Wireless ADSL Router
WA1003A-RU
User Manual

FCC Notices

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

CAUTION: Change or modification not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

NOTE: 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 provid e 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 or more of the following measures:

-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment in to 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.

Table of Contents

Chapter 1 Basic Information of Product

1.1 Packing List

Open the shipping carton and carefully remove all items. Make sure that you have the items listed here.

- One WA1003A-RU
- One screw-on antenna
- One CD-ROM containing the User's Guide and USB driver
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- One USB cable for USB connection
- One AC power adapter suitable for your electric service
- One User manual
- One Quick Installation Guide

1.2 Appearance of WA1003A-RU

1.2.1 Front Panel Display

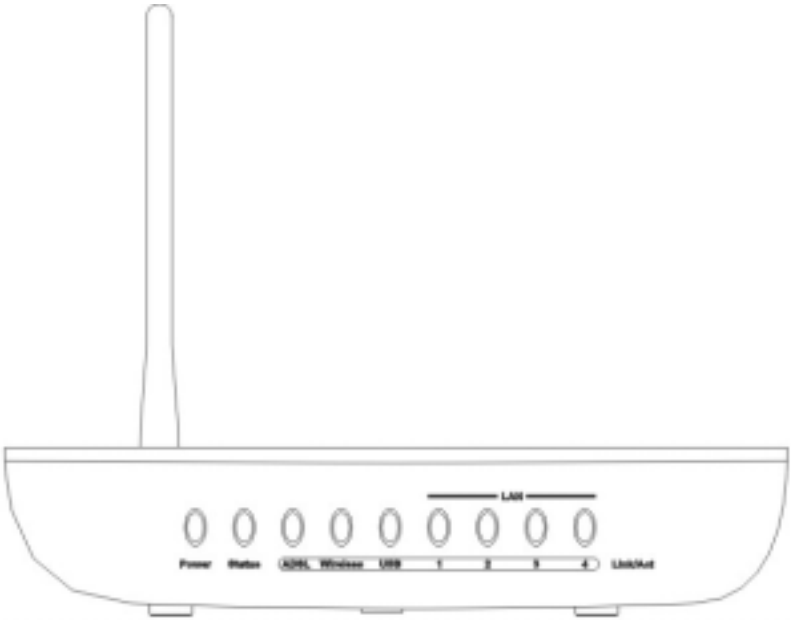

Figure 1-1 Front Panel

Place the WA1003A-RU in a location that permits an easy view of the LED indicators on the front panel.

The LED indicators on the front panel include the **Power**, **Status**, **ADSL Link/Act** and **LAN (1-4) Link/Act** indicators. The ADSL and Ethernet indicators monitor link status and activity (Link/Act).

Table 1-1 LED indicators of WA1003A-RU

LED indicators	Description
Power	Steady green light indicates the unit is powered on. When the device is powered off this remains dark.
Status	Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator lights steady green after the POST, the system has failed and the device should be rebooted.
ADSL: Link/Act	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates activity on the WAN (ADSL) interface.
WLAN 1 – 4: Link/Act	A solid green light indicates a valid link on startup. These lights blink when there is activity currently passing through the Ethernet port.
USB: Link/Act	Steady green light indicates a valid USB connection. A blinking green light indicates activity on the USB interface.

1.2.2 Rear Panel Connections

All cable connections to the WA1003A-RU are made at the rear panel. Connect the power adapter here to power on the WA1003A-RU. Use the Reset button to restore the settings to the factory default values in the next chapter for instructions on using the reset button).

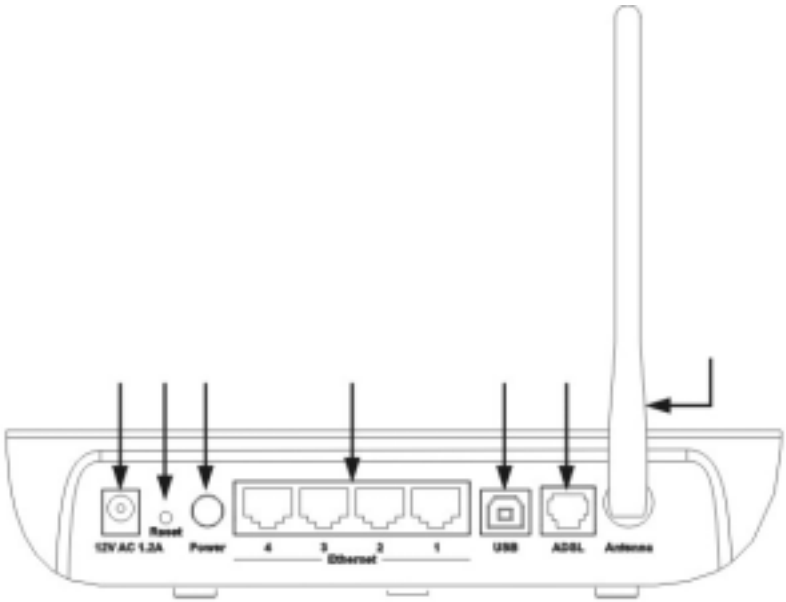

Figure 1-2 Rear panel

1.3 Features and Standards Compatibility and Compliance of Product

The WA1003A-RU is designed to provide a simple, cost-effective and secure ADSL Internet connection for wired (Ethernet) and wireless (802.11b) stations on your network. The WA1003A-RU combines high-speed ADSL connection technology, TCP/IP routing and 802.11b wireless connectivity in one compact unit.

The WA1003A-RU is easy to install and use. The WA1003A-RU connects to an Ethernet LAN via a standard Ethernet 10BASE-T

interface using RJ-45 connectors. The ADSL connection is made using ordinary twisted-pair telephone line with standard RJ-11 connectors. This arrangement allows wired and wireless workstations to share network resources and connect to the Internet using a single WAN interface and IP address.

The WA1003A-RU supports transparent bridging or it can be used for IP packet routing over the Internet. Cost saving features of the WA1003A-RU such as NAT (Network Address Translator) and DHCP (Dynamic Host Configuration Protocol) improve efficiency and security. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents outside your network.

All the 802.11b wireless settings for the WA1003A-RU are entered on a single page in the web manager. Security for the wireless interface comes in two forms, WEP Encryption and MAC Address Control.

1.3.1 Features of Product

The WA1003A-RU utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. WA1003A-RU advantages include:

- **PPP (Point-to-Point Protocol) Security –** The WA1003A-RU supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.
- **DHCP Support –** Dynamic Host Configuration Protocol automatically and dynamically assigns al LAN IP settings to each

host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.

- **Network Address Translation (NAT) –**For small office environments, the WA1003A-RU allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user.

  NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.

- **TCP/IP (Transfer Control Protocol/Internet Protocol) –** The WA1003A-RU supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.

- **RIP-1/RIP-2 –** The WA1003A-RU supports both RIP-1 and RIP-2 exchanges with other routers. Using both versions lets the WA1003A-RU to communicate with all RIP enabled devices.

- **Static Routing –** This allows you to select a data path to a particular network destination that will remain in the routing table and never “age out”. If you wish to define a specific route that will always be used for data traffic from your LAN to a specific destination within your LAN (for example to another router or a server) or outside your network (to a ISP defined default gateway for instance).

- **Default Routing –** This allows you to choose a default path for incoming data packets for which the destination address is

unknown. This is particularly useful when if the WA1003A-RU functions as the sole connection to the Internet.

- **ATM (Asynchronous Transfer Mode) –** The WA1003A-RU supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577) and PPP over ATM (RFC 2364).
- **Precise ATM Traffic Shaping –** Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.
- **G.hs (Auto-handshake) –** This allows the WA1003A-RU to automatically choose either the G.lite or G.dmt ADSL connection standards.
- **High Performance –** Very high rates of data transfer are possible with the WA1003A-RU. Up to eight Mbps downstream bit rate using the G.dmt.
- **Full Network Management –** The WA1003A-RU incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or Telnet connection.
- **Telnet Connection –** The Telnet enables a network manager to access the WA1003A-RU's management software remotely.
- **Easy Installation –** The WA1003A-RU uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the WA1003A-RU.

1.3.2 Standards Compatibility and Compliance

The WA1003A-RU complies with or is compatible with the following standards as recognized by their respective agencies.

- ITU G.992.2 (G.lite “Splitterless ADSL”) compliant
- ITU-T Rec. I.361 compliant
- RFC 791 Internet Protocol compliant
- RFC 792 UDP compliant
- RFC 826 Address Resolution Protocol compliant (ARP) compliant
- RFC 1058 Routing Information Protocol (RIP) compliant
- RFC 1213 MIB II for IP compliant
- RFC 1334 PPP Authentication Protocol compliant
- RFC 1389 Routing Information Protocol 2 (RIP2) compliant
- RFC 1483 IP over AAL5/ Bridged Ethernet over AAL5 compliant
- RFC 1557 Classical IP over ATM (IPoA) compliant
- RFC 1661 Point to Point Protocol (PPP) compliant
- RFC 1877 Automatic IP assignment compliant
- RFC 1994 Challenge Handshake Authentication Protocol compliant
- Supports RFC 2131 and RFC 2132 DHCP functions including: automatic assignment of IP address, use of subnet mask and default gateway and provision of DNS server address for all hosts
- RFC 2364 PPP over ATM compliant (PPPoA) compliant
- RFC 2516 PPP over Ethernet compliant (PPPoE) compliant

- RFC 2684 Bridged/Routed Ethernet over ATM compliant
- IEEE 802.3 compliant
- IEEE 802.3u compliant
- IEEE 802.1d compliant
- IEEE 802.3x compliant
- Embedded web server support
- Supports Dynamic Learning
- Supports Static Routing
- Supports NAPT for up to 4096 connections
- Supports DHCP for up to 253 hot connections
- Supports IGMP
- Supports DVMRP
- Supports ATM Forum UNI 3.1/4.0
- Supports ATM VCC (Virtual Channel Circuit) for up to eight sessions
- Supports TELNET and TFTP
- Supports back pressure for half-duplex

Chapter 2 Installation

2.1 Before You Start

Please read and make sure you understand all the prerequisites for proper installation of your new WA1003A-RU. Have all the necessary information and equipment on hand before beginning the installation.

