

Zhone 6652-A2 VDSL2 Users Guide

Document Part Number: 830-01754-03
May 2008



Z H O N E_™

Zhone Technologies, Inc.
@ Zhone Way
7001 Oakport Street
Oakland, CA 94621
USA
510.777.7000
www.zhone.com
info@zhone.com

COPYRIGHT ©2000-2008 Zhone Technologies, Inc. All rights reserved.

This publication is protected by copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission from Zhone Technologies, Inc.

Bitstorm, EtherXtend, IMACS, MALC, MXK, Raptor, SLMS, Z-Edge, Zhone, ZMS, zNID and the Zhone logo are trademarks of Zhone Technologies, Inc.

Zhone Technologies makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability, non infringement, or fitness for a particular purpose. Further, Zhone Technologies reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Zhone Technologies to notify any person of such revision or changes.

Table of Contents

Chapter 1. Introduction	5
Product Overview	5
Features	5
Device Requirements	5
Packaging	6
System Description	7
WAN (VDSL Line) Interface	7
Local Interface	7
Reset Switch	7
Status Indicators	8
Rear Panel	9
Hardware Installation	10
Default Values	10
 Chapter 2 Connecting your device	 1
Connecting the Hardware	1
Next step	2
 Web User Interface	 3
Accessing the Web pages	3
Advanced Setup	4
Management	4
Commonly used buttons	5
Help information	5
Testing your Setup	5
Default device settings	6
Basic Setup	8
Operation Mode	8
Internet Port	8
PPPoE Connection	9
DHCP (Dynamic IP Configuration)	10
Static IP Configuration	11
Local Port	12
 Advanced Setup	 13
Access Control List	13
Dynamic DNS	14
Firewall	15
Static Routes	17
Dynamic Routes	18
UPnP	18
Virtual Server	19
IP QoS	21
QoS Scheduler	21
QoS Policy	22
Port-Based VLAN	23

Management	24
Remote Management.....	24
System Reset.....	25
Firmware Upgrade	25
Network Status	26
Save Configuration	27
Diagnostic	28
Time	28
 Appendix A - Configuring the Internet Settings	 29
Configuring Ethernet PCs	29
Before you begin.....	29
Windows® XP PCs	29
Windows 2000 PCs	29
Windows Me PCs	30
Windows 95, 98 PCs	31
Windows NT 4.0 workstations	31
Assigning static Internet information to your PCs.....	32
 Appendix B - Troubleshooting	 33
Troubleshooting Suggestions	33
Diagnosing Problem using IP Utilities	34
Ping.....	34
Nslookup.....	34
 Appendix C – Glossary	 37
 Appendix D - Specification	 45
A1. Hardware Specifications for 6652–A2.....	45
A2. Software Specifications.....	46

Chapter 1. Introduction

Product Overview

The **6652–A2** is an Ethernet-over-VDSL gateway that complies with various VDSL standards, and provides unprecedented broadband service over a single pair of copper wires. Four 10/100 Base-T Ethernet ports can easily connect to any PC or LAN in home or small office environments. The **6652–A1** delivers a compact, cost-effective, and innovative solution.

Features

- Built-in four-port 10/100BaseTX Ethernet switch for PC or LAN connection
- High Speed Data Transmission on Twisted Copper Pair Wire
- User-friendly configuration program accessed via a web browser
- Service providers can deploy VDSL rapidly over existing wire infrastructure (POTS line)
- Supports mandatory and optional features of VDSL2 (G.993.2) standard
- Supports VDSL2 profiles, 8a/8b/8c/8d, 12a/12b, 17a and 30a
- Supports the speed of downstream or upstream up to 100Mbps
- Supports bridge and router mode
- Interchangeable between Bridge and Router mode
- Provides security for your LAN and multiple PCs surfing Internet simultaneously using Network address translation (NAT) functionality
- Network configuration through DHCP Server and DHCP Client
- Services including IP route, QoS and UPnP
- Configuration and management with Telnet through the Ethernet interface, and remote Telnet through VDSL interface
- Firmware upgradeable through HTTP

Device Requirements

In order to use the **6652–A2**, you must have the following:

- DSL service up and running on your telephone line
- Instructions from your ISP about the type of Internet access, and the addresses needed to set up access
- One or more computers, each containing an Ethernet card (10Base-T/100Base-T network interface card (NIC)).
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v4 or later, or Netscape v4 or later. Note that version 4 of each browser is the minimum version requirement – for optimum display quality, use Internet Explorer v5, or Netscape v6.1



Note

You do not need to use a hub or switch in order to connect more than one Ethernet PC to the device. Instead, you can connect up to four Ethernet PCs directly to the device using the ports labeled LAN1 to LAN4 on the rear panel.

Packaging

This package consists of the following items:



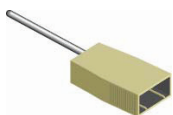
6652-A2 VDSL2 Gateway



RJ-45 Cable



RJ-11 Cable



Single Line DSL Filter



AC Adapter



User's Manual CD

System Description

WAN (VDSL Line) Interface

The two-wire VDSL loop has line impedance 100 Ohms in RJ-11 or RJ-45 connector, and complies with ITU-T G.993.2, G.993.1, ANSI T1.424, ETSI TS 101 270-1 and TS 101 270-2.

Local Interface

Four 10/100 Mbps Ethernet ports in RJ-45 connectors with switching functionality, comply with IEEE 802.3/3u. Each port features auto-negotiation of link speed, and can be configured individually with different QoS level and priority via web interface. Auto MDI/MDIX function allows using either crossover or straight cable to connect to hub or PC easily.

Reset Switch

The reset switch serves two functions:

- Reset the device
Push down the switch and release immediately to reset the device.
- Reset and restore default settings
Push down and hold the switch for 6 seconds, then release. This device will reset then restore its default settings.

Status Indicators

The front panel has four front panel status indicators: LAN, PPP, DSL and PWR.



Label	Indicator	Function
PWR	Blinking Red	Only occurs when you open the modem, the light will become green after five seconds.
	Green	The device is powered on
	Red	The device failed to boot
DSL	Green	DSL link reaches showtime, which means that your device has successfully connected to your ISP's DSL network.
	Blinking Green	Device is attempting to connect to the ISP's DSL network
	Off	Device not successfully connected to the ISP's DSL network
PPP	Green	Device has established a PPP connection
	Red	PPP disconnection
LAN	Green	LAN link established and active
	Blinking Green	Data is being transmitted
	Off	No LAN link

Rear Panel

The rear panel has a power switch and jack, a reset button, a DSL jack for connecting the device to the network and four Ethernet jacks.



6652-A2 Rear Panel Connections

Label	Function
Power Switch	ON/OFF switch
Power Jack	Connects to the supplied power adapter
RES	A reset button to reset the device or reset to default settings
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
DSL Jack	Connects to the ISP's DSL network

Safety Guidelines

In order to reduce the risk of fire, electric shock and injury, please adhere to the following safety guidelines.

- ✓ Carefully follow the instructions in this manual; also follow all instruction labels on this device.
- ✓ Only use the power adapter supplied with the device.
- ✓ Do not spill liquid of any kind on this device.
- ✓ Do not place the unit on an unstable stand or table; the unit may drop and become damaged.
- ✓ Do not expose this unit to direct sunlight.
- ✓ Do not place any hot devices close to this unit, as it may degrade or cause damage to it.
- ✓ Do not place any heavy objects on top of this unit.
- ✓ Do not use liquid cleaners or aerosol cleaners. Use a soft dry cloth for cleaning.

