wireless broadband router to meet his or her specific needs.

In the remainder of this guide, a wireless broadband (switch) router is often referred to as a WIASA (*Wireless Internet Access Server Appliance*) for short. In addition to using Web-based management user interface to configure a WIASA, the Windows-based Wireless Network Manager can also be used to configure and monitor deployed WIASAs. See the on-line help of Wireless Network Manager for more information.

1.2. Features

- [Operational modes](#)

- **Simple Access Point.** In this mode, the WAN interface is disabled and the device acts as a wireless-to-Ethernet IEEE 802.11b access point.
- **Router with a PPPoE-Based DSL/Cable Connection.** In this mode, the device is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by PPPoE.
- **Router with a PPPoE-Based DSL/Cable Connection.** In this mode, the device is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by DHCP.
- **Router with a Static-IP DSL/Cable Connection.** In this mode, the device is to be used with a DSL or cable modem and the IP address of the Ethernet WAN interface has to be manually configured.
- **Router with a Dial-up Connection.** In this mode, the device is to be used with a V.90

modem or ISDN TA.

- **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 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 wireless router 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. The ACL (Access Control List) can be downloaded from a TFTP server.
- **IEEE 802.1x/RADIUS.** 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).
- **Repeater.** A wireless router can communicate with other wireless APs/routers via WDS (Wireless Distribution System). Therefore, a wireless router can wirelessly forward packets from wireless clients to another wireless AP/router, and then the later AP/router forwards the packets to the Ethernet network.
- **Wireless client isolation.** 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 wireless APs/routers can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the wireless APs/routers.
- **Transmit power control.** Transmit power of the wireless router’s RF module can be adjusted to change RF coverage of the wireless router.
- **Link integrity.** When the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the wireless router and no wireless client can associate with it.
- **Association control.** The wireless router 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.** Showing the status of all wireless clients that are associated with the wireless router.
- **Detachable antennas.** The factory-mounted antennas can be replaced with high-gain antennas for different purposes.

- **Internet Connection Sharing**

- **DNS proxy.** The wireless router 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.
 - ◆ **Static DNS mappings.** The administrator can specify static FQDN (Fully Qualified Domain Name) to IP address mappings. Therefore, a host on the internal network can access a server also on the intranet by a registered FQDN.
- **DHCP server.** The wireless router can automatically assign IP addresses to client computers 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.
- **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 passthrough.** 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 unrecognized IP packets from the Internet can be forwarded to a specific computer on the intranet.
 - ◆ **Multiple public IP addresses support.** An ISP may provide several public IP addresses to a customer. The wireless router can map each of the public IP addresses to a host with a private IP address on the intranet.
 - ◆ **H.323 passthrough.** Passing H.323 packets through the intranet-Internet boundary so that users on the intranet can use VoIP (Voice over IP) applications.
 - ◆ **MSN Messenger support.** Supporting Microsoft MSN Messenger for chat, file transfer, and real-time communication applications.
- **DSL/Cable Modem Support.** Supporting dynamic IP address assignment by PPPoE (Point-to-Point Protocol over Ethernet) or DHCP and static IP address assignment.
 - **Telstra BigPond support.** Supporting Telstra BigPond (<http://www.bigpond.com>) for user authentication on the cable-based Internet connection service.
- **V.90/ISDN Modem Support.** Supporting PPP (Point-to-Point Protocol) dial-up networking over RS232.
- **Auto-dial.** When the wireless router detects outgoing packets to the Internet, it dials up to the ISP automatically. This functionality applies to PPP and PPPoE.
- **Network Security**
 - **Packet address and port filtering.** Filtering outgoing packets based on IP address and

port number. (Incoming packet filtering is performed by NAT.)

- **URL filtering.** Preventing users from accessing unwelcome Web sites. The HTTP (Hepertext Transfer Protocol) traffic to the specified Web sites identified by URLs (Universal Resource Locators) is blocked.
- **WAN ICMP requests blocking.** Some DoS (Denial of Service) attacks are based on ICMP requests with large payloads. Such kind of attacks can be blocked.
- **Stateful Packet Inspection (SPI).** Analyzing incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile.
- **Printer Sharing.** The wireless broadband switch router can serve as a print server for Windows 9x/2000 client computers.
- **Changeable MAC Address of the Ethernet WAN Interface.** Some ADSL modems work only with Ethernet cards provided by the ISP. If a wireless router is used in such an environment, the MAC address of the WAN interface of the router has to be changed to the MAC address of the ISP-provided Ethernet network card.
- **Firmware Tools**
 - **Firmware upgrade.** The firmware of the wireless router can be upgraded in the following methods:
 - ◆ **Xmodem-based.** Upgrading firmware over RS232.
 - ◆ **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).
 - ◆ **HTTP-based.** Upgrading firmware by HTTP (Hepertext Transfer Protocol).
 - **Configuration backup.** The configuration settings of the wireless router can be backed up to a file via TFTP or HTTP for later restoring.
 - **Configuration reset.** Resetting the configuration settings to factory-default values.
- **Management**
 - **Windows-based Wireless Network Manager** for configuring, monitoring, and diagnosing the local computer and neighboring wireless APs/routers. The management protocol is MAC-based.
 - **Web-based Network Manager** for configuring and monitoring the wireless broadband router via a Web browser. The management protocol is HTTP (Hepertext Transfer Protocol)-based.
 - **Remote Web-based management.** The wireless router can be managed from the Internet using a Web browser.
 - **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, and Private Enterprise MIB are supported.
 - **UPnP.** The wireless router responds to UPnP discovery messages so that a Windows XP user can locate the wireless router in My Network Places and use a Web browser to configure it.

- **Telnet.** The user is enabled to manage the wireless router by using Telnet.
- **System log.** For system operational status monitoring.
 - ◆ **Local log.** System events are logged to the on-board RAM of the wireless router 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.
- **4-Port Ethernet Switch.** The wireless broadband switch 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.
- **Power over Ethernet (optional).** Supplying power to a wireless broadband router 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 wireless router. This way, the wireless router can provide continuous services.

1.3. Feature Comparison

	<i>Pro</i>	<i>Advanced</i>	<i>Advanced+</i>
IEEE 802.1x/RADIUS		■	■
SNMP IEEE 802.1x MIB		■	■
Wireless client isolation			■
AP load balancing			■
Association control			■

- PoE is *optional* on the wireless broadband router.
- Ethernet switching and printer sharing are available only on the wireless broadband switch router.

1.4. LED Definitions

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

Wireless Broadband Router

- **PPP:** *PPP/PPPoE.* Lights up when a PPP or PPPoE link has been established.
- **ALV:** *Alive.* Blinks when the WIASA is working normally.
- **RF:** IEEE 802.11b interface
- **LAN:** Ethernet LAN interface
- **WAN:** Ethernet WAN interface
- **PWR:** Power

Wireless Broadband Switch Router

- **PWR:** *Power*
- **RF:** IEEE 802.11b interface

- **LNK:** *Link*. Lights up when the IEEE 802.11b interface is initialized successfully.
 - **ACT:** *Active*. Lights up when the IEEE 802.11b interface is transmitting or receiving data.
- **PPP:** *PPP/PPPoE*. Lights up when a PPP or PPPoE link has been established.
- **ALV:** *Alive*. Blinks when the WIASA is working normally.
- **ST1-ST2:** Status 1 to 2 for status indication
- **WAN:** Ethernet WAN interface
 - **LNK:** *Link*. Lights up when the Ethernet WAN interface is initialized successfully.
 - **ACT:** *Active*. Lights up when the Ethernet WAN interface is transmitting or receiving data.
- **100/10 1-4:** 10/100 Ethernet LAN switch ports
 - **LNK:** *Link*. Lights up when an Ethernet cable is connected firmly to this Ethernet port.
 - **ACT:** *Active*. Lights up when this Ethernet port is transmitting or receiving data.

2. First-Time Installation and Configuration

2.1. Inserting the Accompanying PCMCIA WLAN Card

For some models, the wireless interface of a WIASA 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, you have 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.

2.2. Selecting a Power Supply Method

Optionally, the wireless broadband router can be powered by the supplied power adapter or PoE (Power over Ethernet). The wireless broadband router automatically selects the suitable one depending on your decision.

To power the wireless broadband (switch) router 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 wireless broadband (switch) router.

NOTE: This product is intended to be power-supplied by a Listed Power Unit, marked "Class 2" or "LPS" and output rated "5V DC, 1 A minimum" or equivalent statement.

To power the wireless broadband router by PoE:

1. Plug one connector of an Ethernet cable to an available port of a PoE hub.
2. Plug the other connector of the Ethernet cable to the **LAN/CONFIG** port of the wireless broadband router.

NOTE: The PoE capability of the bridge is PowerDsine-compatible. Please visit the Web site of PowerDsine for more information (<http://www.powerdsine.com>).

2.3. Mounting the Wireless Broadband Router on a Wall

The wireless broadband router is wall-mountable.

1. Stick the supplied sticker for wall-mounting.
2. Use a $\phi 7.0$ mm 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 screw in each plastic conical anchor for a proper depth so that the wireless broadband router can be hung on the screws.
5. Hang the wireless broadband router on the screws.

