

VDSL2 Router



User's Manual

Table of Contents

1	Introduction.....	7
	Features	7
	Device Requirements	7
	Using this Document.....	8
	Notational conventions	8
	Typographical conventions.....	8
	Special messages.....	8
	Getting Support.....	8
2	Getting to know the device.....	9
	Computer / System requirements	9
	Package Contents	9
	For Annex-B VDSL2 Router	9
	For Annex-A VDSL2 Router	9
	Installation & Setup	10
	LED meanings & activations	12
	Back Panel Connectors	13
3	Computer configurations under different OS, to obtain IP address automatically.....	14
4	Utility CD execution	27
	Connecting the Hardware.....	27
	VDSL WAN Configuration (VDSL Line User)	28
	DSL WAN Configuration (ADSL Line User).....	37
5	Getting Started with the Web pages	47
	Accessing the Web pages.....	47
	Testing your Setup.....	49
	Default device settings.....	50
6	Overview	53
	Internet access settings	54
	About VDSL2 Router	54
7	Status	55
	Device Info	55
	IPv6	56
8	Local Network Configuration.....	57
	Changing the LAN IP address and subnet mask	57

	Adding the Secondary LAN IP address and subnet mask	59
	Change IP Pool Range and Subnet mask.....	60
9	PTM WAN	62
	Configuring PTM WAN IPoE Static IP connection	65
	Configuring PTM WAN IPoE DHCP Client connection	69
	Configuring PTM WAN PPPoE connection	70
	Configuring PTM WAN DS-Lite connection.....	72
	Configuring PTM WAN 6rd connection.....	73
10	ATM WAN	74
	Types of DSL WAN Internet Access	75
	Configuring your PPPoE DSL connection	76
	Configuring your PPPoA DSL connection	78
	Configuring your Bridged DSL connection.....	80
	Configuring your 1483 MER by DHCP	81
	Configuring your 1483 MER by Fixed IP	81
	ATM Settings.....	83
	DSL Settings	86
11	DHCP Settings	88
	DHCP Server Configuration	88
	DHCP Relay Configuration.....	90
	DHCP None Configuration	91
12	DHCPv6 Settings	92
	DHCP Server (Manual) Configuration.....	92
	DHCP Server (Auto) Configuration	95
	DHCP Relay Configuration.....	96
	DHCP None Configuration	97
13	DNS Configuration	98
	DHCP Server Configuration - Attain DNS Automatically	98
	DHCP Server Configuration - Set DNS Manually.....	99
14	Dynamic DNS Configuration	101
	Overview of Dynamic DNS.....	101
	Dynamic DNS Configuration – DynDNS.org	103
	Dynamic DNS Configuration – TZO.....	104
15	IP/Port Filtering.....	106
	IP/Port Filtering.....	106

16	MAC Filtering	108
	Configuring MAC filtering to Deny for outgoing access.....	108
17	Port Forwarding	110
	Port Forwarding for TCP with specified IP.....	112
	Port Forwarding for UDP with specified IP.....	114
18	URL Blocking	116
	Configuring URL Blocking of FQDN.....	116
	Configuring URL Blocking of Keyword.....	118
19	Domain Blocking	120
	Configuring Domain Blocking	120
20	DMZ	122
	Configuring DMZ.....	122
21	UPnP	124
	Configuring UPnP	125
	UPnP Control Point Software on Windows ME.....	126
	UPnP Control Point Software on Windows XP with Firewall	126
	SSDP requirements	127
22	RIP	130
23	ARP Table	132
	ARP Table	132
24	Bridging	133
	Bridging	133
25	Routing	134
	Static Route.....	134
26	SNMP	136
	SNMP	136
27	Remote Access	138
	Remote Access.....	138
28	Others	139
	Others.....	139
29	IPv6	140
	IPv6	140
	RADVD.....	140
	DHCPv6	141
	MLD Proxy	141
	MLD Snooping	142