2.1.1 Installation Overview

The procedure to install the WA1003A-RU can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.
2. Install the hardware, that is, connect the cables (Ethernet and telephone) to the device and connect the power adapter.
3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built into the WA1003A-RU.
4. Use the web-based management software to configure the device to suit the requirements of your ADSL account.

2.1.2 Installation Requirements

In order to establish a connection to the Internet it will be necessary to provide information to the WA1003A-RU that will be

stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the WA1003A-RU. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

Low Pass Filters

Since ADSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the ADSL line. These filters are easy to install passive devices that connect to the ADSL device and/or telephone using standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems

The WA1003A-RU uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, and Windows XP.

Web Browser

Any common web browser can be used to configure the WA1003A-RU using the web configuration management software.

The program is designed to work best with more recently released browsers such as Opera, Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)

Any computer that uses the WA1003A-RU must be able to connect to it through the Ethernet port on the WA1003A-RU. This connection is an Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet NIC adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the WA1003A-RU. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

802.11b Wireless LAN Configuration

All the 802.11b wireless LAN settings may be configured on a single page using the web-based manager. For basic wireless communication you need to decide what channel to use and what SSID to assign. These two settings must be the same for any wireless workstations or other wireless access point that communicate with the WA1003A-RU through the wireless interface.

Security for wireless communication can be accomplished in a number of ways. The WA1003A-RU supports WEP encryption, 802.1X authentication, and WPA (Wi-Fi Protected Access). Wireless access can also be controlled by selecting MAC addresses that are allowed to associate with the device. Please read the section on Wireless Configuration.

Additional Software

It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using the device a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the WA1003A-RU itself.

If your ADSL service is delivered through a PPPoE, PPPoA or CLIP (IPoA) connection, the information needed to establish and maintain the Internet connection can be stored in the WA1003A-RU. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a PC, a server, a gateway device such as a router or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

About CLIP Connections (RFC 1577)

Classical IP over ATM (CLIP) connections may require global IP settings for the device. Your service provider will give you IP settings information if needed. Some CLIP connections function like peer-to-peer connections and therefore do not require IP settings on the WAN interface.

Table 2-1 Information you will need from your ADSL service provider

Username	This is the Username used to log on to your ADSL service provider's network. It is commonly in the form – user@isp.com. Your ADSL service provider uses this to identify your account.
Password	This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.
Connection Protocol	This is the method your ADSL service provider uses to send and receive data between the Internet and your computer. Your Modem supports the following connection protocols: PPPoE, PPPoA, PPPoA with DHCP, Bridge, and CLIP (IPoA).
Modulation Type	ADSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (MMODE) used for the WA1003A-RU automatically detects all types of ADSL modulation. However, if you are instructed to specify the modulation type used for the WA1003A-RU, you have three alternatives: G.LITE, G.DMT and T1.413
Security Protocol	This is the method your ADSL service provider will use to verify your Username and Password when you log on to their network. Your Modem supports the PAP and CHAP protocols.
VPI	This is the Virtual Path Identifier (VPI). It is used in conjunction with the Virtual Channel Identifier (VCI) below, to identify the data path between your ADSL service provider's network and your computer.
VCI	This is the Virtual Channel Identifier (VCI). It is used in conjunction with the VPI above to identify the data path between your ADSL service provider's network and your computer.

IP Address (RADIUS server)	For 802.1X and WPA security.
Port	For 802.1X and WPA security.
Secret	For 802.1X and WPA security.

Table 2-2 Information you will need about your WA1003A-RU

Username	This is the Username needed access the Modem's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Modem is admin. This may be changed by the user.
Password	This is the Password you will be prompted to enter when you access the Modem's management interface. The default Password is admin. This may be changed by the user.
LAN IP addresses for the WA1003A-RU	This is the IP address you will enter into the Address field of your web browser to access the Modem's configuration graphical user interface (GUI) using a web browser. The default IP address is 192.168.1.1 and it is referred to as the "Management IP" address in this User's Manual. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.
LAN Subnet Mask for the WA1003A-RU	This is the subnet mask used by the WA1003A-RU, and will be used throughout your LAN. The default subnet mask is 255.0.0.0. This can be changed later.

Table 2-3 Information you will need about your LAN or computer

Ethernet NIC	If your computer has an Ethernet NIC, you can connect the WA1003A-RU to this Ethernet port using an Ethernet cable. You can also use the Ethernet port on the WA1003A-RU to connect to other Ethernet devices, such as a Wireless Access Point.
USB port	If your computer has an available USB port, you can connect the WA1003A-RU to this USB port using a USB cable
DHCP Client status	Your DSL-302T ADSL Modem is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-302T will assign are from **192.168.1.2** to **192.168.1.254**. Your computer (or computers) needs to be configured to **Obtain an IP address automatically** (that is, they need to be configured as DHCP clients.)

It is recommended that your collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your WA1003A-RU.

2.2 Choosing Installation Location

The WA1003A-RU functions on three separate networks: a wired Ethernet LAN, a wireless LAN and a wired ADSL WAN. Placement of the WA1003A-RU must take into account the fact that it is connected to these three networks with three types of media. Ethernet cables connect the WA1003A-RU to computers and network devices and the

ADSL line connects it to a wall socket. In addition, the device must be near an AC wall outlet for power. How to accommodate these wired connections is often not a complicated matter. However, the added dimension of wireless communication does complicate the decision of WA1003A-RU placement.

Many environmental factors can affect the effective wireless function of the WA1003A-RU. If this is your first time setting up a wireless network device, read and consider the points listed below.

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Designed to go up to 100 meters indoors and up to 300 meters outdoors, Wireless LAN lets you access your network from anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. To range and signal strength, use these basic guidelines:

1. **Keep the number of walls and ceilings to a minimum:** The signal emitted from Wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range of Wireless LAN devices from 1 to 30M. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.
2. **Consider the direct line between access points and workstations:** A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position access points

and client adapters so the signal can travel straight through (90º angle) a wall or ceiling for better reception.

3. **Building Materials make a difference:** Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.
4. **Position the antennas for best reception.** Play around with the antenna position to see if signal strength improves. Some adapters or access points allow the user to judge the strength of the signal.
5. **Keep your product away (at least 1-2 meters) from electrical devices:**
   Position wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

2.3 Installing USB Driver

You should install the USB driver into your PC before using USB connection. To install the USB driver, you must execute “WA1003A-RUDriver.exe” contained on the CD-ROM, which is provided with the modem. During the installation, it doesn’t need any interference from your side.

If you are using Windows XP/2000, a new “Local Area Connection” will then be built for USB port.

2.4 Network Connections

Network connections are provided through the ADSL port and the four Ethernet ports on the back of the WA1003A-RU. See the Rear Panel diagram above and the illustrations below for examples.

2.4.1 Connect ADSL Line

Use the ADSL cable included with the WA1003A-RU to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the WA1003A-RU and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

2.4.2 Connect WA1003A-RU to Ethernet

The WA1003A-RU may be connected to a single computer or Ethernet device through the 10BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the WA1003A-RU to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port.

Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the WA1003A-RU is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the WA1003A-RU directly

to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the WA1003A-RU to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch.

The rules governing Ethernet cable lengths apply to the LAN to WA1003A-RU connection. Be sure that the cable connecting the LAN to the WA1003A-RU does not exceed 100 meters.

2.4.3 Hub or Switch to WA1003A-RU Connection

Connect the WA1003A-RU to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable.

If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

2.4.4 Computer to WA1003A-RU Connection

You can connect the WA1003A-RU directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable.

2.5 Power on WA1003A-RU

Caution:

The WA1003A-RU must be used with the power adapter included with the device.

To power on the WA1003A-RU:

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the WA1003A-RU and plug the adapter into a suitable nearby power source.
2. You should see the Power LED indicator light up and remain lit. The Status LED should light solid green and begin to blink after a few seconds.
3. If the Ethernet port is connected to a working device, check the Ethernet Link/Act LED indicators to make sure the connection is valid. The WA1003A-RU will attempt to establish the ADSL connection, if the ADSL line is connected and the WA1003A-RU is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the WA1003A-RU can establish a connection.

2.6 Factory Reset Button

The WA1003A-RU may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP

settings. The factory default IP address of the WA1003A-RU is 192.168.1.1 and the subnet mask is 255.255.255.0, the default management Username is **admin** and the default Password is **admin**.

Chapter 3 Configuring

The first time you setup the WA1003A-RU it is recommended that you configure the WAN connection using a single computer making sure that both the computer and the WA1003A-RU are not connected to the LAN. Once the WAN connection is functioning properly, you may continue to make changes to WA1003A-RU configuration including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection and describes the various menus used to configure and monitor the WA1003A-RU including how to change IP settings and DHCP server setup.

3.1 WAN Configuration Summary

1. **Connect to the WA1003A-RU** To configure the WAN connection used by the WA1003A-RU it is first necessary to communicate with the WA1003A-RU through its management interface, which is HTML-based and can be accessed using a web browser. To access the management software your computer must be able to “see” the WA1003A-RU. Your computer can see the WA1003A-RU if it is in the same “neighborhood” or subnet as the WA1003A-RU. This is accomplished by making sure your computer has IP settings that place it in the same subnet as the WA1003A-RU. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the WA1003A-RU. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client.

2. **Configure the WAN Connection** Once your are able to access the configuration software you can proceed to change the settings required to establish the ADSL connection and connect to the service provider's network. There are different methods used to establish the connection to the service provider's network and ultimately to the Internet. You should know what Encapsulation and connection type you are required to use for your ADSL service. It is also possible that you must change the PVC settings used for the ADSL connection. Your service provider should provide all the information you need to configure the WAN connection.