Hardware Installation

1. *Plug the AC adapter into an AC power socket, and connect its jack to the 6652–A2 power inlet.*
2. *Restore this device to factory defaults if necessary, e.g., Current settings may not be correct because it has been installed and configured before. Please refer to Reset Switch on page 5 for further detail.*
3. *Connect one end of the RJ-45 cable to one of the 6652–A1 RJ-45 ports and the other end to your PC, or LAN if you are setting up an Intranet.*
4. *Connect one end of the RJ-11 cable to the 6652–A1 WAN port and the other end to a VDSL wall outlet.*

Default Values

The device is pre-configured with the following parameters. You may re-load the default values using either the reset switch (refer to section 4.3) or the web interface (refer to chapter 2 section 17 - Factory Reset).

User Name: **admin**

Password: **admin**

Operation Mode: **Bridge Mode**

Local port address: **192.168.1.1**

Subnet mask: **255.255.255.0**

UPnP: **Enabled**

Chapter 2 Connecting your device

This chapter provides basic instructions for connecting the device to a computer or LAN and to the Internet.

In addition to configuring the device, you need to configure the Internet properties of your computer(s). For more details, see the following sections in Appendix A:

Configuring Ethernet PCs section

This chapter assumes that you have already established a DSL service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

Connecting the Hardware

This section describes how to connect the device to the power outlet and your computer(s) or network.



WARNING

Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the device.

The diagram below illustrates the hardware connections. The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

1. *Connect the DSL cable and optional telephone line*

Connect one end of the provided phone cable to the port labeled DSL on the rear panel of the device. Connect the other end to DSL outlet.

5. *Connect the Ethernet cable*

Connect up to four single Ethernet computers or to a HUB/Switch directly to the device via Ethernet cable(s).

Note that the cables do not need to be crossover cables, the switch provides MDI and MDIX auto-detection.

6. *Attach the power connector*

Connect the AC power adapter to the Power connector on the back of the device and plug the adapter into a wall outlet or power strip. Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

7. *Configure your Ethernet PCs*

You must also configure the Internet properties on your Ethernet PCs. See Configuring Ethernet PCs section.

Next step

After setting up and configuring the device and PCs, you can log on to the device by following the instructions in "Getting Started with the Web pages" on chapter 4. The chapter includes a section called Testing your Setup, which enables you to verify that the device is working properly.

Web User Interface

You can access and configure the device settings through a web browser on a PC connected to the device. The DSL Modem includes a series of Web pages which provide an interface to the software installed on the device.

Accessing the Web pages

To access the web pages, you need the following:

A laptop or PC connected to the LAN or WLAN port on the device.

A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox from any of the LAN computers, launch your web browser, type the URL, <http://192.168.2.1> in the web address (or location) box, and press [Enter]. The default IP address of the device is 192.168.2.1. Then enter the default username and password: admin/admin to access [the configuration web page, if you have not changed the username and password.](#)



The home page opens displaying the Internet Port Configuration page of device:

Operation Mode

Based Setup

Summary

Internet Port

Local Port

Advanced Setup

Access Control List

Dynamic DNS

Firewall

Static Routes

Dynamic Routes

UPnP

Virtual Server

IP QoS

Port-Based VLAN

Management

Remote Management

System Reset

Firmware Upgrade

Network Status

Save Configuration

Diagnostics

Time

Based Setup > Summary

ZHONE Firmware:	01.00.04
Product Name:	6652-A2-010004ZHA
Serial Number:	N/A
Software Version:	6652-A2-010004ZHA.107r45
MAC address:	00:01:38:A1:E9:D8

The Web interface provides for the basic configuration of the system:

- Device Configuration
- Internet Port
- Local Port.

By default, the page of Internet Port is displayed after the login.



Advanced Setup

The advanced setup section provides information about the current configuration of various system features with options to change the configuration:

- Dynamic DNS
- Firewall
- Static Routes
- Dynamic Routes
- UPnP
- Virtual Server
- IP
- QoS
- Port-Based VLAN.



Management

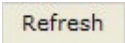




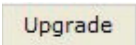
The management section provides administration utilities

- Remote Management
- System Reset
- Firmware Upgrade
- Network Status
- Save Configuration
- Diagnostic
- Time Zone.



Commonly used buttons

The following buttons are used throughout the web pages:

Button	Function
	You could click this button to refresh the information on this current page again so that you could get the real time information.
	This button appears on every configuration page. Click on this button if at any time you decide that you do not want to change the existing settings.
	check button – these appear on many configuration pages. You will be asked to check if you want this feature be selected.
	This button appears on every configuration page. Click on this button once you are through with the changes and decide to save the made changes.
	You may need to browse to find a file which needs to be uploaded for new configuration.
	This button allows you to upgrade to the new configuration file attached using the Browse button.

The following terms are used throughout this guide in association with these buttons:

Click – point the mouse arrow over the button, menu entry or link on the screen and click the left mouse button. This performs an action, such as displaying a new page or performing the action specific to the button on which left mouse button is clicked.

Select – usually is used when describing which radio button to select from a list, or which entry to select from a drop-down list. Point the mouse arrow over the entry and left-click to select it. This does not perform an action – you will also be required to click on a button, menu entry or link in order to proceed.

Help information

To view the help, click the desired menu or submenu. The related help information appears in a separate page.

Testing your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the device's DSL connection to access the Internet.

To test the connection, turn on the device, wait for 30 seconds and then verify that the LEDs are illuminated as follows:

LED	Behavior
Power (PWR)	Red Blinking when you open the modem, it will become green after 5s. Then the device is powered on If Red On means boot fail
PPP	Solid green indicates that the PPPoE WAN function is operational and Solid red indicate the PPPoE not established or the WAN port doesn't run PPPoE mode.
LAN	Solid green to indicate that the device can communicate with your LAN.
DSL	Flashing on/off while trying to SYNC UP with ISP CO site. Solid green to indicate that the device has successfully established a connection with your ISP.

Table 1. LED Indicators

If the LEDs illuminate as expected, test your Internet connection from a LAN computer. To do this, open your web browser, and type the URL of any external website (such as <http://www.zhone.com>).

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. If the LEDs still do not illuminate as expected or the web page is not displayed, see Troubleshooting section or contact your ISP for assistance.

Default device settings

In addition to handling the DSL connection to your ISP, the DSL Modem can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review these settings to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.



WARNING

We strongly recommend that you contact your ISP prior to changing the default configuration.

Option	Default Setting	Explanation/Instructions
User/Password	admin/admin	User name and password to access the device
LAN Port IP Address	Assigned static IP address: 192.168.1.1 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See Local Network section.

Option	Default Setting	Explanation/Instructions
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.10 through 192.168.1.250 (Please be noted that the default DHCP IP address pool may be different in each firmware version.)	The device maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in DHCP Server section.

Basic Setup

The Basic Setup web page menu includes the following submenus:

- Operation Mode
- Internet Port
- Local Port

Operation Mode

The Device Configuration Page of the device allows you to configure the device to work as router or bridge. A bridge is like an intelligent repeater. It regenerates what it receives like a repeater, but only sends to MAC addresses connected to one of the bridges' output ports. A bridge learns MAC addresses when it receives a frame. If the destination address is not in the bridging table or is a broadcast address, it forwards the frame out all of the ports except the one where it was received.