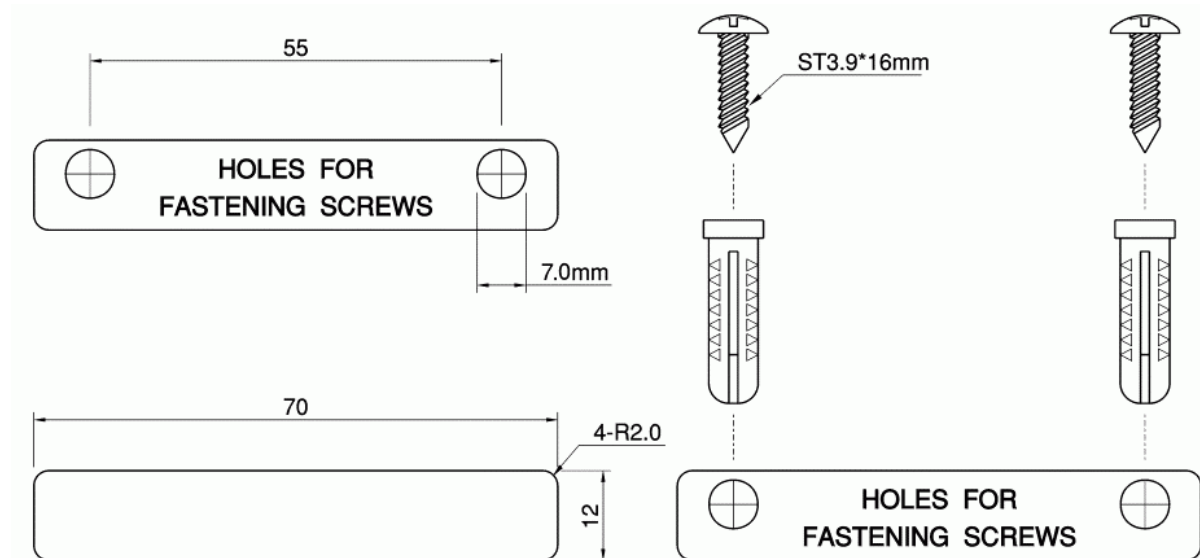


Fig. 1. Mounting the wireless broadband router on a wall.

2.4. Preparing for Configuration

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

NOTE: If you are using the browser, *Opera*, to configure a WIASA, 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 WIASA.

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.

2.4.1. Connecting the Managing Computer and the Wireless Broadband (Switch) Router

2.4.1.1. Router

To connect the Ethernet managing computer and the managed router for first-time configuration, you have two choices as illustrated in Fig. 3.

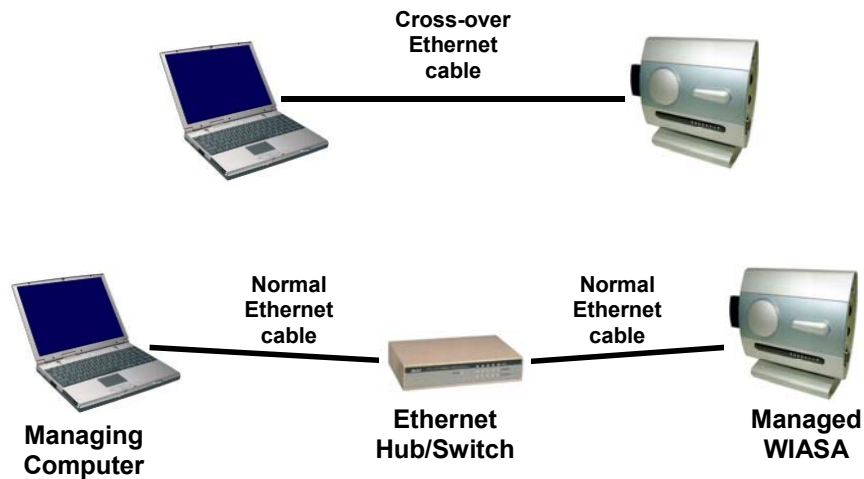


Fig. 2. Connecting a managing computer and a wireless broadband router via Ethernet.

You can use either a *cross-over* Ethernet cable (included in the package) or a switch/hub with 2 normal Ethernet cables. Since the DHCP server functionality is factory-set to be enabled, it's recommended that there are no other computers connected to the switch/hub, so that you can be 100-percent sure that the WIASA will be the DHCP server of the managing computer.

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

2.4.1.2. Switch Router

Connect the Ethernet managing computer to anyone of the LAN switch ports of the managed WIASA with a normal Ethernet cable (see Fig. 3).

NOTE: There are two types of Ethernet cables—*normal* and *crossover*.

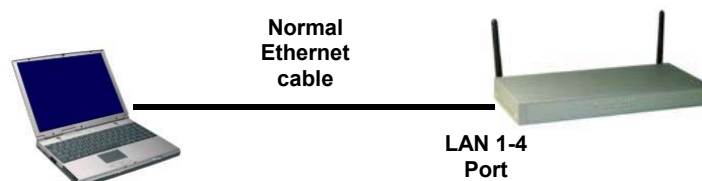


Fig. 3. Connecting a managing computer and a wireless broadband switch router via Ethernet.

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 you can be 100-percent sure that the WIASA will be the DHCP server of the managing computer.

2.4.2. 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, you 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 be restarted for the changes of TCP/IP settings to take effect.

TIP: After you have connected the managing computer and the WIASA via Ethernet, you can install Wireless Network Manager on the managing computer and use it to configure the WIASA 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.

If the computer is already set to obtain an IP address automatically, you can use the Windows-provided tool, **WinIPCfig.exe** (on Windows 9x/Me) or **IPConfig.exe** (on Windows 2000/XP), to re-obtain an IP address from the WIASA. **WinIPCfig.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**.

2.5. Configuring the Wireless Broadband (Switch) 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.

2.5.1. 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.

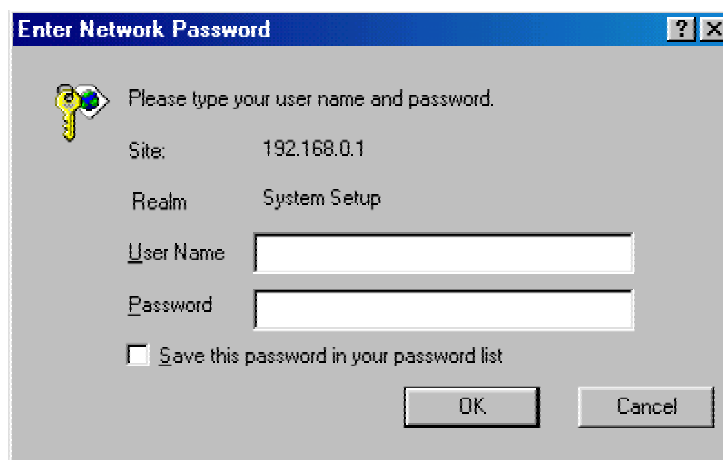


Fig. 4. Entering the user name and password.

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 3.3.2 for more information).

TIP: Since the start page shows the current settings and status of the WIASA, it can be saved or printed within the Web browser for future reference.

On the start page, click the **ConfigWizard** link to use a configuration wizard to quickly change the configuration of the WIASA.

Wireless Broadband Router Settings and Info	
Model	Router Adv+
BIOS/Firmware Version	BRYs v1.30/1.5.10.3190
Operational Mode	Router with a Static-IP DSL/Cable Connection
MAC Address (BSSID)	00-06-F4-00-B8-19
System Up Time (hr:min:sec)	0:00:14
	WAN Interface <ul style="list-style-type: none"> • IP address: 192.168.100.1 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0 • Custom MAC address of WAN interface: Disabled LAN Interface <ul style="list-style-type: none"> • IP address: 192.168.168.88 • Subnet mask: 255.255.255.0 • NAT: Enabled

Fig. 5. 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. We'll explain what to do step-by-step in the following subsections.

2.5.2. ConfigWizard Step 1: Selecting an Operational Mode

<input type="radio"/> Simple Access Point
<input type="radio"/> Router with a PPPoE-Based DSL/Cable Connection
<input type="radio"/> Router with a DHCP-Based DSL/Cable Connection
<input checked="" type="radio"/> Router with a Static-IP DSL/Cable Connection
<input type="radio"/> Router with a Dial-up Connection

Fig. 6. Operational modes.

- 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 **Router with a PPPoE-Based DSL/Cable Connection**.
- 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 **Router with a DHCP-Based DSL/Cable Connection**.
- If the WIASA is to be used with a DSL or cable modem and the IP address of the Ethernet WAN interface has to be manually set, select **Router with a Static-IP DSL/Cable Connection**.
- If the WIASA is to be used with a V.90 modem or ISDN TA, select **Router with a Dial-up Connection**.

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.

2.5.3. ConfigWizard Step 2: Configuring TCP/IP Settings

2.5.3.1. Simple Access Point

Method of obtaining an IP address:	<input type="text" value="Set Manually"/>
IP address:	<input type="text" value="192.168.0.88"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Default gateway:	<input type="text" value="192.168.0.1"/>
Host name:	<input type="text" value="router"/>

Fig. 7. TCP/IP settings for **Simple Access Point** mode.

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. In addition, you can specify the **Host name** of the WIASA.

2.5.3.2. Router with a PPPoE-Based DSL/Cable Connection

Ethernet WAN Interface	
User name:	<input type="text" value="username"/>
Password:	<input type="text"/>
Password again:	<input type="text"/>
Service name:	<input type="text" value="servicename"/>
Idle disconnect time (min.):	<input type="text" value="1"/>
Host name:	<input type="text" value="router"/>
Ethernet/Wireless LAN Interfaces	
IP address:	<input type="text" value="192.168.0.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>

Fig. 8. TCP/IP settings for **Router with a PPPoE-Based DSL/Cable Connection** 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.

The WIASA automatically disconnects the PPPoE connection after there has been no traffic to the Internet for a period specified by **Idle disconnect time**.

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

2.5.3.3. Router with a DHCP-Based DSL/Cable Connection

Ethernet WAN Interface	
Host name:	<input type="text" value="router"/>
Heartbeat for BigPond Cable	
<input type="checkbox"/> Connect with BigPond Cable	
User name:	<input type="text"/>
Password:	<input type="text"/>
Login server:	<input type="text"/>
Ethernet/Wireless LAN Interfaces	
IP address:	<input type="text" value="192.168.0.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>

Fig. 9. TCP/IP settings for **Router with a DHCP-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. If you are using Telstra BigPond cable-based Internet service, select the **Connect with BigPond Cable** check box and specify the **User name**, **Password**, and the IP address of your **Login server**, which is provided by your ISP.

2.5.3.4. Router with a Static-IP DSL/Cable Connection

Ethernet WAN Interface	
IP address:	<input type="text" value="192.168.100.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Default gateway:	<input type="text" value="0.0.0.0"/>
Ethernet/Wireless LAN Interfaces	
IP address:	<input type="text" value="192.168.0.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
DNS Proxy	
Functionality:	<input type="text" value="Enabled"/> ▼
Primary DNS server:	<input type="text" value="0.0.0.0"/>
Secondary DNS server:	<input type="text" value="0.0.0.0"/>

Fig. 10. TCP/IP settings for **Router with a Static-IP DSL/Cable Connection** mode.