3.2 Configuring IP Settings on Your Computer

In order to configure your system to receive IP settings from the WA1003A-RU it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. Below is an illustrated example of how to configure a Windows XP system to automatically obtain IP settings from the WA1003A-RU. Following this example is a step-by-step description of the procedures used on the other Windows operating systems to first check if the TCP/IP protocol has been installed; if it is not, instructions are provided for installing it. Once the protocol has been installed you can configure the system to receive IP settings from the WA1003A-RU.

For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP

address from the WA1003A-RU, that is, configure the system to be a DHCP client.

Note:

If you are using this WA1003A-RU to provide Internet access for more than one computer, you can use these instructions later to change the IP settings for the other computers. However, you cannot use the same IP address since every computer must have its own IP address that is unique on the local network.

3.2.1 Configure Windows XP for DHCP

Use the following steps to configure a computer running Windows XP to be a DHCP client.

1. From the **Start** menu on your desktop, go to **Settings**, then click on **Network Connections**.
2. In the **Network Connections** window, right-click on **LAN** (Local Area Connection), then click **Properties**.

Figure 3-1 Windows XP Network Connections

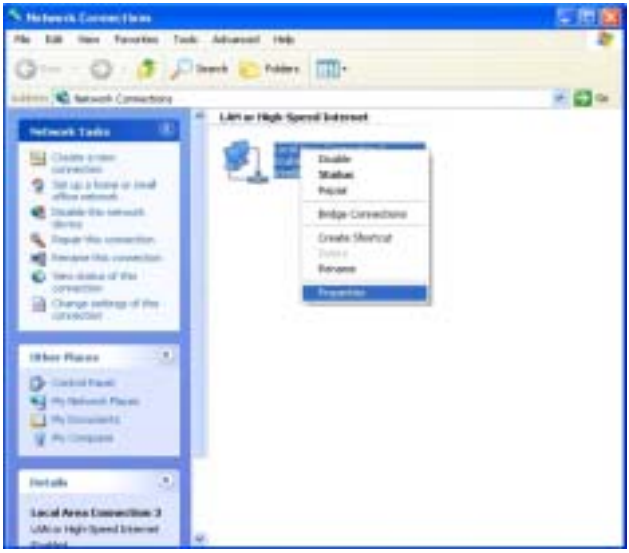

Figure 3-2 Windows LAN Property

3. In the **General** tab of the **Local Area Connection Properties** menu, highlight **Internet Protocol (TCP/IP)** under "This connection uses the following items:" by clicking on it once. Click on the **Properties** button.

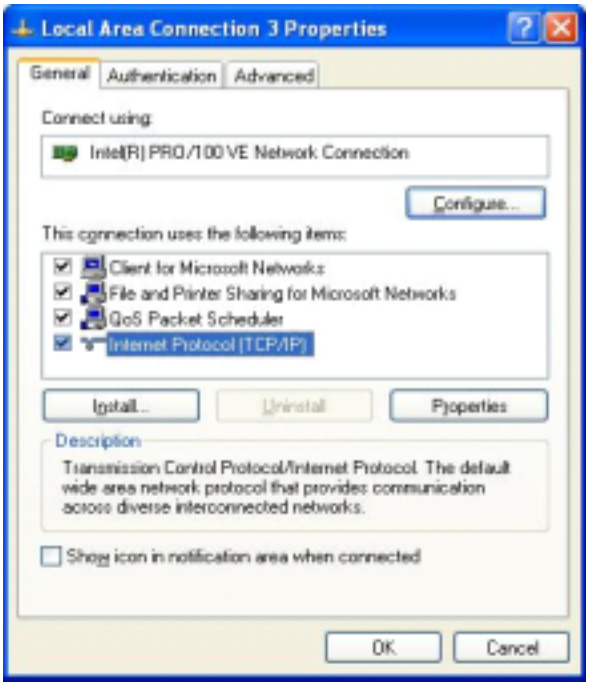

Figure 3-3 Windows XP TCP/IP

4. Select “Obtain an IP address automatically” by clicking once in the circle. Click the **OK** button.

Figure 3-4 Windows XP Client IP Address

Your computer is now ready to use the WA1003A-RU's DHCP server.

3.2.2 Configure Windows 2000 for DHCP

1. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
2. In **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
3. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the button labeled **Obtain an IP address automatically**.

5. Double-click **OK** to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the WA1003A-RU's DHCP server.

3.2.3 Configure Windows ME for DHCP

1. In the **Control Panel**, double-click the **Network and Dial-up Connections** icon.
2. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
3. In the **Network Properties** dialog box, select **TCP/IP**, and then click **Properties**.
4. In the **TCP/IP Settings** dialog box, click the **Obtain and IP address automatically** option.
5. Double-click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the WA1003A-RU's DHCP server.

3.2.4 Configure Windows 95 and Windows 98 for DHCP

1. Open the **Control Panel** window, and then click the **Network** icon.
2. Select the network component labeled TCP/IP, and then click **Properties**.
3. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

4. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
5. Click the **Obtain an IP address automatically** option.
6. Double-click **OK** to confirm and save your changes. You will be prompted to restart Windows.
7. Click **Yes**.

When it has restarted your computer is ready to use the WA1003A-RU's DHCP server.

3.2.5 Configure Windows NT 4.0 for DHCP

1. Open the **Control Panel** window, and then double-click the **Network** icon.
2. In the **Network** dialog box, click the **Protocols** tab.
3. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
4. In the **Microsoft TCP/IP Properties** dialog box, click the **Obtain an IP address automatically** option.
5. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

3.3 Login to Home Page

Now that your computer's IP settings allow it to communicate with the WA1003A-RU, you can access the configuration software.

Note:

Be sure that the web browser on your computer is not configured to use a proxy server in the Internet settings. In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:

1. In Windows, click on the Start button, go to Settings and choose Control Panel.
2. In the Control Panel window, double-click on the Internet Options icon.
3. Click the Connections tab and click on the LAN Settings button.
4. Verify that the "Use proxy server" option is NOT checked. If it is checked, click in the checked box to deselect the option and click OK.

Alternatively, you can access this Internet Options menu using the Tools pull-down menu in Internet Explorer.

To use the web-based management software, launch a suitable web browser and direct it to the IP address of the WA1003A-RU. Type in **http://** followed by the default IP address, **192.168.1.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.1.1**.

A new window will appear and you will be prompted for a user name and password to access the web-based manager.

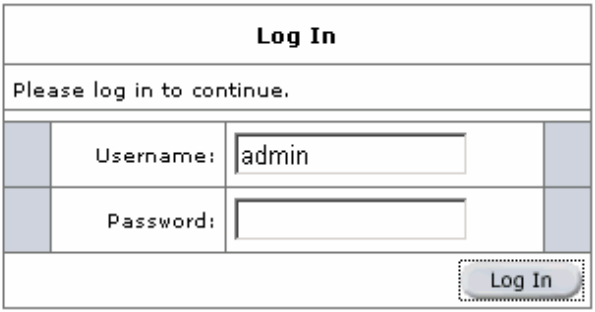

Figure 3-5 Home - Login window

Use the default user name **admin** and password **admin** for first time setup. You should change the web-based manager access user name and password once you have verified that a connection can be established. The user name and password allows any PC within the same subnet as the Modem to access the web-based manger.

Note:

Do not confuse the user name and password used to access the web-based manager with the ADSL account user name and password needed for PPP connections to access the service provider's network.

3.4 Configure the WA1003A-RU

The first page that appears after you successfully login displays information about the WA1003A-RU and its connection status. Tabs

across the top of the screen show other available menus: **Setup**, **Advanced**, **Tools**, **Status**, and **Help**.

Figure 3-6 Home – Status Information window

When the WA1003A-RU is used to provide Internet access it actually must first access your service provider's network, that is, it must communicate with computers and other WA1003A-RUs owned by your service provider. These computers and WA1003A-RUs then provide access to the Internet. The WA1003A-RU must be configured to communicate with the systems that give it access to the larger network. Click either the **Setup** tab (or the **Go to setup wizard** hyperlink); the Setup window will appear.

3.4.2 Setup Menu

The **Setup** window offers links to menus to configure settings for the LAN (Local Area Network) and for the WAN (Wide Area Network)

setup. The first menu you see when clicking the **Setup** tab or the **Go to setup wizard** hyperlink is the Setup menu.

Now you are ready to configure the settings needed for the WAN connection. All the information you need to make the changes needed for a functioning WAN connection should have been provided to you by your ISP or network service provider.

Figure 3-7 Opening Setup window

If you are not instructed to change the modulation type, click the **Wireless** button or hyperlink to configure the wireless settings. Skip ahead to Configure Connection below to configure a PPPoA connection type. Detailed instructions follow on how to configure other connection types.

If you are instructed to change the method of modulation used for ADSL, click the **Modem Setup** button or Modem Setup hyperlink and select the Modulation Type used for the connection. Skip ahead to the next page for an example of the Modem Setup menu. Then proceed to

Configure Connection to configure a PPPoA conection or Change the Connection Type for other connection types.

3.4.3 Wireless Settings

Click the **Enable AP** box to allow the WA1003A-RU to operate in the wireless environment.

SSID: The SSID identifies members of Service Set.

Accept the default name or change it to something else. *If the default SSID is changed, all other devices on the wireless network must use the same SSID.*

Channel: What channels are available for use by the access point depends on the local regulatory environment. Remember that all devices communicating with the device must use the same channel (and use the same SSID). Use the drop down menu to select the channel used for your 802.11b wireless LAN.

The wireless channel number is available from your Internet Service Provider (ISP).

If network Security is not used, click **None**, then click **Apply**.

Note:

For initial configuration of the WA1003A-RU, make sure that None is selected. It is more important first to make sure that your wireless network is functioning properly.

Figure 3-8 Wireless configuration window

For information on applying various types of security to your network, see the next few pages.

3.4.4 Wireless Security

The WA1003A-RU offers three types of network security: **WEP**, **802.1X**, and **WPA**.