	IPv6 Routing.....	143
	IP/Port Filtering.....	144
30	Diagnostic.....	145
	Ping	145
	ATM Loopback.....	146
	ADSL Tone Diagnostics	147
	ADSL Connection Diagnostics	148
31	Commit/Reboot	149
	Commit and Reboot.....	149
32	Backup/Restore.....	150
	Backup settings.....	150
	Restore settings	151
	Resetting to Defaults.....	151
33	System Log	153
	System Log	153
34	Password.....	155
	Setting your username and password	155
35	Firmware Update.....	157
	About firmware versions	157
	Manually updating firmware.....	157
36	ACL Configuration	161
	ACL Config.....	161
37	Time Zone	162
	SNTP Server and SNTP Client Configuration settings.....	162
38	TR-069	167
	TR-069 Configuration	167
39	Statistics	169
	Statistics - Interface.....	169
	Statistics - ADSL	170
A	Configuring your Computers	171
	Configuring Ethernet PCs.....	171
	Before you begin	171
	Windows® XP PCs.....	171
	Windows 2000 PCs	171
	Windows Me PCs	173
	Windows 95, 98 PCs	173
	Windows NT 4.0 workstations.....	174

	Assigning static Internet information to your PCs	175
B	IP Addresses, Network Masks, and Subnets	176
	IP Addresses	176
	Structure of an IP address	176
	Network classes	176
	Subnet masks	177
C	Troubleshooting.....	179
	Troubleshooting Suggestions.....	179
	Diagnosing Problem using IP Utilities	181
	ping	181
	nslookup	181
D	Glossary	183

1 Introduction

Congratulations on becoming the owner of the VDSL2 Router. You will now be able to access the Internet using your high-speed DSL connection.

This User Guide will show you how to connect your VDSL2 Router, and how to customize its configuration to get the most out of your new product.

Features

The list below contains the main features of the device and may be useful to users with knowledge of networking protocols. If you are not an experienced user, the chapters throughout this guide will provide you with enough information to get the most out of your device.

Features include:

- Internal DSL modem for high-speed Internet access
- 10/100Base-T Ethernet Router to provide Internet connectivity to all computers on your LAN
- Network address translation (NAT) functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Client
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring
- User-friendly configuration program accessed via a web browser
- User-friendly configuration program accessed via EasySetup program

Device Requirements

In order to use the VDSL2 Router, you must have the following:

- DSL service up and running on your telephone line
- Instructions from your ISP on what type of Internet access you will be using, 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
 - a. 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
 - b. EasySetup program: Graphical User Interface



Note

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

Using this Document

Notational conventions

- Acronyms are defined the first time they appear in the text and also in the glossary.
- For brevity, the VDSL2 Router is referred to as “the device”.
- The term *LAN* refers to a group of Ethernet-connected computers at one site.

Typographical conventions

- *Italic* text is used for items you select from menus and drop-down lists and the names of displayed web pages.
- **Bold** text is used for text strings that you type when prompted by the program, and to emphasize important points.

Special messages

This document uses the following icons to draw your attention to specific instructions or explanations.



Note

Provides clarifying or non-essential information on the current topic.



Definition

Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.



WARNING

Provides messages of high importance, including messages relating to personal safety or system integrity.

Getting Support

Supplied by:
Helpdesk Number:
Website:

2 Getting to know the device

Computer / System requirements

- 1. Pentium 200MHZ processor or above
- 2. Windows 98SE, Windows Me, Windows 2000, Windows XP, Windows Vista, Windows 7 and Windows 8
- 3. 64MB of RAM or above
- 4. 25MB free disk space

Package Contents

For Annex-B VDSL2 Router

- 1. VDSL2 Router
- 2. CD-ROM (Software & Manual)
- 3. Quick Installation Guide
- 4. 1 x Telephone Cable (RJ-11)
- 5. Ethernet Cable (RJ-45)
- 6. Power Adaptor
- 7. Annex-B Splitter (Optional, with an extra RJ-11 Telephone cable)