If the WIASA was set to be in **Router with a Static-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. Consult your ISP for the correct **IP address**, **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings.

2.5.3.5. Router with a Dial-up Connection

Dial-Up WAN Interface	
ISP Telephone number:	<input type="text"/>
User name:	<input type="text" value="username"/>
Password:	<input type="text"/>
Password again:	<input type="text"/>
Idle disconnect time (min.):	<input type="text" value="1"/>
Host name:	<input type="text" value="router"/>
Ethernet/Wireless LAN Interfaces	
IP address:	<input type="text" value="192.168.0.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>

Fig. 11. TCP/IP settings for **Router with a Dial-up Connection** mode.

If the WIASA was set to be in **Router 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.

The WIASA automatically disconnects the PPP dial-up connection after there has been no traffic to the Internet for a period specified by **Idle disconnect time**.

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

2.5.4. ConfigWizard Step 3: Configuring IEEE 802.11 Settings

IEEE 802.11b-related communication settings include **Regulatory domain**, **Channel number**, and **Network name (SSID)**.

Regulatory domain:	<input type="text" value="FCC (U.S.)"/>
Channel number:	<input type="text" value="11"/>
Network name (SSID):	<input type="text" value="wireless"/>

Fig. 12. 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 WIASA must be identical for them to communicate with each other.

2.5.5. ConfigWizard Step 4: Reviewing and Applying Settings

Wireless Broadband Router Settings and Info	
Model	Router Adv+
BIOS/Firmware Version	BRYS v1.30/1.5.10.3190
Operational Mode	Router with a PPPoE-based DSL/Cable Connection
MAC Address (BSSID)	00-06-F4-00-B8-19
System Up Time (hr:min:sec)	0:03:00
	WAN Connection Status: <ul style="list-style-type: none"> • Acquired IP: 192.168.100.1 • Acquired netmask: 255.255.255.0 • Acquired DNS server 1: 0.0.0.0 • Acquired DNS server 2: 0.0.0.0 WAN Interface <ul style="list-style-type: none"> • Service name: servicename • User name: david • Password: 12345

Fig. 13. Settings changes are highlighted in red.

Wireless Settings	<ul style="list-style-type: none"> • Regulatory domain: FCC (U.S.) • Channel number: 6 • Transmit power: High (16~17 dBm) • Network name (SSID): wireless • Security mode: Open System • Authentication algorithm: Auto • AP functionality: Enabled • SSID broadcasts: Enabled • Wireless client isolation: Disabled • MAC-address-based access control: Disabled • AP load balancing: Disabled • Number of WDS links: 0
<p><< Back Save & Restart Cancel</p>	

Fig. 14. Settings review.

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 7 seconds are needed for the WIASA to complete its restart process.

2.6. Deploying the Wireless Broadband (Switch) Router

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

2.6.1. Connecting the Wireless Broadband (Switch) Router to Ethernet Client Computers

2.6.1.1. Router

To connect the router with Ethernet client computers:

1. Plug one connector of a *normal* Ethernet cable to the **LAN/CONFIG** Ethernet jack of the WIASA.
2. Plug the other connector of this cable to a free Ethernet port of the switch/hub, to which all the Ethernet client computers have been connected.

2.6.1.2. Switch Router

To connect the switch router with Ethernet client computers:

1. Plug one connector of a *normal* (not *crossover*) Ethernet cable to a **LAN** Ethernet switch port of the WIASA, and the other connector 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.

2.6.2. Connecting the Wireless Broadband (Switch) Router to a Modem

To connect the WIASA with a DSL or cable modem:

1. Plug one connector of a *crossover* 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 modem. Refer to the user's manual of the modem if necessary.

TIP: If the WIASA has been connected to the DSL or cable modem successfully, the **WAN** LED indicator on the housing lights up when both devices are powered on. If not, flip the **Normal/Crossover**

switch on the side plate of the WIASA (if it exists), flip the switch until the **WAN** LED indicator lights on.

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

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 modem or ISDN TA. Refer to the user's manual of the modem or TA if necessary.

2.7. Setting up Client Computers

Before the client computers can use the services provided by the WIASA, their TCP/IP settings must be configured 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.

2.7.1. 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 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 associate with a wireless access point or broadband router.

NOTE: The SSID of the wireless client computer and the SSID of the WIASA must be identical. Or, in case the **SSID broadcasts** capability of the WIASA is enabled (by default), the SSID of the wireless client computer could be set to "any".

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

NOTE: For better wireless security, IEEE 802.1x capability of the WIASA 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.

2.7.2. 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 WIASA 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 WIASA, or select an automatically-obtain-an-IP-address option if the DHCP server functionality of the WIASA is enabled.

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

If the computer is already set to obtain an IP address automatically, you 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.

2.8. Confirming the Settings of the Wireless Broadband (Switch) 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.

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

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

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 WIASA.

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

2.8.2. 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 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 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 client computer. Then press **Enter**.

NOTE: If the WIASA is set to be in *router* 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 B-2, “TCP/IP Settings Problems” for troubleshooting.

4. Type “**ping wiasa_default_gateway**”, where *wiasa_default_gateway* is a placeholder for the IP address of the default gateway of the WIASA. Then press **Enter**.

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

TIP: You can view the default gateway of the WIASA on the start page of the Web-based Network Manager.

NOTE: If the WIASA is set to be in **Router with a PPPoE-Based DSL/Cable Connection** or **Router with a Dial-up Connection**, it needs some time to establish a PPPoE or PPP link to the ISP. Therefore, this step will fail but the WIASA will be triggered to establish a link to the ISP. Wait for a few seconds, and then try again.

5. 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 B-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.

6. 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 B-2, “TCP/IP Settings Problems” for troubleshooting.

2.9. Installing the Print Client Components (Switch Router)

The print server components on the WIASA work in conjunction with the print client components on a client computer, and they communicate through 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 companion CD-ROM disk of the WIASA 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’s *LAN interfaces* 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.

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

Wireless Broadband Router Settings and Info	
Model	Router Adv+
BIOS/Firmware Version	BRY8 v1.30/1.5.10.3190
Operational Mode	Router with a Static-IP DSL/Cable Connection
MAC Address (BSSID)	00-06-F4-00-B8-19
System Up Time (hr:min:sec)	0:00:14
	WAN Interface
	• IP address: 192.168.100.1
	• Subnet mask: 255.255.255.0
	• Default gateway: 0.0.0.0
	• Custom MAC address of WAN interface: Disabled
	LAN Interface
	• IP address: 192.168.168.88
	• Subnet mask: 255.255.255.0
	• NAT: Enabled

Fig. 15. The Start page.

3.1.1. Menu Structure

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

- **Home.** For going back to the start page.
- **ConfigWizard.** For you to quickly set up the WIASA.
- **Status.** Status information.
 - **Wireless Clients.** The status of the wireless clients currently associated with the WIASA.
 - **DHCP Mappings.** Current IP-MAC address mappings.
 - **System Log.** System events log.

- **General.** Global operations.
 - **Operational Mode.** Operational mode of the WIASA based on the type of the Internet connection provided by the ISP.
 - **Password.** For gaining rights to change the settings of the WIASA.
 - **Firmware Tools.** For upgrading the firmware of the WIASA, backing up and restoring configuration, and configuration reset settings of the WIASA.
- **TCP/IP.** TCP/IP-related settings.
 - **Addressing.** IP address settings for the WIASA to work with TCP/IP, or user name and password provided by the ISP.
 - **DNS Proxy.** DNS (Domain Name System) proxy settings.
 - **NAT Server.** Settings for the NAT (Network Address Translation) server on the WIASA.
 - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the WIASA.
- **IEEE 802.11.** IEEE 802.11b-related settings.
 - **Communication.** Basic settings for the IEEE 802.11b interface of the WIASA 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 WIASA.
 - **Filters & Firewall.** Packet filtering and firewall settings for user access control and protection from hacker attacks from the Internet, respectively.
 - **Management.** Remote Web-based management, UPnP, System Log, and SNMP settings.

3.1.2. Save, Save & Restart, and Cancel Commands



Fig. 16. 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 WIASA and brings you back to the start page. Clicking **Save & Restart** stores the settings changes to the memory of the WIASA and restarts the WIASA 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 WIASA for the settings changes to take

effect.

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

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

Wireless Broadband Router Settings and Info	
Model	Router Adv+
BIOS/Firmware Version	BRYS v1.30/1.5.10.3190
Operational Mode	Router with a DHCP-based DSL/Cable Connection
MAC Address (BSSID)	00-06-F4-00-B8-19
System Up Time (hr:min:sec)	0:05:06
	WAN Connection Status: <ul style="list-style-type: none"> • Acquired IP: 192.168.100.1 • Acquired netmask: 255.255.255.0 • Acquired DNS server: 0.0.0.0 WAN Interface <ul style="list-style-type: none"> Obtain from a DHCP server • Custom MAC address of WAN interface: Disabled Heartbeat <ul style="list-style-type: none"> • Heartbeat login: Disabled • User name:

Fig. 17. Settings have been changed.

3.1.3. Home and Refresh Commands



Fig. 18. Home and Refresh.

At the bottom of each status page that shows read-only information, there are two buttons—**Home** and **Refresh**. Clicking **Home** brings you back to the start page. Clicking **Refresh** updates the shown status information.

3.2. Viewing Status

3.2.1. Associated Wireless Clients

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

Fig. 19. Status of associated wireless clients.

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1x authenticated), number of bytes it has send, number of bytes it has received, and the time of its last activity, is shown.

3.2.2. Current DHCP Mappings

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

Fig. 20. Current DHCP mappings.

On this page, all the current *static* or *dynamic* DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

A static mapping indicates that the DHCP client always obtains the specified IP address from the DHCP server. You can set static DHCP mappings in the **Static DHCP Mappings** section of the **DHCP Server** configuration page (see Section 3.4.4). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool specified by the **First allocateable IP address** and **Allocateable IP address count** settings on the **DHCP Server** configuration page.