WEP

WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys.

The WA1003A-RU offers 64, 128, or 256-bit encryption with four keys available.

To bring up the WEP configuration window, click the **WEP** radio button.

Figure 3-9 WEP configuration window

From the drop-down menu, select an Authentication Type: **Open**, **Shared**, or **Both**.

Select a key by clicking a radio button on the left, select an encryption level from the drop-down menu on the right, then enter the proper-length key. (Key length is outlined at the bottom of the window.)

Click **Apply**.

Note:

If encryption of any kind, at any level is applied to the WA1003A-RU, all devices on the network must comply with all security measures.

802.1X

Some network-security experts now recommend that wireless networks use 802.1X security measures to overcome some weaknesses in standard WEP applications. A RADIUS server is used to authenticate all potential users.

Server IP Address: enter the IP address of the Radius server

Port: enter a port number, or accept the default

Secret: enter a password (1-63 character)

Group Key Interval: time (in seconds) after which the Group Key is changed automatically (1-99999).

Note:

The values needed for the above entries can be obtained from your Internet Service Provider (ISP).

Figure 3-10 802.1X configuration window

Note:

If encryption of any kind, at any level is applied to the WA1003A-RU, all devices on the network must comply with all security measures.

WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP.

For most small networks, such as in a small business or home-based enterprise, WPA is the easiest way to obtain effective network security. Of the three options in WPA, **PSK String** is the easiest to implement.

Figure 3-11 WPA configuration window

Group Key Interval: time (in seconds) after which the Group Key is changed automatically (1-99999).

802.1X

IP address of the RADIUS server, **Port** number, and **Secret** (password) can be obtained from your Internet Service Provider (ISP).

PSK HEX

PSK (Pre-Shared Key) Hex is a hexadecimal value 1-32 characters in length.

PSK String

PSK (Pre-Shared Key) is an alphanumeric value 1-63 characters in length.

Enter the appropriate values, then click **Apply**.

Note:

If encryption of any kind, at any level is applied to the WA1003A-RU, all devices on the network must comply with all security measures.

Modem Setup

The Modem Setup menu is used to change the Modulation Type used for the ADSL connection. This setting should only be changed if your service provider has given explicit instructions to change it.

Note:

Do not change the (ADSL) Modulation type used unless you have been instructed to do so. If this setting is not configured properly, the WA1003A-RU will not work.

Figure 3-12 Modem Setup menu (change modulation type)

If you are instructed by your ISP to change the Modulation type is used for your service, select the desired modulation type and then click **Apply**. The modulation types available are **T1413**, **G.DMT**, **GLITE** and **MMODE**. By default, the WA1003A-RU will automatically detect the modulation used; this setting is listed as MMODE (Multi-mode).

3.4.5 Configure Connection 1 for PPPoA

PPP or Point-to-Point protocol is a standard method of establishing a network connection/session between networked devices. Different forms of PPP include PPPoA and PPPoE (discussed below) involve an authentication process that requires a username and password to gain access to the network. PPPoA (PPP over ATM) as described in RFC 2364, is a method of using PPP on an

ATM network. ATM is used for many types of telecommunications services including ADSL.

To configure the WAN connection for PPPoA, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

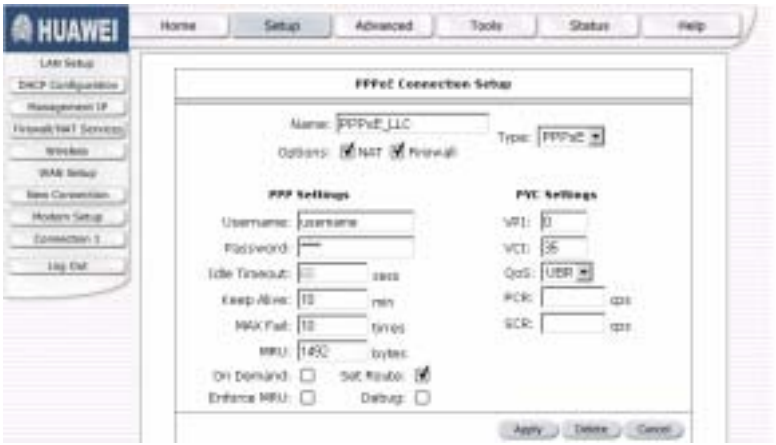

Figure 3-13 PPPoA Connection 1 Setup menu

To configure the default connection type (PPPoA) for Connection 1, follow the steps listed below. To change the connection type of Connection 1 to an alternative type follow the instructions according to the desired type as described below in Change the Connection Type.

1. Click the **Connection 1** button under **WAN Setup** to view the **PPPoA Connection Setup** menu pictured in the example above.
2. Type in a **Name** for the connection or use the default name *WAN_PPPoA* in the space provided.

3. Under **Options**, enable **NAT** and/or **Firewall** by selecting the corresponding selection box.
4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
7. Type the **Username** and **Password** used to verify the identity of your account. Typically, the Username is an account number assigned by your ISP and appears in the form *account#@serviceprovider.com*, while the Password may have been chosen by the account holder. For most users, the remaining settings will not need to be changed. See your ISP for further information.
8. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the WA1003A-RU.
9. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.

10. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

3.5 Change the Connection Type

The default connection protocol used for the WA1003A-RU is Point-to-Point Protocol over ATM (PPPoA). The menu used to configure a PPPoA connection is the first menu to appear when you click on the **Connection 1** button in the Setup menu. The alternative connection types supported by the WA1003A-RU are the **PPPoE** (PPP over Ethernet), **CLIP** (Classical IP over ATM or IPoA), **DHCP** (for WAN), **Static** (IP for WAN), and **Bridge** connection types. There are two ways you may configure the WAN connection to use these alternative types. You can create a **New Connection** using the alternative connection type or you may configure the Connection 1 settings to use the connection type of choice. This section describes how to change the Connection 1 settings to use a different connection type. To change the Connection 1 settings to use a different connection type, follow the instructions below according to the type of connection you want to use. To create and configure a New Connection, skip ahead to Create a New Connection.

3.5.1 Configure Connection 1 for PPPoE

PPP or Point-to-Point protocol is a standard method of establishing a network connection/session between networked devices. PPPoE configuration requires the same basic information as

the previously discussed PPPoA and both menus are nearly identical. It may be worthwhile for the user to change the default name of Connection 1 to something that states what connection type is being used, for example, *WAN_PPPoA*, the name used in the example below. Notice the VPI and VCI values are included in the name. It is not functionally necessary to change the name of the connection, this is done merely to provide descriptive reference.

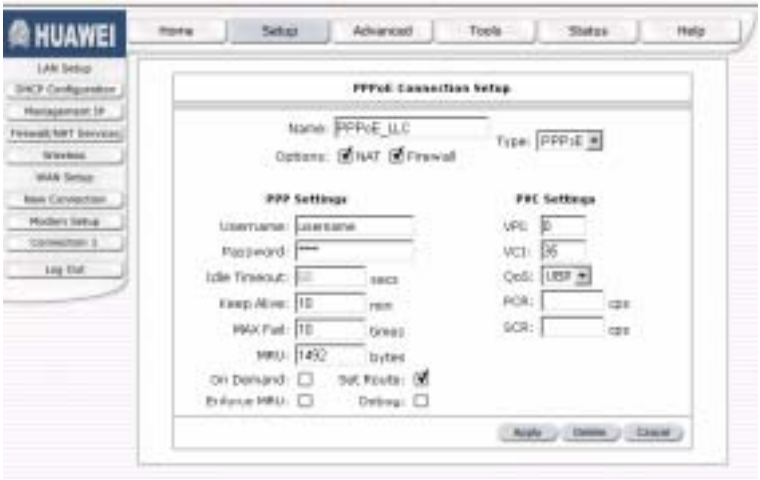

Figure 3-14 Setup – Configure Connection 1 for PPPoE

To configure Connection 1 for PPPoE, follow the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *PPPoE* from the **Type:** pull-down menu. The menu will blink momentarily

3. Type in a **Name:** for the connection or use the default name in the space provided (*WAN_PPPoA* used in the above example).
4. Under **Options**, enable **NAT** and/or **Firewall** by selecting the corresponding selection box.
5. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
6. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
7. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
8. Type the **Username** and **Password** used to verify the identity of your account. Typically, the Username is an account number assigned by your ISP and appears in the form *account#@serviceprovider.com*, while the Password may have been chosen by the account holder. For most users, the remaining settings will not need to be changed. See your ISP for further information.
9. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the WA1003A-RU.

10. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
11. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

3.5.2 Configure Connection 1 for Bridge

"Bridge" means a pure bridged connection with no IP address assigned to the WA1003A-RU. This connection method makes the WA1003A-RU act as a bridge, and just passes packets across the DSL port. When the device is used in this manner, it is necessary to install additional connection software on any computer or server used to access the Internet.

Figure 3-15 Setup – Configure Connection 1 for Bridge

To configure the WAN connection for Bridge, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *Bridge* from the **Type:** pull-down menu. This action will change the menu so it offers fewer settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPoA* is used in the above example).
4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.

6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
7. The **Encapsulation** values LLC (SNAP) and VC (MUX) are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.
8. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the WA1003A-RU.
9. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
10. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

3.5.3 Configure Connection 1 for Static IP for WAN

Static is used whenever a known static IP is assigned. The accompanying information such as the Subnet mask and the gateway should also be specified in order to be able to connect. Up to three

Domain Name Server (DNS) addresses can also be specified. These are the servers would enable you to have access to other web servers. Valid IP addresses range from 0.0.0.0 to 255.255.255.255.