Bridges handle network segments very well and can be daisy chained to segment a network, however there cannot be any looped segments or the frames will loop forever. Bridges do not do any IP addressing. Routers can handle IP addressing and have loops. Bridges can only forward to the next network fragment. Routers learn a logical multiple hop route to the destination.

Bridges are good for joining networks, given you follow the no-looping restriction. Routers allow looping, build a picture of the whole picture of the networks, but require more configuration during installation.

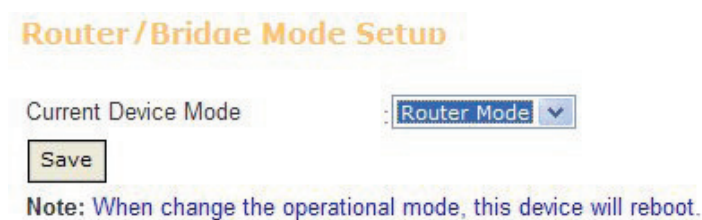


Figure 6: Operation Mode

To configure Device Mode:

- Select Route Mode or Bridge Mode from the list.

Internet Port

You can configure your internet connection from this page. This page displays the details of existing internet connection, if any. This page contains all of options that could establish a connection to your Telco or ISP.

NOTE: Before configuring the device, you should ask for and get the following information from your ISP:

- Connection Protocol: PPPoE (dynamic IP assignment), DHCP (dynamic IP assignment) or Static IP address from ISP.
- If the connection protocol is "fixed IP address", need more information about subnet mask, default gateway, and DNS server.
- NAT: Disabled or Enabled
- Default Route: Disabled or Enabled
- IGMP: Disabled or Enabled
- PPP User Name and Password (also known as Broadband User Name and Password)

PPPoE Connection

Point to point protocol over Ethernet networks (PPPoE) encapsulates PPP frames inside of Ethernet frames. This encapsulation allows individual users to connect to ADSL modems as are commonly used in Metro networks.

The screenshot shows a web interface for configuring Multi-PPPoE. At the top, there is a breadcrumb trail: "Internet Port > Multi-PPPoE Configuration". Below this is a blue header bar with the text "Multi-PPPoE Configuration". The main configuration area contains several fields and checkboxes. The "Protocol" dropdown is set to "Multi-PPPoE(Dynamic IP Configuration)". The "Interface Name" field is empty. The "User Name" and "Password" fields are empty, with a "Confirm Password" field below them. The "Service Name" and "AC Name" fields are empty. The "Authentication Type" dropdown is set to "PAP". The "Packet Size (MTU)" dropdown is set to "1492". The "Disconnect after Idle" dropdown is set to "0" minutes. The "VLAN ID" field is set to "0" with a range of "(0 ~ 4094)". There are three checkboxes: "NAT Enable" (checked), "Default Route" (checked), and "IGMP Enable" (unchecked). At the bottom, there are "Add" and "Undo" buttons.

Figure 7: Internet Port – PPPoE (Dynamic IP assignment)

To configure the PPPoE settings:

1. From the **Protocol** drop down select **Multiple-PPPoE (Dynamic IP Configuration)**.
8. In **Interface Name** enter a name
9. Enter the username and password provided from your Telco or ISP and enter the password again in the **Confirm Password** field again to double check the password.
10. In **Service Name** and **AC Name** enter name.
11. In the **Authentication Type** dropdown select PAP or CHAP
Password Authentication Protocol (PAP), and the Challenge Handshake Authentication Protocol (CHAP) are two authentication types for PPP networks. Please contact your service provider for the proper setting.
12. In the **Packet Size (MTU)** drop down select a packet size.
13. In the **Disconnect after Idle** dropdown select the number of minutes.
If there is no traffic for the number of minutes selected, the device will disconnect.
14. In the **VLAN ID** text box enter the VLAN ID if the traffic is tagged with VLAN ID.
15. Click **Enable NAT**.

16. Click **Default Route**
17. Click **Enable IGMP** if needed
18. Click **Add** and then **Save** to save the configuration, otherwise click **New** to configure it again.

DHCP (Dynamic IP Configuration)

The Dynamic IP Configuration option allows you to “get an IP address automatically”.

Internet Port > DHCP Configuration

DHCP Configuration

Protocol: DHCP(Dynamic IP Configuration)

☐ VLAN ID (0 ~ 4094)

☐ Use Static DNS. (Primary DNS can't be empty)

Primary: . . .

Secondary: . . .

☐ NAT Enable

☐ IGMP Enable

Save Undo

Figure 8: Internet Port - DHCP (Dynamic IP Configuration)

To configure the DHCP (Dynamic IP Configuration) settings:

1. In the **Protocol** dropdown select **DHCP (Dynamic IP Configuration)**.
19. In **VLAN ID** enter the VLAN ID if the traffic is tagged with VLAN ID.
20. Click to use **Static DNS (Domain Name Server)** and then enter the IP addresses of Primary DNS and Secondary DNS.
Usually, the information of DNS sever will be given from your ISP.
21. Click **NAT** if needed.
22. Click **IGMP** if needed.
23. Click **Save** to save the configuration

Static IP Configuration

This web page allows you to set the fixed IP address in the Internet (WAN) port.

[Internet Port](#) > [Static IP Configuration](#)

Static IP Configuration

Protocol Static IP Configuration

☐ VLAN ID (0 ~ 4094)

IP Address . . .

Submask . . .

Gateway . . .

Primary DNS . . .

Secondary DNS . . .

☐ NAT Enable

☐ IGMP Enable

Save Undo

Figure 9: Internet Port – Static IP Configuration

To configure the Static IP settings:

1. In the Protocol dropdown select the Fixed IP Configuration.
24. In the VLAN ID text box enter the VLAN ID if the traffic is tagged with VLAN ID.
25. Enter the IP address, Submask, Gateway, Primary DNS address and Secondary DNS address.
26. Click NAT if needed.
27. Click IGMP if needed.
28. Click **Save** to save the configuration

Local Port

Configure the Local Network (LAN) connection.

The screenshot displays a configuration interface for a Local Port. It is divided into two main sections: 'Private Network' and 'DHCP Server'.
The 'Private Network' section contains two rows of IP address input fields. The first row is labeled 'IP Address' and has four fields with values 192, 168, 2, and 1. The second row is labeled 'Subnet Mask' and has four fields with values 255, 255, 255, and 0.
The 'DHCP Server' section contains several settings:
- A checkbox labeled 'DHCP Server Enable' which is checked.
- A 'Start IP Address' row with four fields containing 192, 168, 2, and 10.
- A 'Number of IP Address' row with a single field containing 240.
- A 'Lease Time' row with a dropdown menu showing '24' and the unit 'Hours'.
- A 'WINS Server' row with four empty fields.
At the bottom of the DHCP Server section, there are two buttons: 'save' and 'Undo'.