3.2.3. System Log

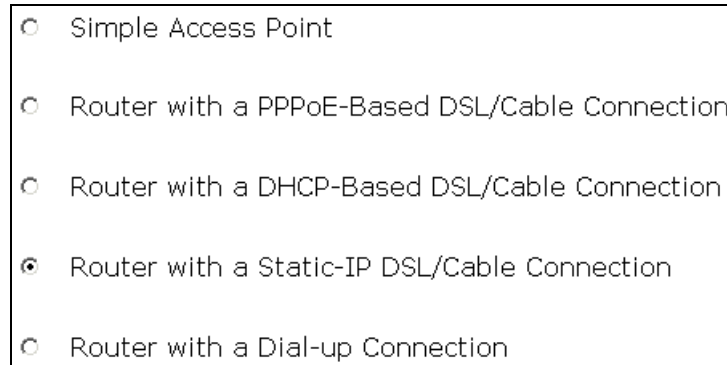
Model:	Router Adv+
BIOS/Firmware version:	BRY5 v1.30/1.5.10.3190
Operational mode:	Router with a Static-IP DSL/Cable connection
Current time:	12/26/2002 17:16:45
<hr/>	
12/26/2002 16:51:49 SYSTEM START UP!	
12/26/2002 16:51:49 Wireless LAN interface initializes success	
12/26/2002 16:51:49 BSSID --> 00-06-F4-00-B8-19	
12/26/2002 16:51:49 LAN IP address --> 192.168.168.88	
12/26/2002 16:51:49 WAN IP address --> 192.168.100.1	
12/26/2002 16:51:49 Default router IP address --> 0.0.0.0	
12/26/2002 16:51:49 Primary DNS IP address --> 0.0.0.0	
12/26/2002 16:51:49 Secondary DNS IP address --> 0.0.0.0	

Fig. 21. System log.

System events such as PPPoE dialup results are recorded in the memory of the WIASA. The logged information is useful for troubleshooting purposes. For example, if the password configured for PPPoE is incorrect, this error can be easily spotted by inspecting the system log. The system events are divided into several categories, and you can select which categories of events to log. See Section 3.6.2.3 for more information.

3.3. General Operations

3.3.1. Specifying Operational Mode



A screenshot of a configuration interface showing five radio button options for operational modes. The options are: Simple Access Point, Router with a PPPoE-Based DSL/Cable Connection, Router with a DHCP-Based DSL/Cable Connection, Router with a Static-IP DSL/Cable Connection (which is selected), and Router with a Dial-up Connection.

- Simple Access Point
- Router with a PPPoE-Based DSL/Cable Connection
- Router with a DHCP-Based DSL/Cable Connection
- Router with a Static-IP DSL/Cable Connection
- Router with a Dial-up Connection

Fig. 22. Operational modes.

On this page, you can specify the 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 Static-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.
- **Router with a Dial-up Connection.** In this mode, the WIASA assumes that a V.90 modem or ISDN TA 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.

TIP: When you have selected the operational mode of the WIASA, go to the **TCP/IP, Addressing** section of the management UI (see Section 3.4.1) to configure the addressing settings of the WAN and LAN interfaces.

3.3.2. Changing Password

Old password:	<input type="password" value="****"/>
New user name:	<input type="text" value="admin"/>
New password:	<input type="password" value="*****"/>
New password again:	<input type="password" value="*****"/>

Fig. 23. Password.

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

3.3.3. Managing Firmware

Firmware management protocol:	<input type="text" value="HTTP"/>
-------------------------------	-----------------------------------

Fig. 24. Firmware management protocol setting.

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

TIP: You can use Upgrade Wizard of Wireless Network Manager to upgrade firmware. See the on-line help of Wireless Network Manager for more information.

3.3.3.1. Upgrading Firmware by HTTP

Firmware Upgrade	
Firmware file name:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/>	

Fig. 25. Firmware upgrade by HTTP.

To upgrade firmware of the WIASA by HTTP:

1. Click **Browse** and then select a correct firmware **.bin** file. The firmware file path will be shown in the **Firmware file name** text box.
2. Click **Upgrade** to begin the upgrade process.

3.3.3.2. Backing up and Restoring Configuration Settings by HTTP

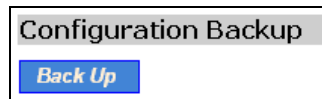


Fig. 26. Firmware backup by HTTP.

To back up configuration of the WIASA 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 WIASA's MAC address. For example, if the WIASA'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.

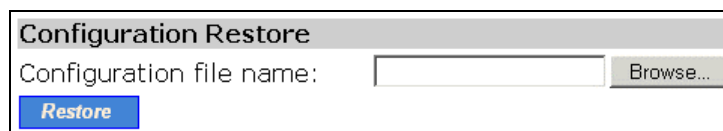


Fig. 27. Configuration restore by HTTP.

To restore configuration of the WIASA by HTTP:

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

3.3.3.3. Upgrading Firmware by TFTP

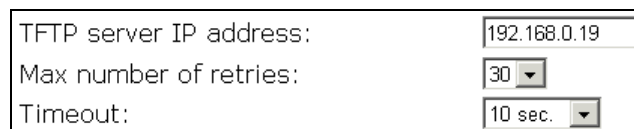


Fig. 28. TFTP server settings.

When use TFTP as the firmware management protocol, you can configure settings for the WIASA's TFTP client to communicate with a TFTP server. If the TFTP client does not get a response from the TFTP server within a period specified by the **Timeout** setting, it will resend the previous request. The **Max number of retries** setting specifies the maximal number of resend before the TFTP client stops communicating with the TFTP server.

Within the folder "Utilities" on the companion CD-ROM disk, we offered a TFTP server program (**TftpSrvr.exe**) for firmware upgrade. Run this program on the computer that is to serve as a TFTP server.

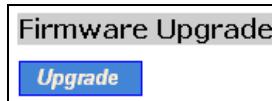


Fig. 29. Firmware upgrade by TFTP.

To upgrade firmware of the WIASA by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure IP address of the computer so that the WIASA and the computer are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.
8. Trigger the firmware upgrade process by clicking **Upgrade**.

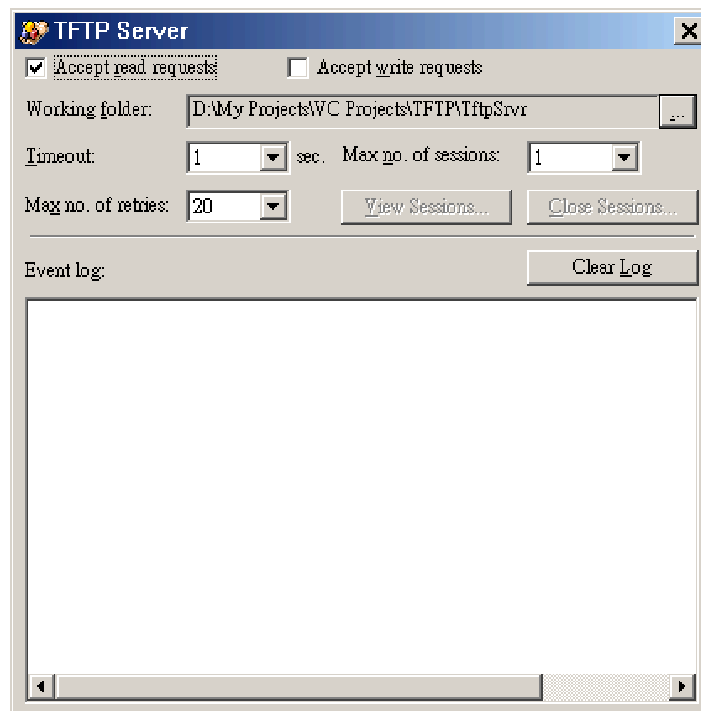


Fig. 30. TFTP Server.

NOTE: After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.

NOTE: Make sure the **Accept read requests** check box of TFTP Server is selected.

NOTE: The LAN IP address of the WIASA and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless WIASA 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 WIASA unstartable. When this occurs, call for technical support.

TIP: The firmware of a *deployed* WIASA can also be upgraded remotely from the Internet. In this case, you must have configured the WIASA to be remotely manageable (see Section 3.6.2.1) and adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP upgrade to succeed.

3.3.3.4. Backing up and Restoring Configuration Settings by TFTP



Fig. 31. Configuration backup/restore.

To back up configuration of the WIASA by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the backup process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the WIASA are in the same IP subnet.
4. On the computer, run the TFTP Server utility. Select the **Accept write requests** check box, and specify the folder to which the configuration settings of the WIASA will be saved.
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.
8. Trigger the backup process by clicking **Back Up**. The WIASA's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "AaBbCcDdEeFf" is the WIASA's MAC address. For example, if the WIASA's MAC address is 00-01-02-33-44-55, the configuration backup file will be "000102334455.hex".

NOTE: Remember to select the **Accept write requests** check box of TFTP Server.

To restore configuration of the WIASA by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the restoring process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the WIASA are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the configuration backup file resides. A configuration backup file is named by the WIASA's MAC address. For example, if the WIASA's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.
8. Trigger the restoring process by clicking **Restore**. The WIASA will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the WIASA.

TIP: The configuration of a *deployed* WIASA can also be backed up or restored remotely from the Internet. In this case, you must have configured the WIASA to be remotely manageable (see Section 3.6.2.1) and adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

3.3.3.5. Resetting Configuration to Factory Defaults

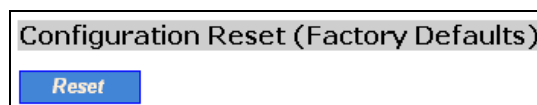


Fig. 32. Configuration reset.

Clicking the **Reset** button resets the device configuration to factory defaults.

WARNING: Think twice before clicking the **Reset** button. You'll lose all your current configuration settings.

3.4. Configuring TCP/IP Related Settings

3.4.1. Addressing

The addressing settings depend on the operational mode of the WIASA. Each operational mode requires different addressing settings.