For Annex-A VDSL2 Router

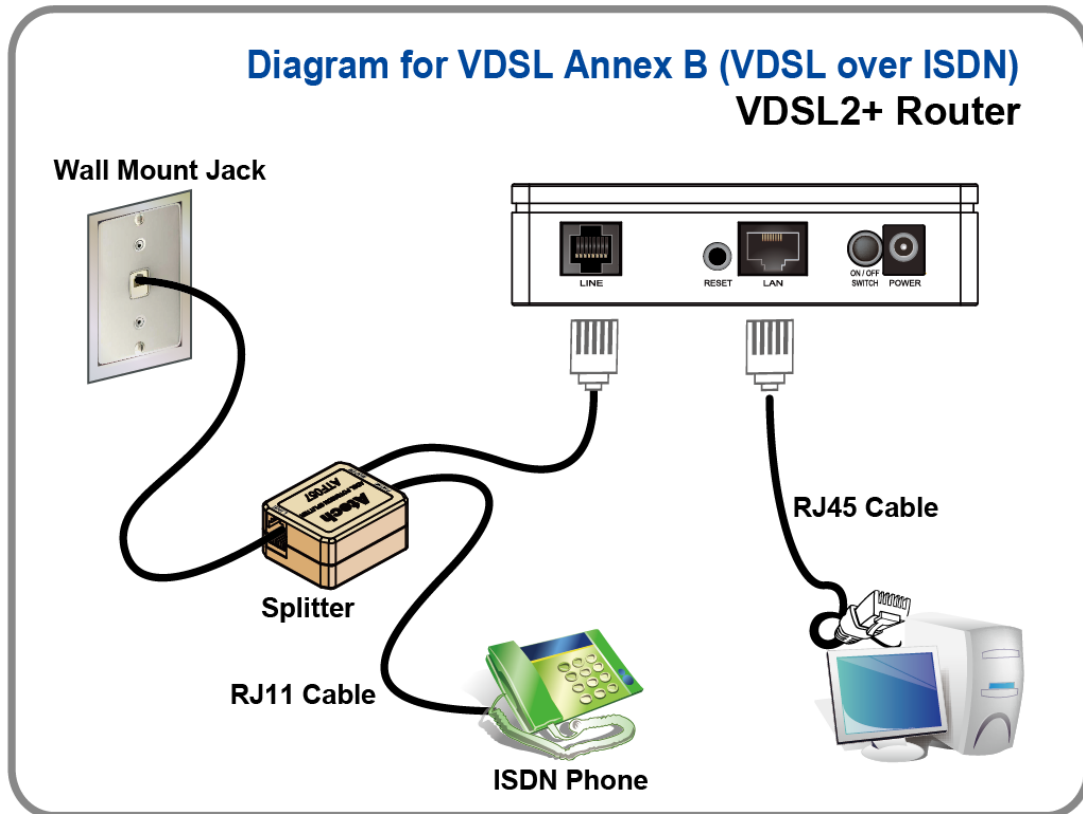
- 1. VDSL2 Router
- 2. CD-ROM (Software & Manual)
- 3. Quick Installation Guide
- 4. 1 x Telephone Cable (RJ-11)
- 5. Ethernet Cable (RJ-45)
- 6. Power Adaptor
- 7. Annex-A Splitter (Optional, with an extra RJ-11 Telephone cable)

Installation & Setup

Follow each STEP carefully and only go to the next step once you have complete the previous STEP.