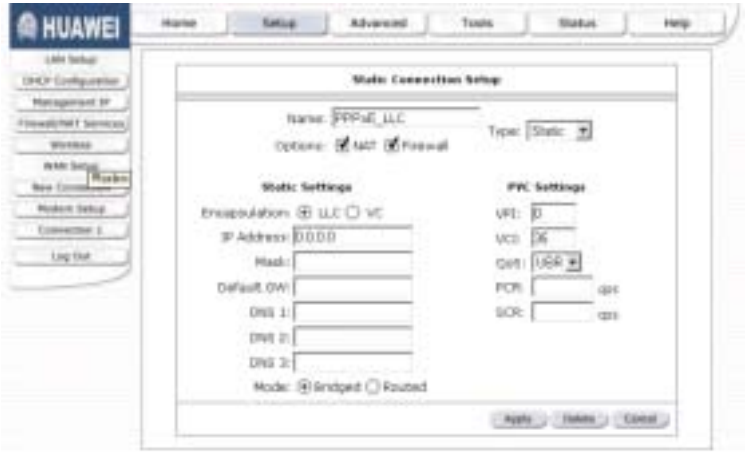

Figure 3-16 Setup – Configure Connection 1 for Static IP for the WAN

To configure the WAN connection for Static, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *Static* from the **Type:** pull-down menu. This action will change the menu so it offers different settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPoA* is used in the above example).

4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
7. The **Encapsulation** values LLC (SNAP) and VC (MUX) are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.
8. Based on the information provided by your ISP, enter the **IP Address**, Subnet **Mask**, **Default Gateway** (if provided), and Domain Name Services (**DNS**) values (if provided).
9. Select the desired **Mode**, **Bridged** or **Routed**.
10. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the WA1003A-RU.
11. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.

12. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

3.5.4 Configure Connection 1 for DHCP for WAN

Dynamic Host Configuration Protocol (DHCP) allows the gateway to automatically obtain the IP address from a DHCP server on the service provider's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the WA1003A-RU requests an IP address.

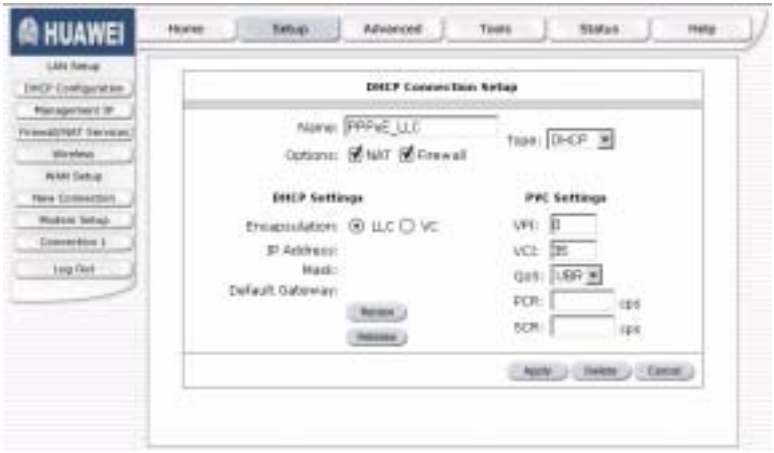

Figure 3-17 Setup – Configure Connection 1 for DHCP service for the WAN

To configure the WAN connection for DHCP, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *DHCP* from the **Type:** pull-down menu. This action will change the menu so it offers different settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPoA* is used in the above example).
4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
7. The **Encapsulation** values LLC (SNAP) and VC (MUX) are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.
8. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to

save the changes you just made and restart the WA1003A-RU.

9. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
10. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

3.5.5 Configure Connection 1 for CLIP

CLIP or IPoA connections function in a similar way to DHCP or Static IP connections. Certain CLIP connections function like P2P networks. The WA1003A-RU must obtain IP settings from a server owned by an ISP, or use a static IP address assigned by the ISP.

Figure 3-18 Setup – Configure Connection 1 for CLIP (IPoA)

To configure the WAN connection for CLIP, perform the steps listed below. Some of the settings do not need to be changed when you first set up the device but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *CLIP* from the **Type:** pull-down menu. This action will change the menu so it offers different settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPoA* is used in the above example).
4. Under **Options**, enable **NAT** and/or **Firewall** by selecting the appropriate checkbox. This option is not available for a Bridge connection.

5. Based upon the information your ISP provided, enter the **IP Address** (e.g. 168.128.1.1), the Subnet **Mask** (e.g. 255.255.255.0), **ARP Server** (e.g. 168.128.1.2) and the **Default Gateway** (e.g. 168.128.1.1).
6. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
7. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
8. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
9. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the WA1003A-RU.
10. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
11. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a

few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

3.6 Create a New Connection

An alternative method of changing the connection type used by the WA1003A-RU is to create a new connection. Creating a new connection will not change the Connection 1 settings, it will make a new set of coneciton configuration settings. The new set created will be labeled **Connection 2**, additional connections created will be likewise labeled Connection 3, Connection 4 and so on. Use the method described here to create up to 8 different connection configuration sets. At any time you may reconfigure the settings for any previously created connection by clicking on the menu button for the connection displayed under the **WAN Setup** heading.

I. New Connection Example 1 - Create a New PPPoE Connection

The example below describes how to set up a new connection that uses a PPPoE type WAN conneciton. To create a new connection:

1. Click on the **New Connection** button.
2. Configure the WA1003A-RU for the **Type:** of conneciton used and all the remaining settings as discussed in the preceding section. In this example, the type of connection used for **Connection 2** is *PPPoE*. Notice also that the VPI and VCI values have been changed.
3. Click the **Apply** button to cerate the new connection. Notice that a new menu button is created (Connection 2), this links to

the configuration menu for Connection 2 (see example below). If at any time you want to change, delete, disconnect or connect this WAN connection, click on the Connection 2 button.

Figure 3-19 Set up a New Connection – Connection 2

II. New Connection Example 2 - Create a New Bridge Connection

You may create new connections to suit different purposes. For example, let's create a new Bridge connection used to connect directly to a server acting as a firewall and proxy.

1. Click the **New Connection** button.
2. Select *Bridge* from the **Type:** menu.
3. Configure the remaining settings (including **VPI:** and **VCI:**) as necessary.

4. Click the **Apply** button. Notice that a new menu button, Connection 3, appears under WAN Setup.
5. Remember to save any newly created connections using the **Save All** procedure in the **Tools/System Commands** menu.

Figure 3-20 Set up a New Connection – Connection 3

To disconnect the Bridge connection, click the **Delete** button.

3.7 DHCP Configuration for LAN

The WA1003A-RU supports three DHCP modes for the LAN. By default, DHCP service is provided using an IP pool of 192.168.1.2 – 192.168.1.254 for a total of 253 IP addresses available. The WA1003A-RU can also relay DHCP service from another server through the WAN port. You may prefer to disable DHCP service and DHCP relay and use a different preferred method for IP addressing on your LAN.

To disable the embedded DHCP server, select the **Server and Relay Off** option and click the **Apply** button.

Figure 3-21 Configure DHCP service for the LAN

For DHCP service on the LAN, select the **Server On** option to enable DHCP service from the WA1003A-RU (enabled by default) and configure DHCP server parameters as follows:

Table 3-1 DHCP Parameter Description

Start IP	Type in the base address for the IP pool of unassigned IP addresses. This IP address must be consistent with the Management IP address of the WA1003A-RU. Normally the Start IP address is one greater than the Management IP address.
End IP	Type in the last address of the contiguous IP address range to be used by the WA1003A-RU for DHCP function. Up to 253 consecutive IP addresses may be used for the pool.
Lease Time	This specifies the amount of time (in seconds) a client can lease an IP address, from the dynamically allocated IP pool.

Click the **Apply** button to make the changes to the DHCP settings. Remember to **Save All** in the **Tools/System Commands** menu.

3.7.2 Enable DHCP Relay

Some service providers provide DHCP service for private networks from their own servers. To enable DHCP service form outside your LAN select the **DHCP Relay** option and type in the server IP address in the **Relay IP** field.

Figure 3-22 Configure DHCP Relay Service

Click the **Apply** button to change the DHCP Relay settings. Remember to **Save All** in the **Tools/System Commands** menu.

3.8 Management IP

The IP address of the WA1003A-RU can be changed to suit the requirements of your LAN. Remember, if you are using DHCP from the WA1003A-RU, the IP address must be consistent with the DHCP IP settings.

Figure 3-23 Configure Management IP

Change IP settings as desired and click the **Apply** button to change the DHCP Relay settings. You may also provide a Host name and Domain name if necessary for your LAN. Remember to **Save All** in the **Tools/System Commands** menu.

3.9 Save Configuration Changes

Any changes made to the WA1003A-RU's configuration must be saved to non-volitile memory or they will be lost if the WA1003A-RU is restarted or powered off. When you are finished making changes to the WA1003A-RU settings, follow the instructions here to save the new settings.

Figure 3-24 WA1003A-RU Tools Menus

Click on the **Tools** tab to access the **System Commands** menu link - then click the System Commands link to see the menu pictured below.

Figure 3-25 Available System Commands

3.10 Advanced WA1003A-RU Management

Click the **Advanced** tab to access menus used to configure **UPnP**, **Port Forwarding**, **Access Control**, **Advanced Security** (including NAT, Firewall and DMZ setup), **LAN Clients**, **Bridge Filters**, **Multicast** pass-through, **Static Routing** and **Dynamic Routing** (RIP setup).

Figure 3-26 Advanced setup main menu

3.10.2 UPnP

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network,

obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network.

UPnP can be supported by diverse networking media including Ethernet, 802.11b wireless, Firewire, phoneline and powerline networking.

Figure 3-27 Advanced – UPnP window

To enable UPnP for any available connection, click to check the **Enable UPnP** selection box, select the connection or connections on which you will enable UPnP listed under **Available Connections** and click the **Apply** button.

3.10.3 LAN Clients

The LAN Clients menu is used when establishing Port Forwarding, Access Control and Advanced Security rules for IP addresses on the LAN. This menu can be accessed directly by clicking on the **LAN Clients** button or hyperlink in the **Advanced** setup menu. You can also click on the New IP button located in the Port Forwarding, Access Control and Advanced Security menus to access this menu. In order to use these advanced features it is necessary to have IP addresses available for configuration. If there are no IP addresses listed in the LAN Clients menu, it will not be possible to configure Port Forwarding, Access Control and Advanced Security.