3.4.1.1. Simple Access Point

Method of obtaining an IP address:	Set Manually
IP address:	192.168.0.88
Subnet mask:	255.255.255.0
Default gateway:	192.168.0.1
Host name:	router
Domain (DNS suffix):	

Fig. 33. TCP/IP settings for **Simple Access Point** mode.

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. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the WIASA.

3.4.1.2. Router with a PPPoE-Based DSL/Cable Connection

Ethernet WAN Interface	
<input type="checkbox"/> Custom MAC address of WAN interface:	00-06-F4-00-B8-19
User name:	david
Password:	*****
Password again:	*****
Service name:	servicename
Idle disconnect time (min.):	1
Host name:	router
Domain (DNS suffix):	
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 34. TCP/IP settings for **Router with a PPPoE-Based DSL/Cable Connection** 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.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the WIASA can mimic the

ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

The WIASA automatically disconnects the PPPoE connection after there has been no traffic to the Internet for a period specified by **Idle disconnect time**.

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

3.4.1.3. Router with a DHCP-Based DSL/Cable Connection

The screenshot shows a configuration window titled "Ethernet WAN Interface". It contains several sections:

- Ethernet WAN Interface**:
 - Custom MAC address of WAN interface: 00-06-F4-00-B8-19
 - Host name: router
 - Domain (DNS suffix):
- Heartbeat for BigPond Cable**:
 - Connect with BigPond Cable
 - User name:
 - Password:
 - Login server:
- Ethernet/Wireless LAN Interfaces**:
 - IP address: 192.168.0.1
 - Subnet mask: 255.255.255.0

Fig. 35. TCP/IP settings for **Router with a DHCP-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. If you are using Telstra BigPond cable-based Internet service, select the **Connect with BigPond Cable** check box and specify the **User name**, **Password**, and the IP address of your **Login server**, which is provided by the ISP.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the WIASA can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

3.4.1.4. Router with a Static-IP DSL/Cable Connection

Ethernet WAN Interface	
<input type="checkbox"/> Custom MAC address of WAN interface:	00-06-F4-00-B8-19
IP address:	192.168.100.1
Subnet mask:	255.255.255.0
Default gateway:	0.0.0.0
Host name:	router
Domain (DNS suffix):	
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 36. TCP/IP settings for **Router with a Static-IP DSL/Cable Connection** mode.

If the WIASA was set to be in **Router with a Static-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. Consult your ISP for the correct **IP address**, **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the WIASA can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

3.4.1.5. Router with a Dial-up Connection

Dial-Up WAN Interface	
ISP Telephone number:	<input type="text" value="86650305"/>
User name:	<input type="text" value="david"/>
Password:	<input type="password" value="*****"/>
Password again:	<input type="password" value="*****"/>
Idle disconnect time (min.):	<input type="text" value="1"/>
Host name:	<input type="text" value="router"/>
Domain (DNS suffix):	<input type="text"/>
AT Commands	
Modem init command 1:	<input type="text" value="ATLD"/>
Modem init command 2:	<input type="text"/>
Hang-up command:	<input type="text" value="ATH"/>
Ethernet/Wireless LAN Interface	
IP address:	<input type="text" value="192.168.0.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>

Fig. 37. TCP/IP settings for **Router with a Dial-up Connection** mode.

If the WIASA was set to be in **Router 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.

The WIASA automatically disconnects the PPP dial-up connection after there has been no traffic to the Internet for a period specified by **Idle disconnect time**.

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

The **AT commands** settings are for modem compatibility. The default AT commands for dial-up and hang-up are suitable for most modems. However, if your modem or TA needs special AT commands for these purposes, set them in the corresponding fields. You may need to consult the manual of the modem or TA for proper AT commands.

3.4.2. DNS Proxy

The DNS Proxy component of the WIASA forwards DNS requests and reply messages between client computers and DNS servers. To client computers, the WIASA acts like a DNS server; to DNS servers, the WIASA acts like a client.

3.4.2.1. Basic

Functionality:	Enabled ▾
Primary DNS server:	0.0.0.0
Secondary DNS server:	0.0.0.0

Fig. 38. Basic DNS proxy settings.

In this section of the page, you can specify the IP addresses of the DNS servers, when the WIASA is in **Router with a Static-IP DSL/Cable Connection** mode. In other modes, the WIASA obtains the DNS server information automatically from the ISP.

3.4.2.2. Static DNS Mappings

Enabled	Domain Name	IP Address
<input type="checkbox"/>	www.company-name.com	192.168.0.201
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Fig. 39. Static DNS mappings.

By **Static DNS Mappings**, an internal server can be given a domain name, so that other hosts on the intranet can access the server by its domain name instead of by its IP address. For example, an internal Web server for the intranet, say 192.168.0.2, may be associated with the domain name, www.wiasa.com.

To give an internal server a domain name:

1. Specify the domain name and the private IP address of the internal server.
2. Select the corresponding **Enabled** check box for the internal server.

3.4.3. NAT Server

3.4.3.1. Basic

Functionality:	Enabled ▾
<input type="checkbox"/> DMZ host:	

Fig. 40. Basic NAT server settings.

When the WIASA is in **Router with a Static-IP DSL/Cable Connection** mode, the NAT server functionality can be enabled or disabled.

A DMZ (*DeMilitarized Zone*) host receives all unrecognized TCP/IP packets from the NAT server on the WIASA; therefore TCP/IP networking applications running on the DMZ host would have better compatibility with NAT.

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.

3.4.3.2. Static NAT Mappings

Enabled	Public IP Address	Private IP Address
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Fig. 41. Static NAT mappings.

An ISP may provide more than one *public* IP address to its customer. A customer could use each of the public IP addresses for one type of server to be accessed from the Internet. This requirement can be satisfied by **Static NAT Mappings**. This functionality can be enabled only when the WIASA is in **Router with a Static-IP DSL/Cable Connection** mode.

For example, say an ISP provides 5 public IP addresses, 61.16.33.114 to 61.16.33.118 inclusive, to its customer, WIASA Technology. The network administrator of WIASA Technology decides to use 61.16.33.114 for the wireless broadband router, 61.16.33.115 for their public Web server, and 61.16.33.116 for their public POP3 server. And the administrator has registered with InterNIC (Internet Network Information Center) some domain name-to-IP address mappings—www.wiasa.com to 61.16.33.115 and pop3.wiasa.com to 61.16.33.116. However, the public Web server and POP3 server for WIASA Technology sit on the intranet and use private IP addresses, 192.168.0.2 and 192.168.0.3, respectively. To expose the servers in this situation, the network administrator needs two static NAT mappings to associate 61.16.33.115 with 192.168.0.2 and 61.16.33.116 with 192.168.0.3, respectively.

To associate a public IP address with a private IP address:

1. Specify the public IP address and the private IP address for the association.
2. Select the corresponding **Enabled** check box.

3.4.3.3. Virtual Server Mappings

Enabled	Service Name	Private IP Address	Port	Protocol
<input type="checkbox"/>	FTP	192.168.0.201	21	TCP
<input type="checkbox"/>	IMAP4		143	TCP
<input type="checkbox"/>	SMTP		25	TCP
<input type="checkbox"/>	POP3		110	TCP
<input type="checkbox"/>	TELNET		23	TCP
<input type="checkbox"/>	HTTP		80	TCP
<input type="checkbox"/>			0	TCP
<input type="checkbox"/>			0	TCP
<input type="checkbox"/>			0	TCP
<input type="checkbox"/>			0	TCP

Fig. 42. Virtual server mappings.

The WIASA enables you to expose internal servers on the intranet through NAT to the Internet for public use. The exposed internal servers are called *virtual servers* because from perspective of hosts on the Internet, these servers are invisible in terms of TCP/IP.

To expose “preset” internal servers:

1. Select the corresponding **Enabled** check boxes for the kinds of servers (FTP, IMAP4, SMTP, POP3, TELNET, and HTTP) you want to expose.
2. Specify the private IP addresses of the internal servers.

To expose other internal servers:

1. Specify the **Service Name**, **Private IP Address**, **Port Number**, and whether the service is *TCP-based* or *UDP-based* for a non-preset internal server you want to expose.
2. Select the corresponding **Enabled** check box for the internal server.
3. Repeat Steps 1 to 2 for other non-preset internal servers.

3.4.4. DHCP Server

3.4.4.1. Basic

Functionality:	Enabled
Default gateway:	192.168.0.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.0.1
Secondary DNS server:	
First allocatable IP address:	192.168.0.2
Allocatable IP address count:	20

Fig. 43. Basic DHCP server settings.

The WIASA 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.

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.

3.4.4.2. Static DHCP Mappings

Enabled	Desc.	MAC Address	IP Address
<input type="checkbox"/>	Bill	00-22-32-5D-80-02	192.168.0.203
<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. 44. Static DHCP mappings.

IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. By **Static DHCP Mappings**, you can ensure that a host will get the same IP address when

it requests one from the DHCP server. Therefore, instead of configuring the IP address of an intranet server manually, you can configure the server to obtain an IP address by DHCP and it is always assigned the same IP address.

To always assign a static IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. Then, give a description for this mapping.
2. Select the corresponding **Enabled** check box.

3.5. Configuring IEEE 802.11b-Related Settings

3.5.1. Communication

3.5.1.1. Basic

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

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

Fig. 45. IEEE 802.11b basic communication settings.

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

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 WIASA 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 WIASA can be adjusted so that the RF coverage of the WIASA can be changed.

3.5.1.2. Link Integrity

Functionality:	Disabled
Reference host:	0.0.0.0

Fig. 46. Link integrity settings.

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

3.5.1.3. Association Control

Max number of clients (1~64):	<input type="text" value="64"/>
Block clients if traffic load exceeds:	<input type="button" value="Disabled"/>

Fig. 47. Association control settings.

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

3.5.1.4. AP Load Balancing

Functionality:	<input type="button" value="Enabled"/>
Group ID:	<input type="text" value="APLB_Group"/>
Policy by:	<input type="button" value="Number of Users"/>

Fig. 48. AP load balancing settings.