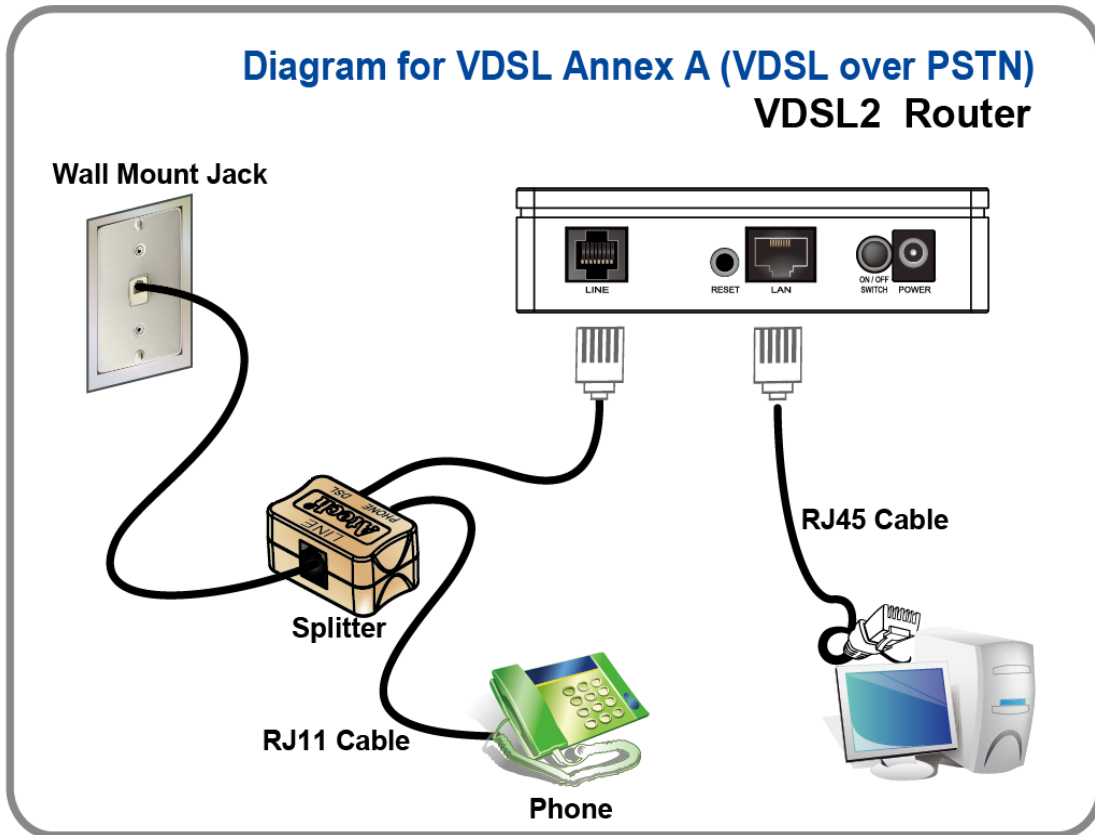
Connection of VDSL2 Router

If you have an ISDN telephone line connect the modem router as shown below:



1. Connect the supplied RJ45 Ethernet cable from your PC's Ethernet port to VDSL2 Router's LAN Port.
2. Connect the supplied RJ11 telephone cable from your home's telephone jack to the "LINE" port of the supplied splitter. Connect another RJ11 telephone cable to the "MODEM" port of the splitter and connect the other end of this cable to the LINE port of your VDSL2 Router. (If there is no option Splitter, please connect the supplied RJ11 telephone cable from your home's telephone jack to the "LINE" port of your VDSL2 Router.)
3. Connect a RJ11 telephone cable to the "PHONE" port of the splitter and connect the other end to your telephone.
4. Connect the power adapter to the power inlet "POWER" of the VDSL2 Router and turn the "ON/OFF SWITCH" switch of your VDSL2 Router on.





If you have a PSTN telephone line (normal analog line) connect the router as shown below:



1. Connect the supplied RJ45 Ethernet cable from your PC's Ethernet port to VDSL2 Router's LAN Port.
2. Connect the supplied RJ11 telephone cable from your home's telephone jack to the "LINE" port of the supplied splitter. Connect the other supplied RJ11 telephone cable to the "DSL" port of the splitter and connect the other end of this cable to the "LINE" port of your VDSL2 Router. (If there is no option Splitter, please connect the supplied RJ11 telephone cable from your home's telephone jack to the "LINE" port of your VDSL2 Router.)
3. Connect a RJ11 telephone cable to the "PHONE" port of the splitter and connect the other end to your telephone.
4. Connect the power adapter to the power inlet "POWER" of the VDSL2 Router and turn the "ON/OFF SWITCH" switch of your VDSL2 Router on.

LED meanings & activations

Your VDSL2 Router has indicator lights on the front side. Please see below for an explanation of the function of each indicator light.

 POWER	Power indicator	 INTERNET	Internet Active indicator
 1	Ethernet Active indicator	 DSL	ADSL Link indicator

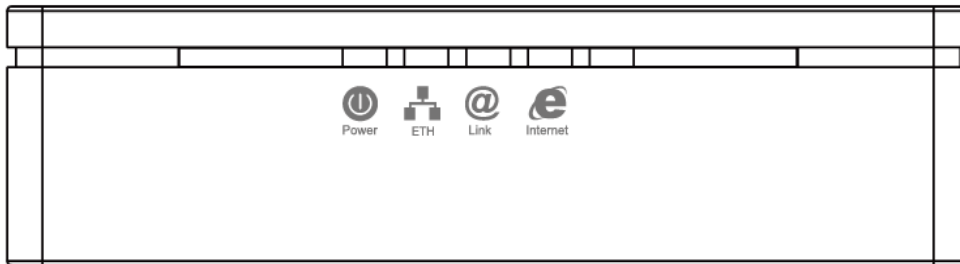






Table1. LED function

Label	Color	On	Flash	Off
 POWER	Red	N/A	N/A	N/A
	Green	Ready	Waiting for device ready	Power Off
 1	Green	Ethernet Connected	Transmit / Receive Data	Ethernet Disconnected
 DSL	Green	Connect to DSLAM	Disconnect to DSLAM	N/A
 INTERNET	Green	The device has a WAN IP address from ISP	Transmit / Receive Data	N/A
	Red	N/A	N/A	N/A

The icons appear on the products are for application indication only.