Figure 10: Local Port Configuration

To configure the Local Port settings:

1. In **IP Address** enter the device IP address 192.168.1.1 (Default).
29. In **Subnet Mask** enter the Subnet Mask :
The subnet mask determines the number of computers are allowed in this network. Usually a class (255.255.255.0) is satisfactory for a local network.
30. Click **DHCP Server Enable**.
This option will assign IP addresses to the client.
31. In **Start IP Address** enter the first of the IP addresses for DHCP client users.
The default value is 192.168.1.10. Please make sure there is no fixed IP address within the range of DHCP IP pool, otherwise the DHCP client may not get the IP address correctly.
32. In **Number of IP Address** enter the number of IP addresses (users) allowed to use the DHCP service.
33. In the **Lease Time** dropdown select the lease time.
A DHCP client gets the IP address with a lease time. When the lease time is expired, the client must connect to the DHCP server to request the dynamic IP address again.
34. In **WINS Server** enter the IP address of WINS (Windows Internet Naming Service).
The WINS provides a distributed database for registering and querying dynamic computer name-to-IP address in a routed network environment. It means WINS provides easy configuration and administration of Windows-based TCP/IP networks. If you do not use WINS server, leave it as blank.
35. Click **Save** to save the configuration

Advanced Setup

The Configuration web page menu comprises:

- Access Control List
- Dynamic DNS
- Firewall
- Static Routes
- Dynamic Routes
- UPnP
- Virtual Server
- IP QoS
- Port-Based VLAN

Access Control List

Using the access control list you can filter incoming or outgoing packets based on IP, Port or both. You can select from a provided list of applications or customize the application list. Blocking may also be scheduled.

Advanced Setup > Access Control List

	Start IP Address	End IP Address
Source	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Destination	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Destination Port Type: ▼

Select the direction to filter packets: ☐ Inbound Traffic ☐ Outbound Traffic ☐ Both

Schedule:

☒ Always

☐ By schedule

☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

☐ Time Period ▼ to ▼

Rule Action:

☒ Accept ☐ Drop

Figure 11: Local Port Configuration

To configure the Access Control List page:

1. In the **Source** and **Destination** fields provide the IP range in **Start** and **End IP Address**
If there is only a single IP address, enter it in start IP address
36. In the **Destination Port Type drop** down select the *Destination Port* or *Application* you need to accept or drop.

The destination port type “Any” provides that all the ports of the IP address or the IP address range will be accepted or dropped based on the configuration of the **Rule Action**.

The destination port type “Port” requires that you also define protocol, port number or port number range.

The destination port type “application” requires that you also define which application list in the menu or you can create your own application and the application from the IP or IP range will be accepted or dropped based on the configuration of the **Rule Action**.
37. From the **Select the direction to filter packets** radio buttons, select which direction you want to process the rule, *Inbound*, *Outbound* or *both*.
38. In the **Schedule** options set the time frame to process the rule.
You can select specific times or set always if you want the rule always to be active.
39. In **Rule Action** set whether the action should be *Accept* or *Drop* when the condition is met.

Dynamic DNS

The Dynamic Domain Name System (DDNS) feature allows you to assign a fixed host and domain name to a dynamic Internet IP address. This option is useful when hosting your own website, FTP server and other server applications behind the device. Before using this feature, you need to sign up for DDNS service from the DDNS service provider like dyndns.org (refer to www.dyndns.org).

The screenshot shows the 'Advanced Setup > Dynamic DNS' configuration page. It includes a checkbox for 'Enable Dynamic DNS'. Below this, there's a 'DDNS account' section with two options: 'choose from list' (which shows a dropdown menu with 'ath.cx' selected) and 'enter your account name' (with a text input field). Further down are fields for 'user name' and 'Password'. There's also a 'Wildcard Enable' checkbox and a 'Mail Exchanger' field with a 'Backup MX' checkbox. At the bottom of the configuration section are 'Save' and 'Undo' buttons. Below the configuration section is an 'Update Status' section with 'Update' and 'Refresh' buttons.

Figure 12: Dynamic DNS Configuration

To configure the Dynamic DNS (DDNS) page:

1. In **Enable Dynamic DNS** click to enter a check to enable the Dynamic DNS feature
2. Enter account and configuration information:
 - a. In **DDNS account** enter your registered account name (host name) and select the DDNS service provider from the pull down list.
 - b. Enter your account name (full registered host name) if your DDNS service provider is not supported in the above pull down list.
 - c. Enter your username and password for login which you register the account name in the DDNS service provider field.
 - d. Click to enter a check in **Wildcard** to have an unregistered hostname followed by the registered hostname and domain name.
 - e. In the **Mail Exchanger** text field enter a mail server to redirect emails sent to your DDNS name to the mail server specified in the **Mail Exchanger** field.
 - f. Click to enter a check in **Backup MX** to back up the mail exchanger's address while you login the DDNS service provider.
3. Click **Save** to save the configuration.
4. Click **Update** to update the DDNS service or click **Refresh** to refresh display.

Firewall

The firewall feature protects the device.

Advanced Setup > Firewall

Firewall Configuration

☐ Block Request From Wan Port

☐ Block Ping From Wan Port

☐ Block PPTP, L2TP, IPSec Request

☐ Use this DMZ Host . . .

ALG Configuration

☐ Enable SIP ALG

☐ Enable IRC ALG

☐ Enable TFTP ALG

☐ Enable H.323 ALG

☐ Enable SNMP ALG

Figure 13: Firewall Configuration

Global Setting

Block Request From Wan Port

Block Ping From Wan Port

Block PPTP, L2TP, IPSec Request

DMZ host

A demilitarized zone (DMZ) is a computer on your network which can be accessed from the Internet regardless of NAT, port forwarding and IP filter settings. A DMZ is often used to host Web servers, FTP servers etc that need to be accessible from the Internet.

Enable SIP ALG

Enable IRC ALG

Enable TFTP ALG

Enable H.323 ALG

Enable SNMP ALG

Static Routes

The Static Routes feature allows you to add the routing rules manually.

Advanced Setup > Static Routes

Destination Network / Host . . .

Subnet Mask . . .

Gateway . . .

Metric

#	Destination	Submask	Gateway	Metric

Figure 14: Static Routes Configuration

To get the current routing table click *Routing Table* at the bottom of the screen.

To manually add routes:

1. In *Destination Network/Host* enter the IP address of destination host/network.
2. In *Subnet Mask* enter the subnet mask related the destination host/network gateway to which packets to those IP addresses will be forwarded.
3. In *Gateway* enter the IP address of the gateway
4. In *Metric* enter the number
5. To add the configured route click *Add* to add this routing rule
6. The added routing rule will be shown in the table. Click *Delete All* to remove all entries or click *Delete* to remove the specified entry.

Dynamic Routes

RIP, RIPv2 Authentication, Split-Horizon and Poison-Reverse dynamic routes can be set.

Advanced Setup > Dynamic Routes

RIP Setup

☐ Enable RIP

RIP Version

RIP Operation

Announcement Interval seconds

Routes Expire Time seconds

Garbage Collection Time seconds

☐ Enable RIPv2 Authentication

Mode

Password

☒ Enable Split-Horizon

☐ Enable Poison-Reverse

Figure 15: Dynamic Routes Configuration

UPnP

Universal Plug and Play functionality (UPnP) allows the gateway to configure itself and communicate automatically with other devices on the network.

NOTE: This function may not work properly if not all devices in your LAN do not support UPnP. If you do have devices which do not support UPnP, please turn off the UPnP feature.