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

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

3.5.1.5. Wireless Distribution System

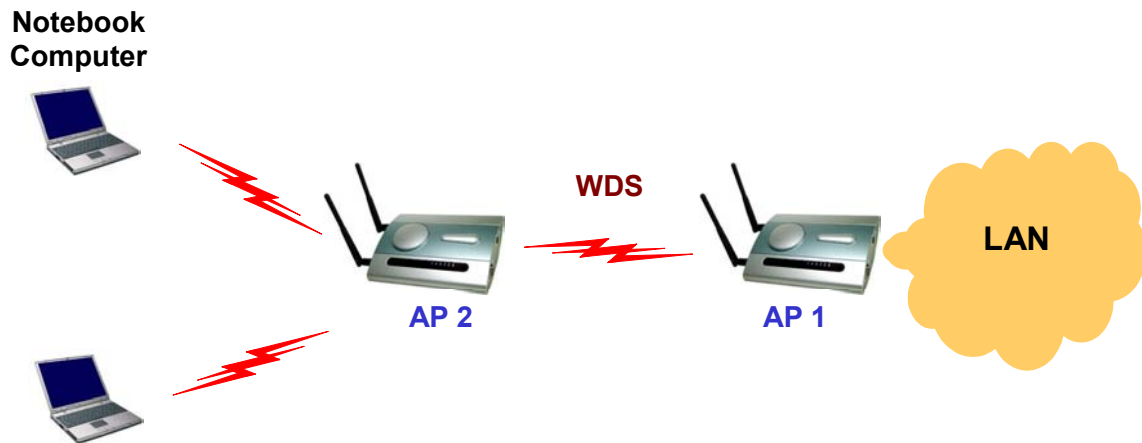


Fig. 49. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 49, 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”.

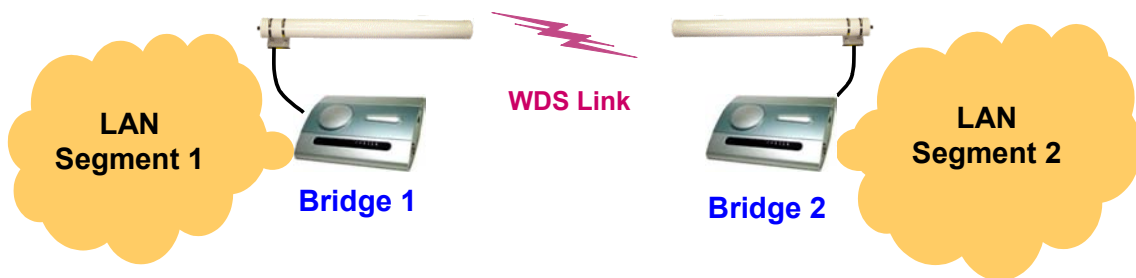


Fig. 50. LAN-to-LAN bridging.

By WDS, two or more LAN segments can be connected wirelessly. As illustrated in Fig. 50, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the WIASA is WDS-enabled, it can be used as a wireless bridge.

NOTE: A WIASA can have up to 6 WDS links to other WIASAs, 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. 51. Wireless Distribution System settings.

To enable a WDS link:

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

For example, assume you want a WIASA and an AP with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6, respectively, to establish a WDS link between them. On WIASA 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 a bridge is connected to other peer bridges by WDS. See the following figure for an example network-planning diagram.

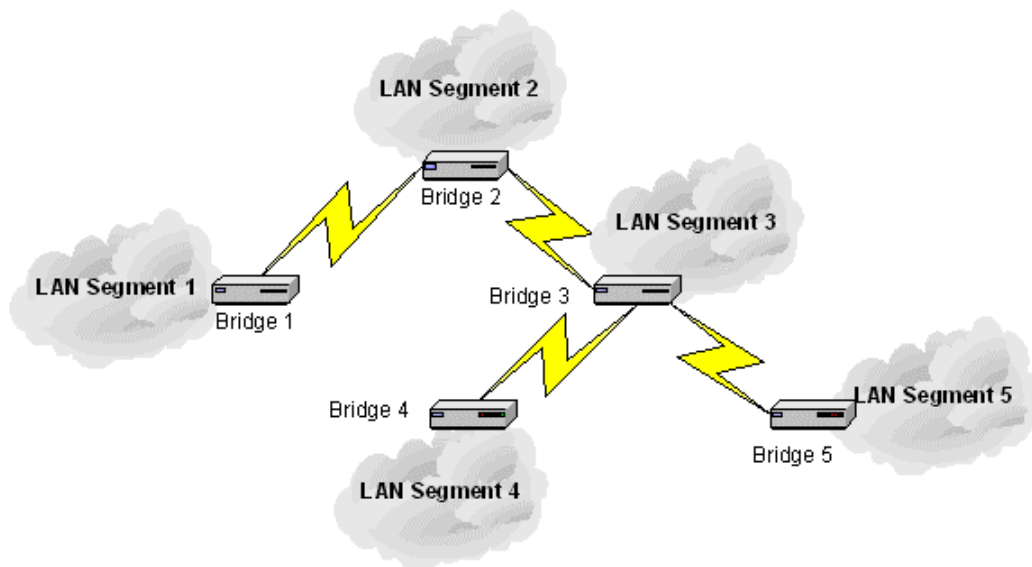
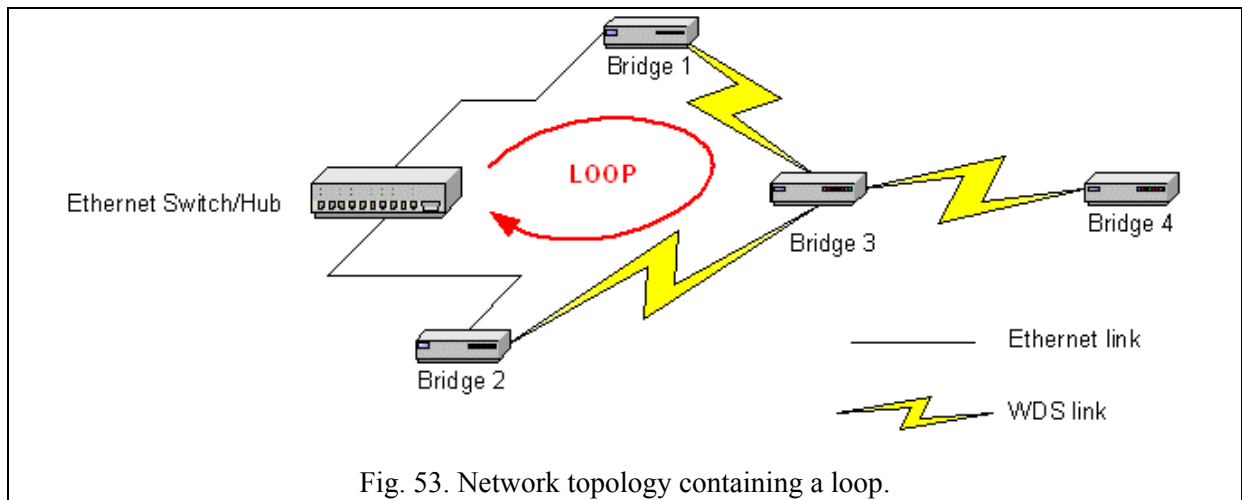


Fig. 52. Sample wireless bridge network topology.

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:

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

Fig. 54 illustrates the idea.

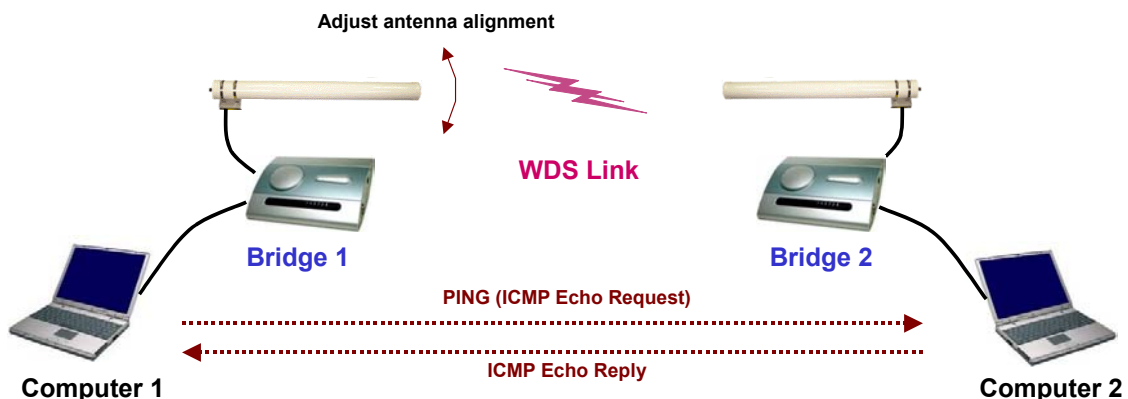


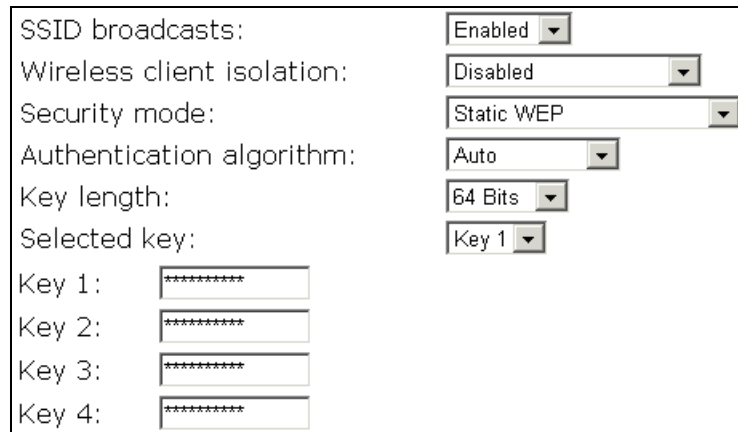
Fig. 54. Adjusting alignments of external directional antennas.

NOTE: There are two antenna connectors on one side of the bridge. Connect your high-gain antenna to the connector labeled "Primary".

3.5.2. Security

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

3.5.2.1. Basic



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

Fig. 55. Basic IEEE 802.11b 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 WIASA.

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

There are up to 5 security modes depending on WIASA model variations:

- **Open System.** No authentication, no data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.
- **IEEE 802.1x EAP without Encryption.** 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.** 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.** 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.