The trademark or intellectual property is belonging to their respective owners.

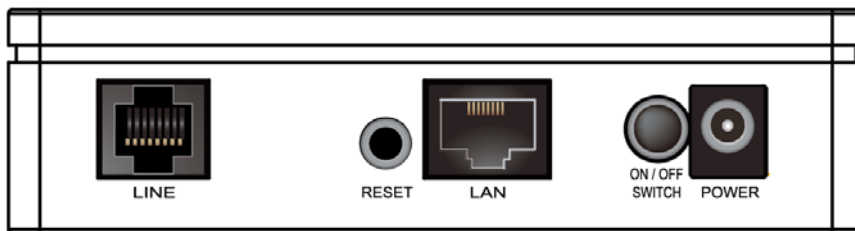
Back Panel Connectors

Table 2 shows the function of each connector and switch of the device.

Table 2. Function / Description of Connectors

Connector	Description
POWER	Connects to your VDSL2 Router 12Vdc power adaptor
SWITCH	Power Switch
LAN1~4	RJ-45 Jack (Ethernet Cable) connection to your PC, or HUB
LINE	Connects to your VDSL2 line – for VDSL2 Line input
RESET	Reset button. RESET the VDSL2 Router to its default settings. Press this button for at least 5 full seconds to start to reset it to its default settings.

Figure1. Rear View of the VDSL2 Router

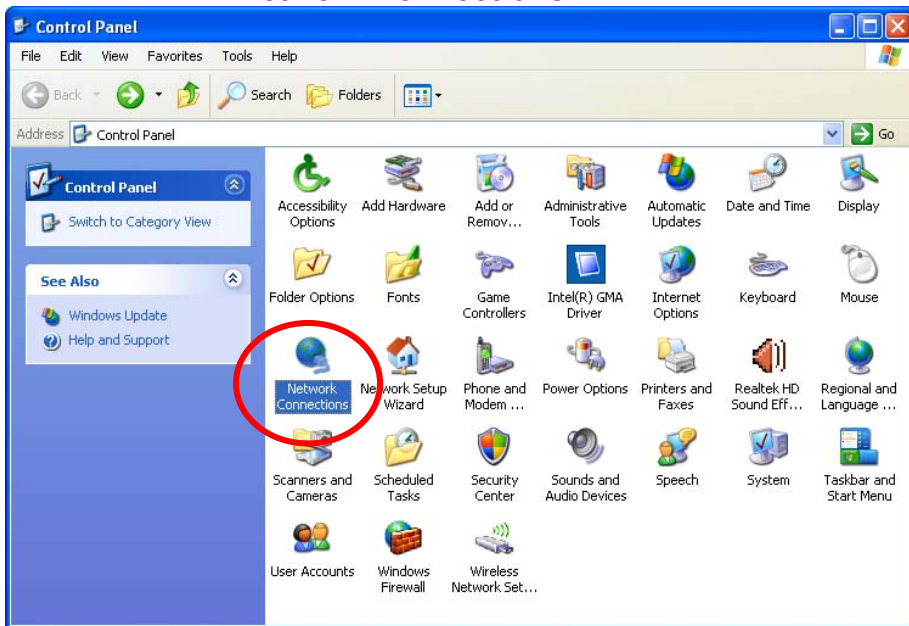


3 Computer configurations under different OS, to obtain IP address automatically

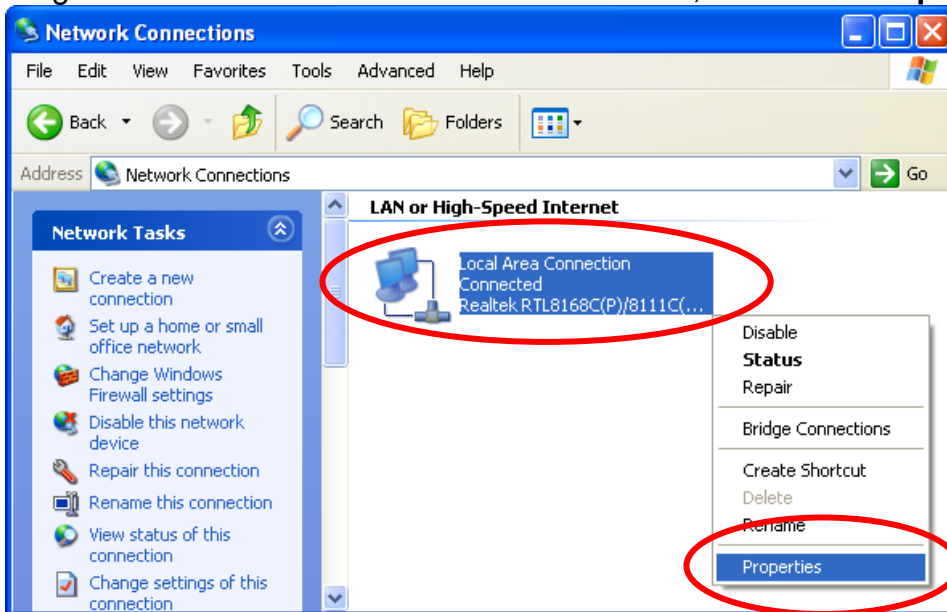
Before starting the VDSL2 Router configuration, please kindly configure the PC computer as below, to have automatic IP address / DNS Server.