Advanced Setup > UPnP

☒ Enable UPnP

Figure 16: UPnP Configuration

To set the Universal Plug and Play functionality:

1. In the *Enable UPnP* check box enter a check.
2. Click **Save** to save the configuration

Virtual Server

The Virtual server feature enables you to run a server on your local network that can be accessed from the Internet. The device provides port mapping to the local host for incoming packets. You need to set up port forwarding rule to tell the device on which computer the server is residing. When port forwarding is enabled, your router (the device) routes all the inbound traffic on a particular port to the chosen computer on your network.

Advanced Setup > Virtual Server

Application

Server IP Address . . .

#	Application	Server IP Address
1.	FTP (TCP 21)	192.168.2.254

Figure 17: Virtual Server Configuration

To define a virtual server:

1. In the **Application** dropdown select the application (port).
If it is not listed in default, click *Define Application* to add your own application as below figure.
2. In **Server IP Address** enter the IP address of Server IP Address in your local network.
3. Click **Add** to add this rule
The added port forwarding rule will be shown in the table. Click *Delete All* to remove all added entries or click *Delete* to remove the specified entry.

To define the application:

Advanced Setup > Virtul Server > Define Application

Application

Protocol TCP ▾

Port Range ☒ Single ☐ Range

Port Number to

Add Undo

#	Application	Protocol	Ports

Delete

Figure 18: Virtual Server Configuration – Define Application

1. In the **Application** text field enter the name of the application
2. In the **Protocol** dropdown select the Protocol (TCP, UDP, or ICMP) used by the application
3. In the **Port Range** check boxes, check if you want to forward the **Single** port or a **Range** of ports
4. If sending to a range of ports, enter the **Port Number** (range) from start to end
5. Click **Add** to add this application into the selection list.

IP QoS

You can configure four different priority queues (High, Middle, Low and Default) and provide bandwidths to them separately. The rules determine the packets sent to each queue. Proper configuring of the queues helps provide better bandwidth efficiency and can be used so that important packets like voice have greater priority and user do not experience drop outs in their calls. You can prioritize voice, email, FTP and so on to provide better quality of service for users.

QoS Scheduler

☒ **UpStream QoS Enable**

Bandwidth: Auto Kpbs

Priority Percentage: High % Medium % Low % Default %

☒ **DownStream QoS Enable**

Bandwidth: Auto Kpbs

Priority Percentage: High % Medium % Low % Default %

Figure 19: IP QoS – QoS Scheduler

QoS Scheduler

Enable upstream and/or downstream QoS and configure the four different priority queues (High, Middle, Low and Default) and provide bandwidths to them separately.

To configure upstream (packets from LAN to Internet) priority queues:

1. Check **Upstream QoS Enable**.
2. In the **Bandwidth** dropdown select **Auto**.
The device will get the sync up upstream bandwidth and determine the bandwidth used for QoS.
3. Select the **Manual** in the **Bandwidth** and then enter the bandwidth in Kbps used for QoS.
4. Enter the **Priority Percentage** for **High**, **Medium**, and **Low** queues.
The rest of percentage will be assigned to **Default** queue automatically.
5. Click **Save** to save the configuration

To configure downstream (packets from LAN to Internet) priority queues:

1. Check **Downstream QoS Enable**.
2. In the **Bandwidth** dropdown select **Auto**.
The device will get the sync up upstream bandwidth and determine the bandwidth used for QoS.
3. Select the **Manual** in the **Bandwidth** and then enter the bandwidth in Kbps used for QoS.
4. Enter the **Priority Percentage** for **High**, **Medium**, and **Low** queues.
The rest of percentage will be assigned to **Default** queue automatically.
5. Click **Save** to save the configuration

QoS Policy

Configure the rules to check the packet and put it into the right priority queue.

QoS Policy

Protocol

TCP

Source IP Address

Source Port

Destination IP Address

Destination Port

Priority

Medium

Add

Undo

Sel.	#	Protocol	Source IP	Source Port	Destination IP	Destination Port	Priority
<input checked="" type="radio"/>	1.	TCP	ANY	ANY	192.168.2.100	20	Medium

Delete

Figure 20: IP QoS – QoS Policy

1. From the **Protocol** dropdown enter the packet type (TCP or UDP)
2. In **Source IP Address** and **Source Port** enter the source IP address and/or port number if any.
3. In **Destination IP Address** and **Destination Port** enter the Destination IP Address and/or Port Number if any.
4. In the **Priority** drop down select which priority queue this packet should use.
5. Click **Add** to create this rule.

In the above example any packet with destination IP address, 192.168.2.100 and port number, 20 will be put into medium queue.

To delete a rule select the specified entry in the QoS policy table and click *Delete* to remove the rule.

Port-Based VLAN

By configuring Port-Based VLAN you can get up to four separate Ethernet environments. Each VLAN can be associated with the VLAN ID in the Internet (WAN) group to access a Wide Area Network. The default is for LAN1, 2, 3, and LAN4 to be grouped together as a single Ethernet environment.

In the following example all packets which do not match (in other words all of the packets since they do not have anything to match) will be sent to Routing Group which is the default group.

Advanced Setup > Port-Based VLAN

	WAN VLAN ID	LAN1	LAN2	LAN3	LAN4
Routing Group		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Bridge Group 1	<input type="text" value="0"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bridge Group 2	<input type="text" value="0"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bridge Group 3	<input type="text" value="0"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 21: Port-Based VLAN Configuration

To configure a WAN

1. In the text box for **Bridge Group 1, 2 or 3** enter the value of **WAN VLAN ID**.
2. Select the LAN ports from LAN1 to LAN4 for each Bridge Group.
3. Click **Save** to save the configuration.

Management

Several management features are provided:

- Remote Management
- System Reset
- Firmware Upgrade
- Network Status
- Save Configuration
- Diagnostic
- Time

Remote Management

Check and configure the device from a remote site by setting up credentials.

The image shows two screenshots of a web interface. The top screenshot is titled "Remote Management Setting" and contains three input fields: "User Name" with the value "admin", "Password" with masked characters "•••••", and "Confirm Password" which is empty. Below these fields are two buttons: "Change Login Password" and "Undo". The bottom screenshot is titled "Management via WAN & Restrict LAN Access MAC". It features a checked checkbox for "Enable Management Via WAN Port Web Port" with a text box containing "80". Below this is an unchecked checkbox for "Restrict Management from LAN (default is none)". Underneath are two rows of MAC address input fields, labeled "MAC Address 1" and "MAC Address 2", each consisting of six boxes separated by hyphens. At the bottom of this section are "Save" and "Undo" buttons.

Figure 22: Management Configuration – Remote Management

Global Setting

1. *Enter user information*

The default username/password is admin/admin.

To create new credentials you must be logged in as admin. To create a new user enter the new username, password in the *Password* and *Confirm Password* fields and then click *Change Login Password* to change it.

2. *To enable management by Web browser check **Enable Management Via WAN Port** check box and enter 80 in the **Web Port** text box.*

3. To restrict Management from the LAN check the **Restrict Management from LAN (default is none)** checkbox

The default for Restricting Management from the LAN disabled. Enter the *MAC addresses* from the LAN that you allow to access the device if this feature is enabled.

4. Click **Save** to save the configuration

System Reset

Reboot the device with current settings or factory default settings.