Use the LAN Clients menus to add or delete static IP addresses for the advanced functions mentioned above, or to Reserve a Dynamically assigned IP address for an advanced function. Dynamically assigned IP addresses will only be listed if DHCP is enabled on the WA1003A-RU.

Figure 3-28 LAN Clients Setup

To add a static IP address to the list of available IP addresses, type an IP address that falls within the range a available IP addresses and click on the **Add** button. In the example above, available addresses range from 10.0.0.1 to 10.255.255.254. Any addresses added will appear in the list of **Static Addresses** available for advanced configuration. These addresses can then be used in the other Port Forwarding, Access Control and Advanced Security menus.

To delete an IP address from the list of Static Addresses, click the **Delete** box for the address or addresses you want to eliminate and click on the **Apply** button.

Dynamically assigned IP addresses may be reserved so that the lease does not expire for the LAN IP address. Click the Reserve box for the address or addresses you want to reserve and click the Apply button. These addresses will become Static IP addresses and will no longer be available for DHCP assignment.

3.10.4 Port Forwarding

Port Forwarding allows specific functions to bypass NAT protection that would otherwise not allow them to function. To use Port Forwarding, you must have specific client IP addresses available for configuration. Use the LAN Clients menu to establish client IP addresses available for port forwarding.

Note:

In order to use Port Forwarding, Firewall support must be enabled. See Keep in mind that when this is enabled, the WA1003A-RU may be vulnerable to denial of service type attacks.
in the Advanced Security menu.

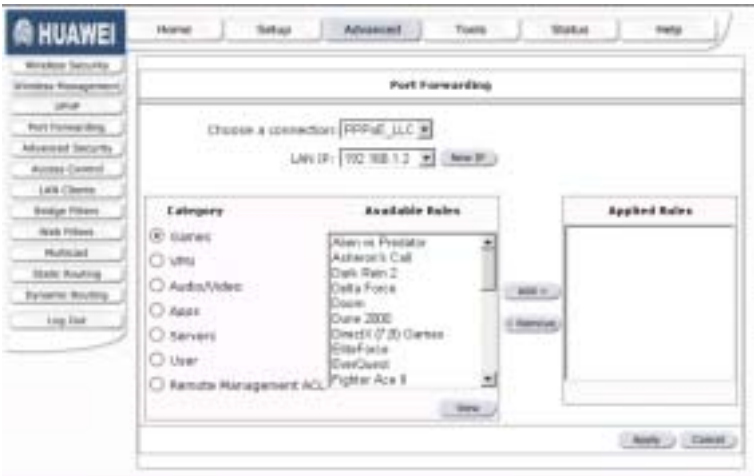

Figure 3-29 Advanced – Port Forwarding window

There are many different pre-configured rules available for specific functions such as Internet gaming, VPN, streaming and interactive multi-media, standard TCP/IP protocols, reserved ports, p2p, network management applications, and so on.

You may also create customized rules to manage TCP/UDP ports. The pre-configured rules include those listed in the table here:

Table 3-2 Category Available Rules

Games	Alien vs. Predator, Asheron's Call, Dark Rein, Delta Force, Doom, Dune, DirectX Games, EliteForce, EverQuest, Fighter Ace II, Half Life, Heretic II, Hexen II, Kali, Motorhead, MSN Gaming Zone, Myth: The Fallen Lords, Need for Speed Porsche, Need for Speed 3, Outlaws, Rainbow 6, Starcraft, Tiberian Sun, Ultima, Unreal Tournament.
VPN	IPSec, PPPTP
Audio/Video	Net2Phone, Netmeeting, QuickTime
Applications	VNC, Win2k Terminal, PC Anywhere, Netbios, RemoteAnything, Radmin, LapLink, CorbonCopy, Gnutella.
Servers	Quake 2, Quake 3, Unreal, Web, FTP, Telnet, DNS, LDAP, NNTP, SMTp, POP 2, POP3, IMAP, IRC, Lotus, Remote.
User	Use this to set up custom TCP/UDP port rules.

To configure a new port-forwarding rule for any of the pre-configured rules, follow these steps:

1. Select the WAN connection you want to use for the new rule from the **Choose a connection** pull-down menu.

2. Select a **LAN IP** from the available client IP addresses listed in the pull-down menu; or, create a **New IP** by clicking the button. This brings up the LAN Client menu (see above).
3. Select the **Category** of the rule you are creating. The **Available Rules** for the category appear listed.
4. Highlight to select the Available Rule you want to apply.
5. Click on the **Add>** button to place the rule in the **Applied Rules** list of port forwarding that are actively applied to the client

The Available Rules can be applied to a single client IP address. That is, it is not possible to use an applied rule for multiple IP addresses on the LAN.

The **User** category for port forwarding is used to set up customized port forwarding rules.

Figure 3-30 Set up Custom Port Forwarding Rules

To set up custom TCP or UDP port forwarding rules, follow these steps:

1. Select the User category and click the **Add** button located below the Available Rules list. This will change the menu to look like the example below.

Figure 3-31 Port Forwarding User Rules Management

2. Type a **Rule Name** in the space provided.
3. Select the port **Protocol** from the pull-down menu - you may select *TCP*, *UDP* or both (*TCP/UDP*).
4. Configure a range of ports for forwarding. Type the lowest numbered port in the range in the Port Start space. Type the highest numbered port in the Port End space. For a single port, just enter the same number in both spaces.
5. Type a number for the Port Map in the space provided.

6. Click the **Apply** button to create the new rule. The new rule will appear listed in the table of custom port forwarding rules.

3.10.5 Access Control

Access Control settings are used to block various services and protocols for specific client IP addresses. The configuration process is similar setting up port forwarding, except access control will deny specific functions to client IP addresses. There are pre-configured rules for specific functions that may be blocked or you can block specific UDP or TCP ports. Access control operates for specific IP addresses across all WAN connections. If you are using more than one WAN connection, a single set of access rules is maintained for each controlled IP address that operates on all WAN connections.

Note:

In order to use Port Access Control, Firewall support must be enabled. See Keep in mind that when this is enabled, the WA1003A-RU may be vulnerable to denial of service type attacks.
in the Advanced Security menu.

Figure 3-32 Access Control menu

Remember, if the client IP address you want does not appear listed in the LAN IP pull-down menu, click on the New IP button to go to the LAN Clients menu.

To block all traffic from the WAN port to a specific IP address, select the **LAN IP** address to block and click to check the **Traffic Type __ Any** selection box, then click the **Apply** button. This will block all traffic from the WAN port to the specified client.

Remember to save the configuration changes.

Access Control pre-configured rules are the same as for port forwarding:

Table 3-3 Category Available Rules

Games	Alien vs. Predator, Asheron's Call, Dark Rein, Delta Force, Doom, Dune, DirectX Games, EliteForce, EverQuest, Fighter Ace II, Half Life, Heretic II, Hexen II, Kali, Motorhead, MSN Gaming Zone, Myth: The Fallen Lords, Need for Speed Porsche, Need for Speed 3, Outlaws, Rainbow 6, Starcraft, Tiberian Sun, Ultima, Unreal Tournament.
VPN	IPSec, PPPTP
Audio/Video	Net2Phone, Netmeeting, QuickTime
Applications	VNC, Win2k Terminal, PC Anywhere, Netbios, RemoteAnything, Radmin, LapLink, CorbonCopy, Gnutella.
Servers	Quake 2, Quake 3, Unreal, Web, FTP, Telnet, DNS, LDAP, NNTP, SMTp, POP 2, POP3, IMAP, IRC, Lotus, Remote.
User	Use this to set up custom TCP/UDP port rules.

To configure a new Access Control rule for any of the pre-configured rules, follow these steps:

1. Select a **LAN IP** from the available client IP addresses listed in the pull-down menu; or, create a **New IP** by clicking the button. This brings up the LAN Client menu (see above).
2. Select the **Category** of the rule you are creating. The **Available Rules** for the category appear listed.
3. Highlight to select the Available Rule you want to apply.

4. Click on the **Add>** button to place the rule in the **Applied Rules** list of port forwarding that are actively applied to the client

The Available Rules can be applied to a single client IP address. That is, it is not possible to use an applied rule for multiple IP addresses on the LAN.

To set up custom TCP or UDP access control rules, follow these steps:

1. Select the User category and click the **Add** button located below the Available Rules list.
2. In the new menu that appears, type a **Rule Name** in the space provided.
3. Select the port **Protocol** from the pull-down menu - you may select *TCP*, *UDP* or both (*TCP/UDP*).
4. Configure a range of ports for forwarding. Type the lowest numbered port in the range in the Port Start space. Type the highest numbered port in the Port End space. For a single port, just enter the same number in both spaces.
5. Type a number for the Port Map in the space provided.
6. Click the **Apply** button to create the new rule. The new rule will appear listed in the table of custom port control rules.

3.10.6 Advanced Security

Use the Advanced Security features of the WA1003A-RU to globally enable or disable NAT and Firewall protection for any WAN connection, enable or disable DMZ IP addresses, enable or disable

remote Telnet or web management from specified IP addresses, and enable/disable ICMP ping packets from the WAN.

Figure 3-33 Advanced Security menu

Follow the instructions below to set up the Advanced Security features. To enable ICMP Ping packets from the WAN, click to check the **Allow Incoming ICMP Ping** selection box and click the **Apply** button. The ICMP (Internet Control Message Protocol) Ping packet is used to test connectivity of IP devices. Keep in mind that when this is enabled, the WA1003A-RU may be vulnerable to denial of service type attacks.