See Section 3.5.3 for more information about IEEE 802.1x.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption.

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

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the 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”.

3.5.2.2. MAC-Address-Based Access Control

Functionality:

Access control type: inclusive exclusive

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

MAC Address	Delete
00-50-C2-01-96-4D	<input type="button" value="Delete"/>
00-09-92-01-02-55	<input type="button" value="Delete"/>

Fig. 56. 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 WIASA. When the table type is set to *inclusive*, entries in the table are permitted to associate with the WIASA. When the table type is set to *exclusive*, entries in the table are not permitted to associate with the WIASA.

To deny wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *exclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

To grant wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *inclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

To delete an entry in the access control table:

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

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

TFTP server IP address:	<input type="text" value="192.168.0.125"/>
MAC ACL file name:	<input type="text" value="MacAcl.txt"/>
<input type="button" value="Download"/>	

Fig. 57. MAC ACL download settings.

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then command the WI-ASA to download the MAC ACL (Access Control List) file from the TFTP server. Fig. 58 shows the contents of a sample ACL file.

```
00-11-22-33-44-50
00-11-22-33-44-51
00-11-22-33-44-52
00-11-22-33-44-53
00-11-22-33-44-54
00-11-22-33-44-55
00-11-22-33-44-56
00-11-22-33-44-57
00-11-22-33-44-58
00-11-22-33-44-59
00-11-22-33-44-5a
00-11-22-33-44-5b
00-11-22-33-44-5c
00-11-22-33-44-5d
00-11-22-33-44-5e
00-11-22-33-44-5f
00-11-22-33-44-60
```

Fig. 58. Sample MAC ACL file.

To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.
2. Specify the name of the MAC ACL file on the TFTP server in the **MAC ACL file name** text box.
3. Click **Download**.

3.5.3. IEEE 802.1x/RADIUS

IEEE 802.1x *Port-Based Network Access Control* is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before granted access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her *user name* and *password* or *digital certificate* to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the WIASA is controlled by the *security mode* (see Section 3.5.1.1).

So far, the WIASA 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 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 WIASA. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

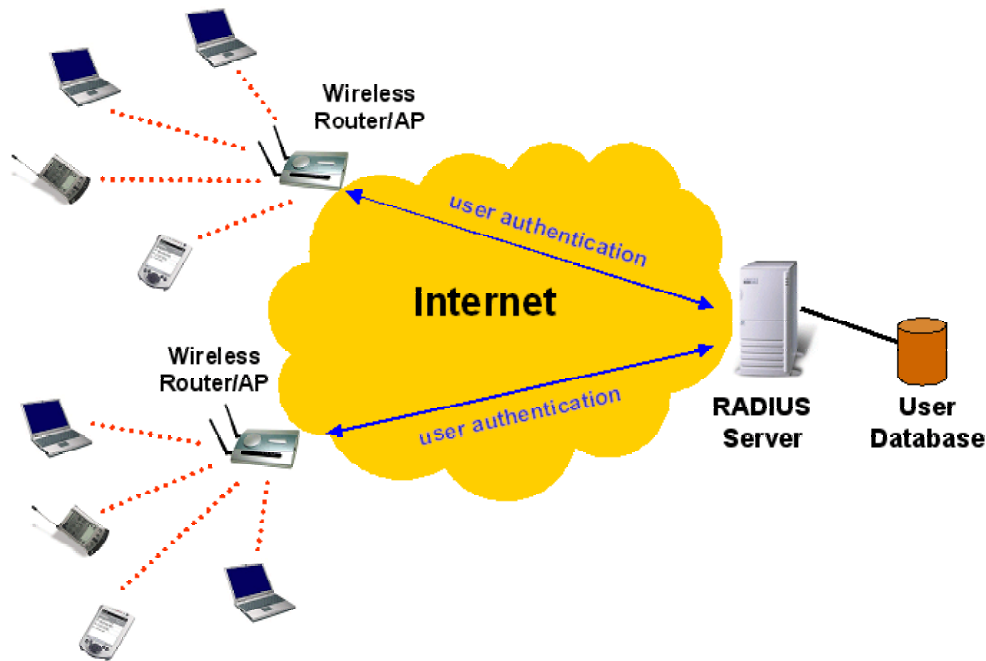


Fig. 59. IEEE 802.1x and RADIUS.

A WIASA supporting IEEE 802.1x can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the WIASA 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 WIASA and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, a WIASA can identify itself by an NAS (Network Access Server) identifier. Each IEEE 802.1x-capable WIASA must have a *unique* NAS identifier.

Primary RADIUS server:	<input type="text" value="192.168.168.220"/>
Secondary RADIUS server:	<input type="text"/>
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Timeout (sec.):	<input type="text" value="5"/>
Max number of retries:	<input type="text" value="3"/>
Shared key:	<input type="text" value="*****"/>
Identifier of this NAS:	<input type="text" value="AP1"/>

Fig. 60. IEEE 802.1x/RADIUS settings.

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

3.6. Configuring Advanced Settings

3.6.1. Filters and Firewall

3.6.1.1. Packet Filters

Functionality:		Disabled ▾					
Policy for unmatched packets:		Pass ▾					
Rules:							
	Action	Protocol	Source IP Address	Subnet Mask	Destination IP Address	Subnet Mask	Destination Port
<input checked="" type="checkbox"/>	Block ▾	ALL ▾	192.168.0.1	255.255.255.0	140.113.23.1	255.255.255.255	100-200,80,25,1
<input type="checkbox"/>	Block ▾	ALL ▾					
<input type="checkbox"/>	Block ▾	ALL ▾					
<input type="checkbox"/>	Block ▾	ALL ▾					
<input type="checkbox"/>	Block ▾	ALL ▾					

Fig. 61. Packet filters settings.

You can specify rules for the firewall component of WIASA to check outgoing packets. Packets that meet the rules can be permitted or denied. The *protocol* field, *source IP address* field, *destination IP address* field, and *destination port* field of a packet's IP header are inspected to see if it meets a rule. A packet that *meets* a rule can be dropped (*Block*) or accepted (*Accept*) as specified in the **Action** setting of the rule. Packets that *do not meet* any rules can be dropped (*Discard*) or accepted (*Pass*) as specified in the **Policy** setting.

A rule is composed of 5 parts:

- What to do if a packet meets this rule (**Action**)
- Protocol type
 - ◆ All
 - ◆ ICMP
 - ◆ TCP
 - ◆ UDP
- Source IP address range (**Source IP Address AND Source Subnet Mask**)
- Destination IP address range (**Destination IP Address AND Destination Subnet Mask**)
- Port ranges

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.

Up to 5 port ranges can be specified in a rule, and these ranges must be separated by commas. For example, “21,80,85-89,140,200-230” in the destination port field signifies 5 port ranges.

To set a rule for packet filtering:

1. Specify the **protocol** type, **source IP address**, **source IP mask**, **destination IP address**, **destination IP mask**, and **destination port** for the rule. Then specify in the **Action** setting how to deal with a packet that meets the rule.
2. Select the corresponding **Enabled** check box.

NOTE: Set the rules with great care since incorrect rules would make the WIASA inaccessible. The last resort to restore the WIASA to service may be resetting its configuration to factory-default values by pressing the **Default** (or **SF-Reset**) switch on the housing of the WIASA. However, Wireless Network Manager can always be used to configure the WIASA even if the filtering rules are incorrect.

3.6.1.2. Firewall

<input type="checkbox"/> Enable SPI (Stateful Packet Inspection)
<input type="checkbox"/> Block ICMP PING from Internet

Fig. 62. Packet filters and firewall settings.

SPI analyzes incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile. To enable SPI, select the **Enable SPI (Stateful Packet Inspection)** check box.

Some DoS (Denial of Service) attacks are based on sending invalid ICMP request packets to hosts. The WIASA can be set to not accept any ICMP requests on the Ethernet WAN interface to defense against attacks of this kind. Enable this capability by selecting the **Block ICMP PING from Internet** check box.

NOTE: Because some of the WIASA’s CPU resources are spent in checking packets for these security features, you may feel networking performance degradation if the security functions are enabled.

3.6.1.3. URL Filters

Functionality:		Disabled ▾	
Enabled	URL	Enabled	URL
<input type="checkbox"/>	www.nba.com	<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. 63. URL filters settings.

The WIASA is capable of blocking HTTP traffic from the intranet to specified unwelcome Web sites.

To block HTTP traffic to an unwelcome Web site:

1. Specify the URL (ex. www.xxx.com) of the unwelcome Web site.
2. Select the corresponding **Enabled** check box.

NOTE: Do not type “http://” when specifying a URL. Just type the domain name.

3.6.2. Management

3.6.2.1. Remote Web-Based Management

Enable remote Web-based management (HTTP port: 8080)

Fig. 64. Remote Web-based management setting.

The WIASA can also be managed from the Internet using a Web browser. To enable this capability, select the **Enable remote Web-based management** check box. To manage the WIASA from the Internet, connect to the WIASA within a Web browser, but be sure to specify the port **8080**. For example, if the WAN interface of a WIASA is configured to be 61.16.33.113, the URL for managing this WIASA is “http://61.16.33.113:8080”.

3.6.2.2. UPnP

Functionality:
 Device friendly name:

Fig. 65. 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 WIASA in My Network Places of Windows XP. The WIASA can be given a *friend name* that will be shown in My Network Places. *Double-clicking* the icon in Network Neighborhood that stands for the WIASA will launch the default Web browser for you to configure the WIASA.

3.6.2.3. System Log

Local log
 Remote log by SNMP trap
Event Types
 General
 Build-in AP
 MIB II traps
 RADIUS user authentication

Fig. 66. System log settings.

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

3.6.2.4. 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. 67. SNMP settings.