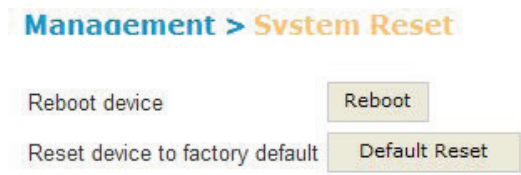


Figure 23: Management Configuration – System Reset

To reboot with current or factory settings:

- Click *Reboot* to reboot the device with current settings
- Click *Default Reset* to reboot the device with factory default settings

Firmware Upgrade

Upgrade the firmware of the device to get current features and improvements.



Figure 24: Management Configuration – Firmware Upgrade

To upgrade the firmware

1. Click *Browse* to specify the location of firmware
2. Click *Upgrade* to start the upgrade procedure.

The device will reboot automatically when the firmware is loaded completely.

Network Status

Display network status and information about LAN, WAN protocol, and VDSL.

LAN	
IP Address	: 192.168.2.1
Subnet Mask	: 255.255.255.0
MAC address	: 00:00:00:04:05:02

WAN (PPPoE)	
Connection Status	: Down
Interface Name	: dfasdf
IP Address	:
Subnet Mask	:
Gateway	:
Primary DNS	:
Secondary DNS	:

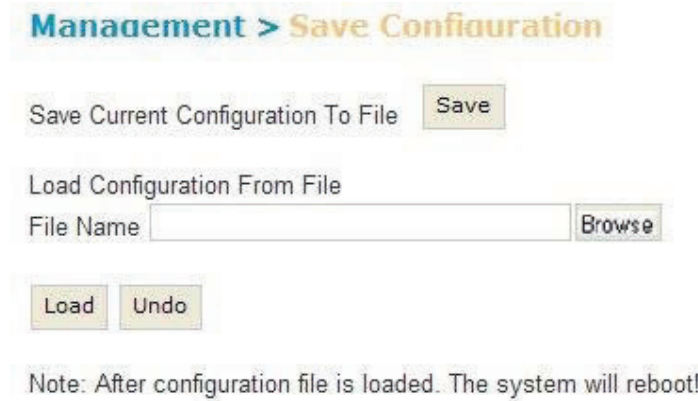
VDSL	
Connection status	: Link down
Firmware version	: 1.0.7r6IK105012 Time May 3 2007, 17:57:07

Refresh

Figure 25: Management Configuration – Network Status

Save Configuration

Save the current configuration into file in your PC or load the configuration from PC.



Management > Save Configuration

Save Current Configuration To File

Load Configuration From File

File Name

Note: After configuration file is loaded. The system will reboot!

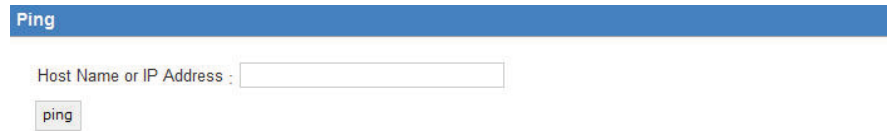
Figure 26: Management Configuration – Save Configuration

To save the current configuration click **Save** and follow the system instructions to save configuration profile into file

To load the configuration profile from a file, click **Browse** to specify the location of file and click **Load** to load the configuration profile into the device. The device will reboot automatically when the configuration is loaded.

Diagnostic

Ping a remote IP or domain name to test whether the Internet connection is working.



The screenshot shows a web interface for a 'Ping' tool. It has a blue header bar with the word 'Ping' in white. Below the header, there is a text input field labeled 'Host Name or IP Address :'. Underneath the input field is a small button labeled 'ping'.

Figure 27: Management Configuration – Diagnostic

To ping a remote device

1. In the Host Name or IP Address field enter the IP address or Host name (domain name)
2. Click ping to start the diagnostic process.

Time

Set the time zone and get the real time clock from the Internet.



The screenshot shows a web interface for 'Time Zone Configuration'. At the top, there is a breadcrumb trail 'Management > Time'. Below this, there is a 'Time Zone' dropdown menu showing '(GMT-08:00) Pacific Time (USA/Canada); Tijuana'. Below the dropdown is a checkbox labeled 'Use Daylight Saving Time'. Further down, there are two text input fields: 'Primary NTP Server' with the value 'tick.stdtime.gov.tw' and 'Secondary NTP Server'. Below these is an 'Update Interval' field with the value '1440' and the unit 'minutes'. At the bottom of the configuration section are two buttons: 'Save' and 'Undo'. Below the configuration section, there is a 'Current Time' display showing 'Fri Dec 31 17:03:53 1999'. At the very bottom are two buttons: 'Update' and 'Refresh'.

Figure 28: Management Configuration – Time Zone Configuration

Global Setting

- ▶ Select the your local *Time Zone* from the list
- ▶ Check to use the *Daylight Saving Time*
- ▶ Enter the NTP server domain name in the *Primary NTP Server* and *Secondary NTP Server* fields which provide the real time network clock
- ▶ Enter the value of *Update Interval* to sync up the clock with NTP server
- ▶ Click *Save* to save your settings
- ▶ Click *Update* to get the real time clock now

Appendix A - Configuring the Internet Settings

This appendix provides instructions for configuring the Internet settings on your computers to work with the device.

Configuring Ethernet PCs

Before you begin

By default, the device automatically assigns the required Internet settings to your PCs. You need to configure the PCs to accept this information when it is assigned.



Note

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the device to do so. See

Assigning static Internet information to your PCs section.

- If you have connected your LAN PCs via Ethernet to the device, follow the instructions that correspond to the operating system installed on your PC:
- Windows® XP PCs
- Windows 2000 PCs
- Windows Me PCs
- Windows\ 95, 98 PCs
- Windows NT 4.0 workstations
- If you want to allow Wireless PCs to access your device, follow the instructions in Configuring Wireless PCs below..

Windows® XP PCs

1. In the Windows task bar, click the **Start** button, and then click **Control Panel**.
2. Double-click the **Network Connections** icon.
3. In the **LAN** or **High-Speed Internet** window, right-click on the icon corresponding to your network interface card (NIC) and select **Properties**.
Often, this icon is labelled **Local Area Connection**. The *Local Area Connection* dialog box is displayed with a list of currently installed network items.
4. Ensure that the check box to the left of the item labelled **Internet Protocol TCP/IP** is checked and click **Properties**.
5. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the radio button labelled **Obtain an IP address automatically**. Also click the radio button labelled **Obtain DNS server address automatically**.

Click **OK** twice to confirm your changes, and then close the Control Panel.

Windows 2000 PCs

1. First, check for the IP protocol and, if necessary, install it:
2. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.

3. Double-click the **Network and Dial-up Connections** icon.
4. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**. The **Local Area Connection Properties** dialog box is displayed with a list of currently installed network components. If the list includes **Internet Protocol (TCP/IP)**, then the protocol has already been enabled. Skip to step 5.
 - a. If **Internet Protocol (TCP/IP)** does not display as an installed component, click **Install**.
 - b. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
 - c. Select **Internet Protocol (TCP/IP)** in the **Network Protocols** list, and then click **OK**. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
 - d. If prompted, click **OK** to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.
 - e. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
 - f. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
5. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
6. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the radio button labelled **Obtain an IP address automatically**. Also click the radio button labelled **Obtain DNS server address automatically**.
7. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

1. In the Windows task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes **Internet Protocol (TCP/IP)**, then the protocol has already been enabled. Skip to step 4.
 - a. If **Internet Protocol (TCP/IP)** does not display as an installed component, click **Add**.
 - b. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
 - c. Select **Microsoft** in the **Manufacturers** box.
 - d. Select **Internet Protocol (TCP/IP)** in the **Network Protocols** list, and then click **OK**. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
 - e. If prompted, click **OK** to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.
 - f. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
 - g. In **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.