Enable/Disable NAT and Firewall

NAT and basic Firewall protection can be enabled or disabled for any WAN connection. These may also be enabled or disabled when configuring the WAN connection for any connection type except Bridge connections. By default, they are enabled for WAN

connections (except Bridge connections) when they are first set up. Firewall protection includes the previously discussed Port Forwarding and Access Control. Therefore, this must be enabled to use these features.

To enable NAT and Firewall protection for any WAN connection including Bridge type connections, check the **Enable NAT and Firewall Services** selection box and click the **Apply** button. Be sure to save the changes in the System Commands menu or the settings will be lost.

To disable NAT and Firewall Services, deselect it and click the **Apply** button. Be aware that this remove basic security and expose your LAN to potentially malicious agents form the WAN.

Remember to save the configuration changes.

DMZ IP Address

A DMZ address is used for a device that is not given basic protection of NAT and Firewall services. You may select an IP address from the pull-down menu or create a **New IP** by pressing the button. This brings up the LAN Clients menu in which you may create a static client IP or reserve a dynamically assigned IP address for DMZ designation.

Setup Remote Management

Telnet and web management through the WAN port can be enabled for specified IP addresses. To enable remote management, click to check the selection box for **Remote Telnet** or **Remote Web** and type in an IP address and net mask of a trusted host.

3.10.7 Bridge Filters

Bridge filters are used to block or allow various types of packets through the WAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. You can set up filter rules and disable the entire set of rules without loosing the rules that have been configured.

Figure 3-34 Bridge Filters menu

To add a bridge filter rule, check **Enable Bridge Filters**, type in a Source MAC, a Destination MAC or both in the entry fields, and click the **Add** button. To edit an existing rule, select the rule by clicking the **Edit** radio button. The rule will appear in the entry fields above as it is currently configured. Make the desired changes and click the **Add** button. To remove a bridge filter from the table in the bottom half of the window, click to select the corresponding **Delete** box, and then click **Apply**. Remember to save the configuration changes.

The protocols that may be specifically allowed or denied to pass through the WAN interface are the following: *IPv4, IPv6, RARP, PPPoE Discovery* and *PPPoE Session.*

3.10.8 Multicast Pass-through

Multicast pass-through can be enabled or disabled for any WAN connection. When enabled it allows IGMP packets to pass through the WAN interface. IGMP packets are used to control multicasts and discontinue multicasts to individual IP addresses when they are no longer needed.

Figure 3-35 Multicast pass-through menu

To enable Multicast pass through for any WAN connection, select the connection and click the **Enable IGMP Multicast** box to select the option, then click the **Apply** button. Remember to save the configuration changes.

3.10.9 Static Routing

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway.

Figure 3-36 Static Routing menu

To add a static route, choose a connection from the pull-down menu and then enter a **New Destination IP** address, subnet **Mask**, **Gateway** IP address and **Metric** value. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation.

To remove a static route from the table in the bottom half of the window, choose to **Delete** it from the table and click the **Apply** button. Remember to save the configuration changes.

3.10.10 Dynamic Routing

The WA1003A-RU supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices. It also supports use of password protection which requires password verification for RIP requests. Use the Dynamic Routing menu to enable RIP and if desired to configure password protection.

Figure 3-37 Dynamic Routing (RIP) menu

To enable RIP v1, check **Enable RIP**, select *RIP v1* **Protocol**, select the **Direction** (*In*, *Out*, or *Both*), and click **Apply**. To enable *RIP v2* or *RIP v1 Compatible*, select the appropriate **Protocol** and **Direction** and click **Apply**. To use password protection for RIP v2 or RIP v1 Compatible protocols, check **Enable Password**, enter a **Password**, and click **Apply**.

3.11 Wireless Management

For added security you can opt to use Access Control based on the MAC address. This feature lets you create a list of MAC addresses that are allowed or denied association with the WA1003A-RU through the wireless interface. When it is enabled, the access point is instructed to forward packets only from wireless devices only if the MAC address of the device is granted association. Packets received through the wireless interface from non-authorized devices, including other access points, will be dropped.

Click **Enable Access List**.

Enter a MAC Address in the box, choose **Allow** or **Ban,** then click **Apply.**

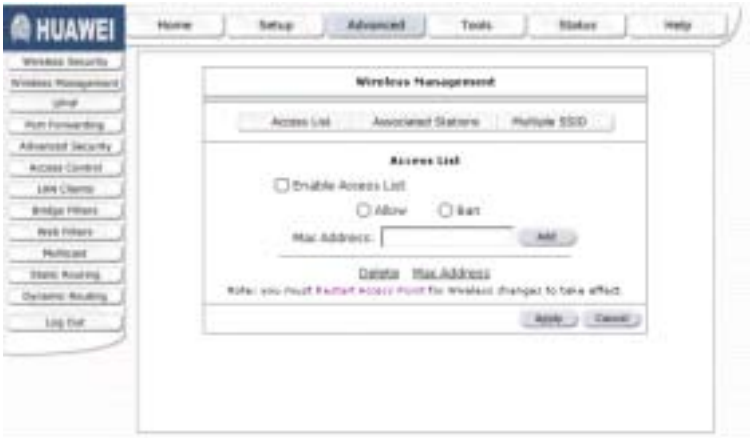

Figure 3-38 Access Control based on the MAC address

3.12 Multiple Virtual Connections

The WA1003A-RU can use up to eight simultaneous PVC connections. These additional connections occupy the same bandwidth used for ADSL service. Additional PVC connections can be added to establish a private connection to remote offices or maintain a server accessible through the WAN port. Provision for additional PVC profiles must be done through the telephone company or telecommunications services company. The remote user must have suitable ADSL equipment for a successful connection.

The New Connection menu is used to configure additional WAN connection that can operate simultaneously with the other connections. PPPoE type WAN connections can be disconnected or connected as needed. Non-PPPoE type connections must be deleted from the configuration settings if you want to disable them.

To set up additional virtual connections, follow the procedure described in Create a New Connection. Keep in mind that each new connection must have a VPI/VCI value set that is unique to the WA1003A-RU. The numbers for these values will be provided by your service provider.

PPPoE and PPPoA connections may be connected and disconnected with the **Connect** and **Disconnect** menu buttons located in the connection settings menu.

The remaining connection types (Bridge, Static, DHCP and CLIP) connect upon saving the settings and restarting the WA1003A-RU. These connections can be disconnected only if the connection set is deleted. To delete any WAN connection set, click on the **Delete** button in the menu for the connection.

3.13 Tools and Utility Menus

The menus lited under the Tools tab are used for **System Commands** to save settings, restart and reset the WA1003A-RU; to set up **Remote Log** information; for **User Management**; to update firmware and load saved configuraiton files (in the **Update Gateway** menu); to perform a **Ping** test; and to test the DSL network connectivitiy in the **Modem Test** menu.

Figure 3-39 Tools and utility menu links

Click the hyperlink or menu button to view the desired menu.

3.13.2 User Management

It is a good idea to change the management user information used for the WA1003A-RU before or immediately after establishing a link to the WAN.

Figure 3-40 User Management menu

To change the user name and password used for management access to the WA1003A-RU:

1. Type the current **User Name** in the entry field provided.
2. Type in the new **Password** in the entry field provided.
3. Type in the new password again in the **Confirm Password** field.
4. If desired, change the **Idle Timeout** value.
5. Click **Apply**.

3.13.3 System Commands

The System Commands are used to save settings to non-volatile memory, to reboot the WA1003A-RU and to restore factory default settings to the WA1003A-RU.

Figure 3-41 Tools – System Commands menu

Click on the appropriate menu button to perform the following system tasks:

Table 3-4 System Function Description

Save All	In order to save the configuration changes you have just made they must be saved to the WA1003A-RU's non-volatile RAM by clicking on the Save All button.
Restart	Click the Restart button to restart the WA1003A-RU. If you have not saved your changes, the WA1003A-RU will revert to the previously saved configuration upon rebooting the WA1003A-RU.
Restart AP	Click to restart the Wireless AP (Access Point). The Wireless AP must be restarted any time wireless configuration is changed.
Restore	The WA1003A-RU can be reset to the default configuration for all settings using the Restore option. This will also change the both the LAN and WAN IP address of the device, so these will need to be reconfigured accordingly. To perform a factory reset, click the Restore button. Since the IP settings will return to their default, you will lose access to the Web Manager. To use the Web Manager interface, the LAN IP address will need to be reconfigured.

3.13.4 Remote Log

Us the Remote Log menu to set up logging to servers or computers that are located outside the LAN or subnet of the WA1003A-RU.

Figure 3-42 Remote Log menu

Select the **Log Level** from the pull-down menu. The levels available are: *Alert, Critical, Debug, Error, Info, Notice, Panic* and *Warning*. Type in the IP address of a receiver for the log message in the **Add an IP** Address field and click on the **Add** button. Log message receivers that are added appear listed in the **Select a logging destination** pull-down menu. These may be used at any time for other types of log messages. To remove a log message receiver from the list, select it and click on the **Remove** button. Click the **Apply** button when you have configured the log message receivers. Remember to save the settings to non-volatile memory.

3.13.5 Update Gateway

Use the Update Gateway feature to load the latest firmware for the device. You can obtain the latest version of the WA1003A-RU firmware by logging onto the Huawei web site at www.dlink.com. Save

the latest firmware version to a file on your computer or an accessible TFTP server.

Figure 3-43 Tools – Update Gateway window

To upgrade firmware, type in the name and path of the file in the Select a Firmware image file space or click on the **Browse** button to search for the file. Click the **Update Gateway** button to begin copying the file. The file will load and restart automatically.

Use the Configuration – Backup & Restore features to store current settings to a file on your computer or to load previously saved configuration files on the device.

To save the current settings to a configuration file on your computer, type in the full name and path in the Select a Configuration file space or click on the **Browse** button to search for the file. Click the **Back Up** button to initiate this action.

To load a saved configuration file from the computer, type in the full name and path in the Select a Configuration file space or click on the **Browse** button to search for the file. Click the **Restore** button to initiate this action.