The WIASA can be managed by SNMP (Simple Network Management Protocol), and the SNMP management functionality can be disabled. 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** (or **SF-Reset**) switch on the housing of a *powered-on* WIASA to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
Operational Mode	Router with a Static-IP DSL/Cable Connection
IEEE 802.11b	
Regulatory Domain	FCC (U.S.)
Channel Number	11
SSID	wireless
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	High
MAC Address	See the label on the accompanying PCMCIA card or the label on the housing of the WIASA.
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
WAN Interface	
Type	Static-IP DSL/Cable
Changeable MAC Address	IEEE 802.11b MAC address
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	router
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
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	
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 Allocateable IP Address	192.168.0.2
Allocateable IP Address Count	20
NAT Server	
Functionality	Enabled
Virtual Server Mappings	Disabled
DMZ Host	Not set
Static NAT Mappings	Not set
DNS Proxy	
Static DNS Mappings	Not set
Filters/Firewall	
Packet Filters	Not set
URL Filters	Not set
WAN ICMP Request Blocking	Disabled
State Packet Inspection (SPI)	Disabled
Management	
Remote Web-Based Management	Disabled
UPnP	Enabled
System Log	Local Log
SNMP	Enabled
SNMP read community	public
SNMP write community	private
Telnet	Enabled

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the WIASA is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the WIASA.
- Make sure that the LED ALV of the WIASA is blinking to indicate the WIASA is working.
- Make sure the types of the Ethernet cables are correct. Recall that there are two types—*normal* and *crossover*.
- Make sure that the DSL, cable, V.90, or ISDN modem connected with the WIASA is powered on.

B-1: Wireless Settings Problems

- **The wireless client computer cannot associate with 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 setting of the WLAN NIC and of the WIASA.
 - Is the WEP functionality of the prospective access point or WIASA enabled?
 - ◆ Make appropriate WEP settings of the client computer 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.

B-2: TCP/IP Settings Problems

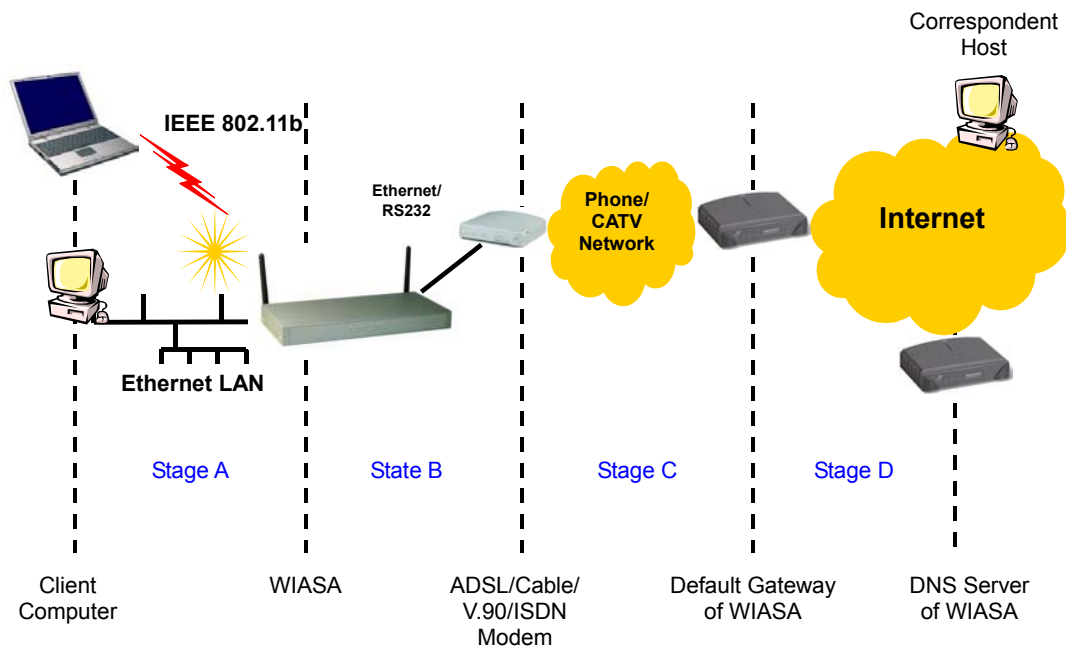


Fig. 68. Communication stages for a client to reach its correspondent host.

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. 68, 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 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-provided **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 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 and the IP address of the WIASA are in the same IP subnet.

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

- **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. Refer 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 server(s) 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.
- **Cannot access the Internet.**
 - Solve the preceding problems first.
 - Make sure there are no incorrect packet filter settings that would block the traffic from the local computer to the Internet. In case you are not sure, the last resort may be resetting the configuration settings of the WIASA to default values by press the **Default** or **SF-Reset** switch.

B-3: Unknown Problems

- **The router has been set to be in Simple Access Point mode and 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 WIASAs and show their MAC addresses and IP addresses. In addition, it can launch the default Web browser on your computer.

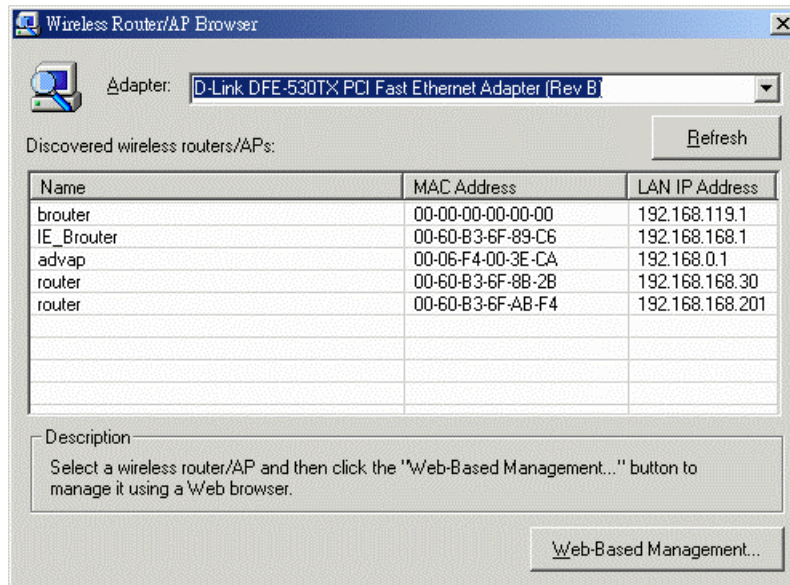


Fig. 69. Wireless Router/AP Browser.

- **The WIASA stops working and does not respond to Web management requests.**
 - The firmware of the WIASA may be stuck in an incorrect state.
 - ◆ Press the **Reset** button on the housing of the WIASA or unplug the power connector from the power jack, and then re-plug the connector to restart the WIASA.
 - ◆ Contact our technical support representatives to report this problem, so that the bugs can be static in future firmware versions.
 - If the WIASA still does not work after restarting, there may be hardware component failures in the WIASA.
 - ◆ Contact our technical support representatives for repair.

Appendix C: Additional Information

C-1: Firmware Upgrade Using Xmodem Upgrade

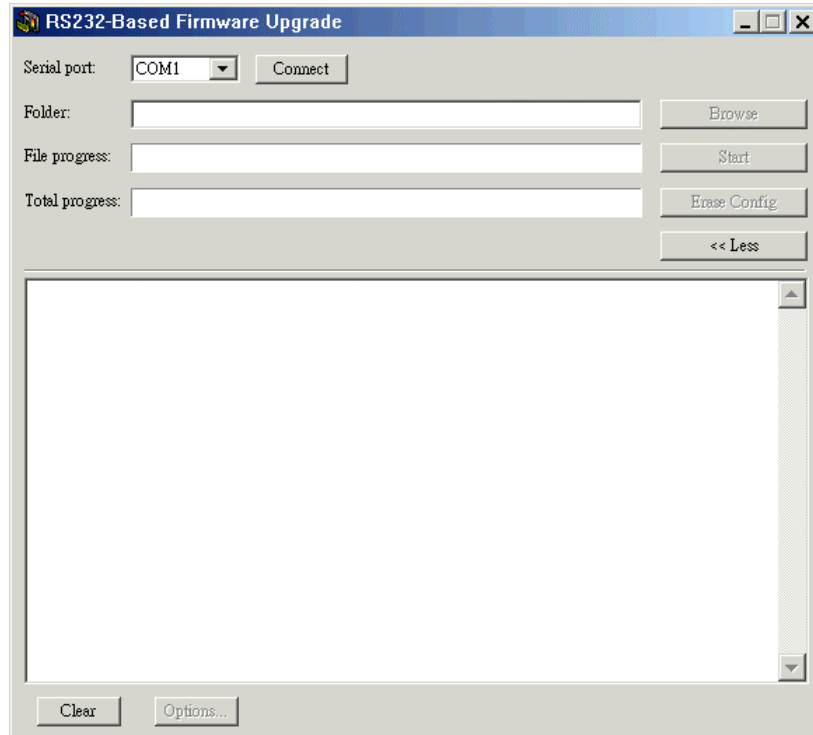


Fig. 70. Xmodem Upgrade.

To upgrade the firmware of WIASA using Xmodem Upgrade over RS232:

1. Power off the WIASA whose firmware will be upgraded.
2. Connect the managing PC and the DRBAP with an *RS232 Null Modem* cable.
3. Select the serial port (COM1 or COM2) you use for connecting the device from the **Serial port** drop-down list and click **Connect**.
4. Chose the folder in which the firmware files reside by click **Browse**.
5. Power on the WIASA and you'll see bootup information.
6. Click **Start** to begin upgrade the firmware of the WIASA.
7. You will be prompted when the upgrade process completes.

Click **Erase Config** to reset the configuration settings of the WIASA to default values.

C-2: Distances and Data Rates

Important Notice: Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those we post below.

IEEE 802.11b Maximum Distance Table				
Environmental Condition	Speed and Distance Ranges			
	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Open Environment: A "line-of-sight" environment with no interference or obstructions between Access Point and Users.	160 m (524 ft)	270 m (886 ft)	400 m (1312 ft)	457 m (1500 ft)
Semi-Open Environment: An environment with no major obstructions such as walls or privacy cubicles between Access Point and users.	50 m (164 ft)	70 m (230 ft)	90 m (295 ft)	120 m (394 ft)
Closed Environment: A typical office or home environment with floor to ceiling obstructions between Access Point and users.	25 m (82 ft)	35 m (115 ft)	45 m (148 ft)	55 m (180 ft)