4. In the **Network Properties** dialog box, select **TCP/IP**, and then click **Properties**.
5. In the **TCP/IP Settings** dialog box, click the radio button labelled **Server assigned IP address**. Also click the radio button labelled **Server assigned name server address**.
6. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

Windows 95, 98 PCs

1. First, check for the IP protocol and, if necessary, install it:
2. In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.
3. Double-click the Network icon. The Network dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 4.
 - a. If **TCP/IP** does not display as an installed component, click **Add**. The **Select Network Component Type** dialog box displays.
 - b. Select **Protocol**, and then click **Add**. The **Select Network Protocol** dialog box displays.
 - c. Click on **Microsoft** in the **Manufacturers** list box, and then click **TCP/IP** in the **Network Protocols** list box.
 - d. Click **OK** to return to the **Network** dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
 - e. Click **OK** to restart the PC and complete the TCP/IP installation. Next, configure the PCs to accept IP information assigned by the device.
4. Open the Control Panel window, and then click the **Network** icon.
5. Select the network component labelled **TCP/IP**, and then click **Properties**. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
6. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
7. Click the radio button labelled **Obtain an IP address automatically**.
8. Click the **DNS Configuration** tab, and then click the radio button labelled **Obtain an IP address automatically**.
9. Click **OK** twice to confirm and save your changes. You will be prompted to restart Windows.
10. Click **Yes**.

Windows NT 4.0 workstations

1. First, check for the IP protocol and, if necessary, install it:
2. In the Windows NT task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
3. In the Control Panel window, double click the **Network** icon.
4. In the **Network** dialog box, click the **Protocols** tab. The **Protocols** tab displays a list of currently installed network protocols. If the list includes **TCP/IP**, then the protocol has already been enabled. Skip to step 5.

- a. If TCP/IP does not display as an installed component, click **Add**.
 - b. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click **OK**. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
 - c. Click **Yes** to continue, and then click **OK** if prompted to restart your computer. Next, configure the PCs to accept IP information assigned by the device.
5. Open the Control Panel window, and then double-click the **Network** icon.
 6. In the **Network** dialog box, click the **Protocols** tab.
 7. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
 8. In the **Microsoft TCP/IP Properties** dialog box, click the radio button labelled **Obtain an IP address from a DHCP server**.
 9. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

Assigning static Internet information to your PCs

If you are a typical user, you will not need to assign static Internet information to your LAN PCs because your ISP automatically assigns this information for you.

In some cases however, you may want to assign Internet information to some or all of your PCs directly (often called “statically”), rather than allowing the device to assign it. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN (subnets are described in Appendix B).

Before you begin, you must have the following information available:

- The IP address and subnet mask of each PC
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the device. By default, the LAN port is assigned the IP address 192.168.2.1. (You can change this number or another number can be assigned by your ISP.)
- The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server and default gateway, click the radio buttons that enable you to enter the information manually.



Your PCs must have IP addresses that place them in the same subnet as the device's LAN port.

Appendix B - Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the device, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
LEDs	
<i>Power LED does not illuminate after product is turned on.</i>	Verify that you are using the power cable provided with the device and that it is securely connected to the device and a wall socket/power strip.
<i>Internet LED does not illuminate after phone cable is attached.</i>	Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the DSL port and your wall phone port. Allow about 30 seconds for the device to negotiate a connection with your ISP.
<i>LINK LAN LED does not illuminate after Ethernet cable is attached.</i>	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the device. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
Internet Access	
My PC cannot access the Internet	Run a health check on your device. Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 192.168.2.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: <ul style="list-style-type: none">• Check that the gateway IP address on the computer is your public IP address (see Current Status on page Error! Bookmark not defined. for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically.• Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
<i>My LAN PCs cannot display web pages on the Internet.</i>	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the device is correct, and then you can use the ping utility, discussed on page 34, to test connectivity with your ISP's DNS server.
Web pages	
<i>I forgot/lost my user ID or password.</i>	If you have not changed the password from the default, try using "admin" as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing three times the Reset Default button on the front panel of the device. Then, type the default User ID and password shown above. WARNING: Resetting the device removes any custom settings and returns all settings to their default values.
<i>I cannot access the web pages from my browser.</i>	Use the ping utility, discussed in the following section, to check whether the PC can communicate with the device's LAN IP address (by default 192.168.2.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the device.
<i>My changes to the web pages are not being retained.</i>	Be sure to use the <i>Confirm Changes</i> function after any changes.

Diagnosing Problem using IP Utilities

Ping

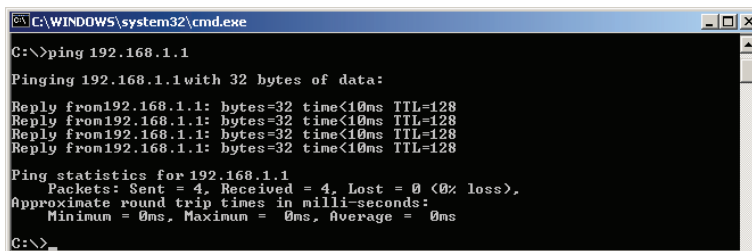
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

```
ping 192.168.2.1
```

Click OK. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window is displayed:



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

If the target computer cannot be located, you will receive the message Request timed out.

Using the ping command, you can test whether the path to the device is working (using the preconfigured default LAN IP address 192.168.2.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

Nslookup

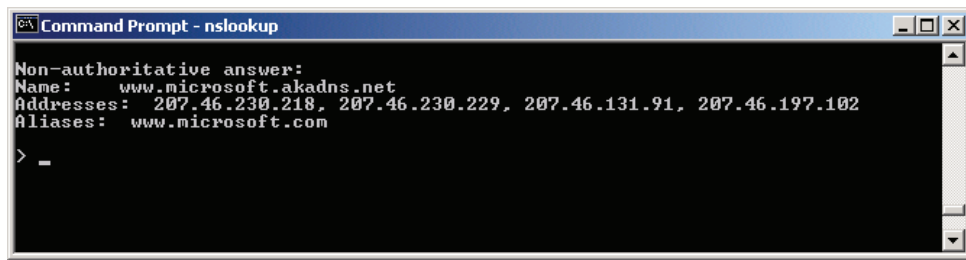
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, and then click Run. In the Open text box, type the following:

```
Nslookup
```

Click OK. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address that you are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown below:



```
Command Prompt - nslookup
Non-authoritative answer:
Name:      www.microsoft.akadns.net
Addresses: 207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases:   www.microsoft.com
> _
```

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type **exit** and press **[Enter]** at the command prompt.

Appendix C – Glossary

Term	Description
802.11	A family of specifications for wireless LANs developed by a working group of the IEEE. This wireless Ethernet protocol, often called Wi-Fi.
10BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See data rate, Ethernet.
100BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See data rate, Ethernet.
ADSL	Asymmetric Digital Subscriber Line The most commonly deployed “flavor” of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.
Analog	An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See digital.
ATM	Asynchronous Transfer Mode A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See data rate.
Authenticate	To verify a user's identity, such as by prompting for a password.
Binary	The “base two” system of numbers that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See bit, IP address, network mask.
Bit	Short for “binary digit,” a bit is a number that can have two values, 0 or 1. See binary.
Bps	bits per second

Bridging	Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing which can add more intelligence to data transfers by using network addresses instead. The device can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See routing.
Broadband	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
Broadcast	To send data to all computers on a network.
DHCP	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP relay	Dynamic Host Configuration Protocol relay A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. See DHCP.
DHCP server	Dynamic Host Configuration Protocol server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.
Digital	Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See analog.
DNS	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, www.yahoo.com is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See domain name.
Domain name	A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See DNS.
Download	To transfer data in the downstream direction, i.e., from the Internet to the user.