3.13.6 Ping Test

The Ping Test menu allows you to ping any IP address from the WA1003A-RU to test connectivity to the address.

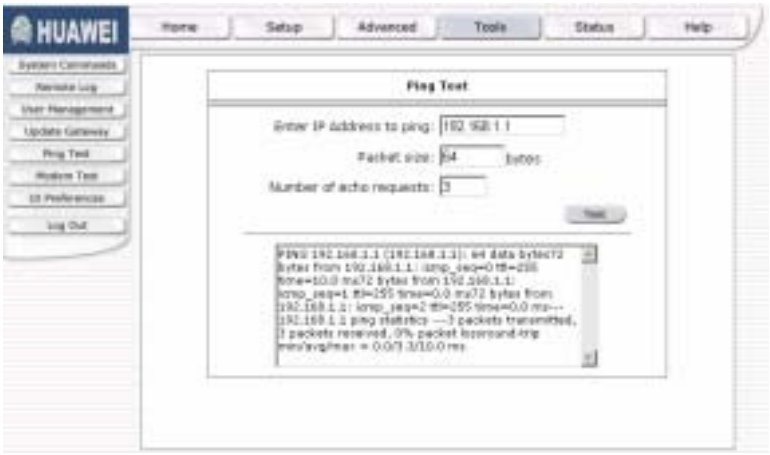

Figure 3-44 Tools – Ping Test window

To Ping a device, first enter the IP address of the device that you wish to Ping into the first field, the Packet Size (in bytes) in the second field, and finally, enter the number of times you wish the Ping function to attempt a connection to the desired device into the third field. Click **Test** to start the Ping mechanism. The results of the Ping will be shown in the result box in the bottom half of the window.

3.13.7 Modem Test

The Modem Test menu is used for trouble shooting connection problems on the WAN interface. You can test for connectivity on the service provider's network for any WAN connection. Test for F5 or F4 connection on the near segment or end-to-end.

Figure 3-45 Tools – Modem Test window

To test your modem, select a **Connection**, choose a **Test Type**, and click **Test**.

3.14 Status Menus

Use the Status windows to display various performance data about the WA1003A-RU

Figure 3-46 Status display links

Click the hyperlink or menu button for the desired Status window.

3.14.2 Network Statistics

Figure 3-47 Network Statistics window

Choose the desired interface at the top of the window and then click **Refresh** to view Ethernet network statistics.

3.14.3 Connection Status

Figure 3-48 Connection Status window

Click **Refresh** to view connection status information.

3.14.4 DHCP Clients

This window displays the status of all current DHCP clients.

Figure 3-49 DHCP Clients window

3.14.5 Modem Status

This window displays DSL statistics and various modem status data.

Figure 3-50 Modem Status window

3.14.6 Product Information

This window displays product information including hardware and firmware versions.

Figure 3-51 Product Information window

3.14.7 System Log

The system log displays chronological event log data.

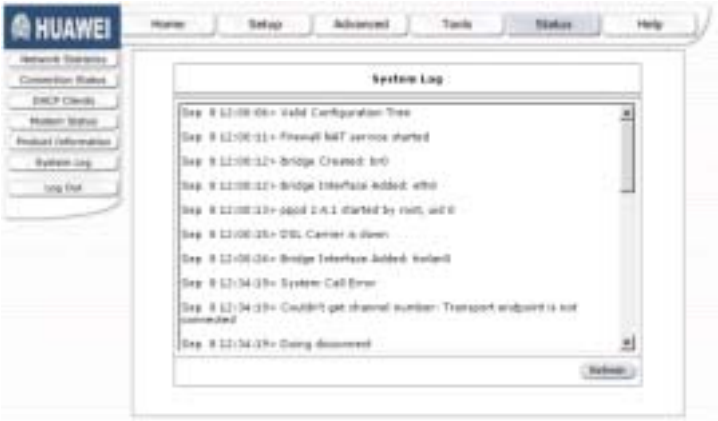

Figure 3-52 System Log window

Click **Refresh** to get the most current system log information.

3.14.8 Help Menu

Help menu links provide more information for configuring various WA1003A-RU functions.

Figure 3-53 Opening Help window

Chapter 4 Trouble Shooting

If you have trouble for using，Please refer to table4-1：

Table 4-1 Trouble Shooting Table

Trouble	Solution
The indicator of power supply is not on	1.Make sure the connection of power supply is correct. 2.Make sure the switch of power supply is turned on. 3.Make sure the output of power supply is correct.
The indicator of PC is not on	1.Check the connection of cable and network adapter. 2.Make sure that the correct cable is used. 3.Make sure the cable works fine by pinging the host IP address.
Can not access Internet or remote networks	1.Make sure the problems list above are all eliminated. 2.Make sure WA1003A-RU software configuration is correct. 3.Make sure you have restarted WA1003A-RU after modifying configuration. 4.Check IP connection using ping command. 5.Make sure the DNS of computer is correct.
Can't access some WEB server	1.The MTU of operating system might be too large 2.Upgrade the operating system with patches.
Can not log in the configuration page	1.Make sure the PC indicator is on. 2.Make sure the configuration of TCP/IP is correct.

Trouble	Solution
	3.Make sure the data indicator of device is on when using Ping command. 4.Make sure the user name and password is correct. 5.Reset the device.。
Wireless mode can't work	1.Make sure the problems list above are all eliminated; 2.Make sure the WLAN card in computer works well. Check the wireless mode is "infrastructure"; 3.Make sure that "wireless" is shown on the configuration page of the device. Otherwise there should be hardware error for the device. Please ask manufacturer to change a new device. 4.Make sure the WLAN card of the computer has the same SSID as that of the device; 5.Check the Security mode. If the encryption is on , make sure the keys is correct. To avoid the possible problems for encryption setting, please don't set the WEP mode with wireless PC card.

Chapter 5 Specifications

Table 5-1 WA1003A-RU Specifications

Item	Feature
Standards	ITU G.992.1 (G.dmt), ITU G.992.2 (G.lite) ITU G.994.1 (G.Hs), ITU-T Rec. I.361 ITU-T Rec. I.610 , IEEE 802.3 IEEE 802.3u , IEEE 802.1d RFC 791 (IP Routing), RFC 792 (UDP) RFC 826 (ARP), RFC 1058 (RIP 1) RFC 1389 (RIP 2), RFC 1213 compliant RFC 1483 (Bridged Ethernet) RFC 1577 (IP over ATM) RFC 1661 (PPP), RFC 1994 (CHAP) RFC 1334 (PAP), RFC 2364 (PPP over ATM) RFC 1631 (NAT), RFC 1877 (Automatic IP assignment), RFC 2516 (PPP over Ethernet) Supports RFC 2131 and RFC 2132 (DHCP) Compatible with all T1.413 issue 2 (full rate DMT over analog POTS), and CO DSLAM equipment Supports ATM Forum UNI V3.1 PVC
Data Rate	1，2，5.5，11Mbps G.dmt full rate: Downstream up to 8 Mbps Upstream up to 640 Kbps G.lite: Downstream up to 1.5 Mbps Upstream up to 512 Kbps
Transmission Technology	DSSS，CCK
Modulation Techniques	DBPSK @ 1Mbps DQPSK @ 2Mbps CCK @ 5.5Mbps and 11Mbps
Protocol& Standard	TCP/IP, UDP, RIP-1,RIP-2, IGMP, DHCP BOOTP, ARP, AAL5
Operating Frequency	2400 ~ 2483.5MHz

Item	Feature
Network Mode	Infrastructure
Channels	13
No Lapping Channel	1，6，11
Receiver Sensitivity	–84dBm @ 11Mbps –87dBm @ 5.5Mbps –89dBm @ 2Mbps –92dBm @ 1Mbps
Transmit Power	15dBm ± 2dB
Operating Range	Free Space:>100m
Antenna	Monopole Antenna
Encryption	64/128 bit WEP
Media Interface	RJ-11 port ADSL telephone line connection RJ-45 port for 10/100BASET Ethernet connection
Device Management	Web
AC Inputs: Power Adapter:	Input: 120V AC, 60 Hz Output: 12V AC, 1.2A
Power Consumption:	12 Watts (max)
Operating Temperature:	0 to 45 C (32 - 113° F)
Humidity:	5 to 95% (non-condensing)
Dimensions:	180 x 141 x 30 cm (device only)
Weight:	380 grams (device only)
EMI:	CE Class B, FCC Class B (Part 15)
Safety:	CSA 950, UL 1950, IEC 60950, EN 60950
Reliability:	Mean Time Between Failure (MTBF) min. 4 years

Chapter 6 Appendix

6.1 Factory Default Settings

User name		admin	
Password		admin	
IP address		192.168.1.1	
Subnet mask		255.255.255.0	
DSL Mode		Multimode	
PVC0	RFC 2684 Bridged Mode	VPI =0	VCI=35
PVC1	RFC 2684 Bridged Mode	VPI =8	VCI=35
PVC2	RFC 2684 Bridged Mode	VPI= 0	VCI= 100
PVC3	RFC 2684 Bridged Mode	VPI =0	VCI=32
PVC4	RFC 2684 Bridged Mode	VPI =8	VCI=81
PVC5	RFC 2684 Bridged Mode	VPI= 8	VCI=32
PVC6	RFC 2684 Bridged Mode	VPI= 14	VCI=24
DHCP Mode		Disable	
NAT		Enable	

6.2 Abbreviations

ADSL	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
AP	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSLAM	Digital Subscriber Line Access Multiplex
HTML	Hypertext Markup Language
IP	Internet Protocols
ICMP	Internet Control Message Protocol
IPoA	Internet Protocols Over ATM
ISP	Internet Service Provider
LAN	Local Area Network
MA	Media Access Module
MAC	Media Access Control
MIB	Management Information Base
NIC	Network Interface Card

NMS	Network Management Station
PPP	Point to Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PVC	Permanent Virtual Connection
RAM	Random Access Memory
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
TCP	Transfer Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
WAN	Wide Area Network
WLAN	Wireless LAN