DSL	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
Encryption keys	See network keys
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, twisted pair.
FTP	File Transfer Protocol A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.
Gbps	Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
Host	A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See web browser, web site.
Hub	A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.
ICMP	Internet Control Message Protocol An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IEEE	The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.
Internet	The global collection of interconnected networks used for both private and business communications.
Intranet	A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP	See TCP/IP.

IP address	<p>Internet Protocol address</p> <p>The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See domain name, network mask.</p>
ISP	<p>Internet Service Provider</p> <p>A company that provides Internet access to its customers, usually for a fee.</p>
LAN	<p>Local Area Network.</p> <p>A network limited to a small geographic area, such as a home or small office.</p>
LED	<p>Light Emitting Diode</p> <p>An electronic light-emitting device. The indicator lights on the front of the device are LEDs.</p>
MAC address	<p>Media Access Control address</p> <p>The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; NN:NN:NN:NN:NN:NN.</p>
Mask	<p>See network mask.</p>
Mbps	<p>Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.</p>
NAT	<p>Network Address Translation</p> <p>A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.</p>
Network	<p>A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.</p>
Network keys	<p>(Also known as encryption keys.) 64-bit and 128-bit encryption keys used in WEP wireless security schemes. The keys encrypt data over the WLAN, and only wireless PCs configured with WEP keys that correspond to the keys configured on the device can send/receive encrypted data.</p>
Network mask	<p>A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See binary, IP address, subnet.</p>

NIC	<p>Network Interface Card</p> <p>An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See Ethernet, RJ-45.</p>
Packet	<p>Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).</p>
Ping	<p>Packet Internet (or Inter-Network) Groper</p> <p>A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.</p>
Port	<p>A physical access point to a device such as a computer or router, through which data flows into and out of the device.</p>
PPP	<p>Point-to-Point Protocol</p> <p>A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the device uses two forms of PPP called PPPoA and PPPoE. See PPPoA, PPPoE.</p>
PPPoA	<p>Point-to-Point Protocol over ATM</p> <p>One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.</p>
PPPoE	<p>Point-to-Point Protocol over Ethernet</p> <p>One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.</p>
Protocol	<p>A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.</p>
Remote	<p>In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.</p>
RIP	<p>Routing Information Protocol</p> <p>The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.</p>
RJ-11	<p>Registered Jack Standard-11</p> <p>The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.</p>
RJ-45	<p>Registered Jack Standard-45</p> <p>The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.</p>
Routing	<p>Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.</p>

SDNS	<p>Secondary Domain Name System (server)</p> <p>A DNS server that can be used if the primary DSN server is not available. See DNS.</p>
Subnet	<p>A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See network mask.</p>
Subnet mask	<p>A mask that defines a subnet. See network mask.</p>
TCP	<p>See TCP/IP.</p>
TCP/IP	<p>Transmission Control Protocol/Internet Protocol</p> <p>The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.</p>
Telnet	<p>An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.</p>
TFTP	<p>Trivial File Transfer Protocol</p> <p>A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.</p>
TKIP	<p>Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.</p>
Triggers	<p>Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them.</p> <p>Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.</p>
Twisted pair	<p>The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an</p>

even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See 10BASE-T, 100BASE-T, Ethernet.

Unnumbered interfaces	An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a router-id that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.2.1). The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.
Upstream	The direction of data transmission from the user to the Internet.
VC	Virtual Circuit A connection from your DSL router to your ISP.
VCI	Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See VC.
VDSL	Very High Speed Digital Subscriber Line It provides faster transmission rate and is capable of supporting high bandwidth applications like IPTV and bandwidth consumed applications.
VPI	Virtual Path Identifier Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See VC.
WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the device, WAN refers to the Internet.
Web browser	A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See HTTP, web site, WWW.
Web page	A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page. See hyperlink, web site.
Web site	A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See hyperlink, web page.

WEP	<p>Wired Equivalent Privacy (WEP) encrypts data over WLANs. Data is encrypted into blocks of either 64 bits length or 128 bits length. The encrypted data can only be sent and received by users with access to a private network key. Each PC on your wireless network must be manually configured with the same key as your device in order to allow wireless encrypted data transmissions. Eavesdroppers cannot access your network if they do not know your private key. WEP is considered to be a low security option.</p>
Wireless	<p>Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. See wireless LAN.</p>
Wireless LAN	<p>A wireless LAN (WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.</p>
WPA	<p>Wi-Fi Protected Access</p> <p>WPA is an initiative by the IEEE and Wi-Fi Alliance to address the security limitations of WEP. WPA provides a stronger data encryption method (called Temporal Key Integrity Protocol (TKIP)). It runs in a special, easy-to-set-up home mode called Pre-Shared Key (PSK) that allows you to manually enter a pass phrase on all the devices in your wireless network. WPA data encryption is based on a WPA master key. The master key is derived from the pass phrase and the network name (SSID) of the device.</p> <p>It provides improved data encryption and stronger user authentication. The mode of WPA supported on your device is called Pre-Shared Key (PSK), which allows you to manually enter a type of key called a pass phrase.</p>
WWW	<p>World Wide Web</p> <p>Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.</p>

Appendix D - Specification

A1. Hardware Specifications for 6652–A2

- LAN Interface
 - Four port 10/100BaseT Ethernet Switch (4 * RJ-45 connectors), IEEE 802.3u with MDI/MDIX auto-detection
 - Integrated 802.11b/g WLAN Access Point
 - WAN VDSL2 Line Interface
 - Comply with VDSL2 and support 8a/8b/8c/8d, 12a/12b, 17a and 30a
- Connection Loops: One (pair wire)
 - Connector: RJ-11
- OAM&P
 - Local: Web management
 - Remote: Web Management
- Environment
 - Operation Temperature: 0°C ~ 40°C
 - Operation Humidity: 5% ~ 95%
 - Storage Temperature: -20 ~ +85°C
 - Storage Humidity: 5%~95%
- Power
 - AC/DC Switching Input =100~240V 50/60Hz Output=12VDC 1.5Amp
 - Certificates
 - CE, CB

A2. Software Specifications

- VDSL
 - Support VDSL2 profiles, 8a/8b/8c/8d, 17a
 - Plug-and-play multi-mode (VDSL2, VDSL) operation
- Bridging
 - Transparent Bridging and spanning(IEEE 802.1D)
- Routing
 - IP routing and PPP supported
 - PAP and CHAP for user authentication in PPP connection
 - RFC2684 (RFC1483) Routed
 - NAT/PAT with extensive ALG support
 - IP QoS Supported
- Configuration and Network Management Features
 - DHCP client and server for IP management
 - UPnP Internet Gateway Device (IGD v1)
 - System Log capability
 - WEB for local or remote management
 - HTTP for firmware upgrade and configuration

Note: Hardware and software specifications are subjected to change without notice.