For Windows 98SE / ME / 2000 / XP

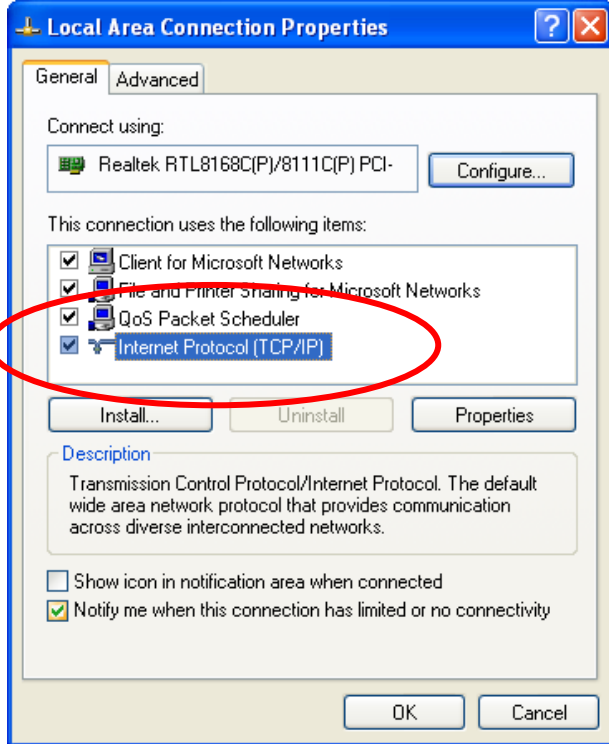
1. Click on **“Start”** -> **“Control Panel”** (in **Classic View**). In the Control Panel, double click on **“Network Connections”** to continue.



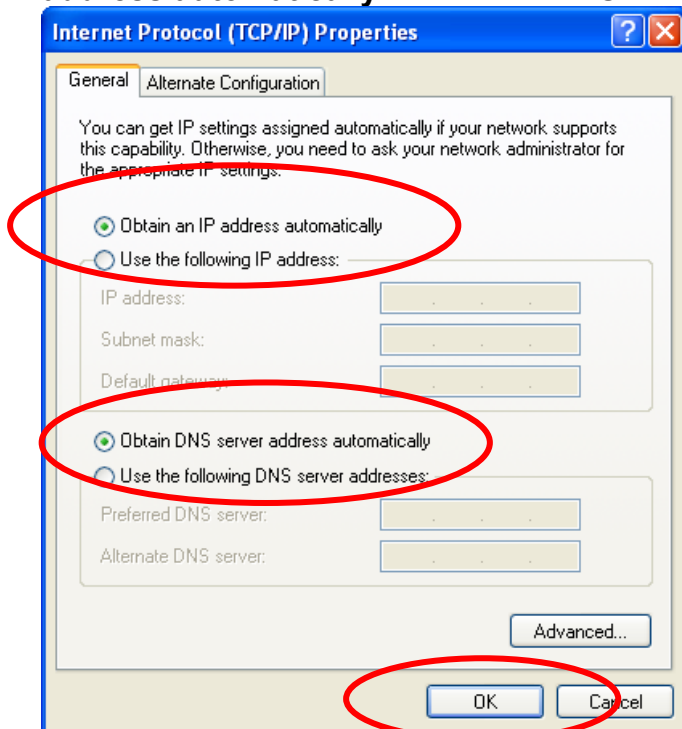
2. Single **RIGHT** click on **“Local Area connection”**, then click **“Properties”**.



3. Double click on **"Internet Protocol (TCP/ IP)"**.



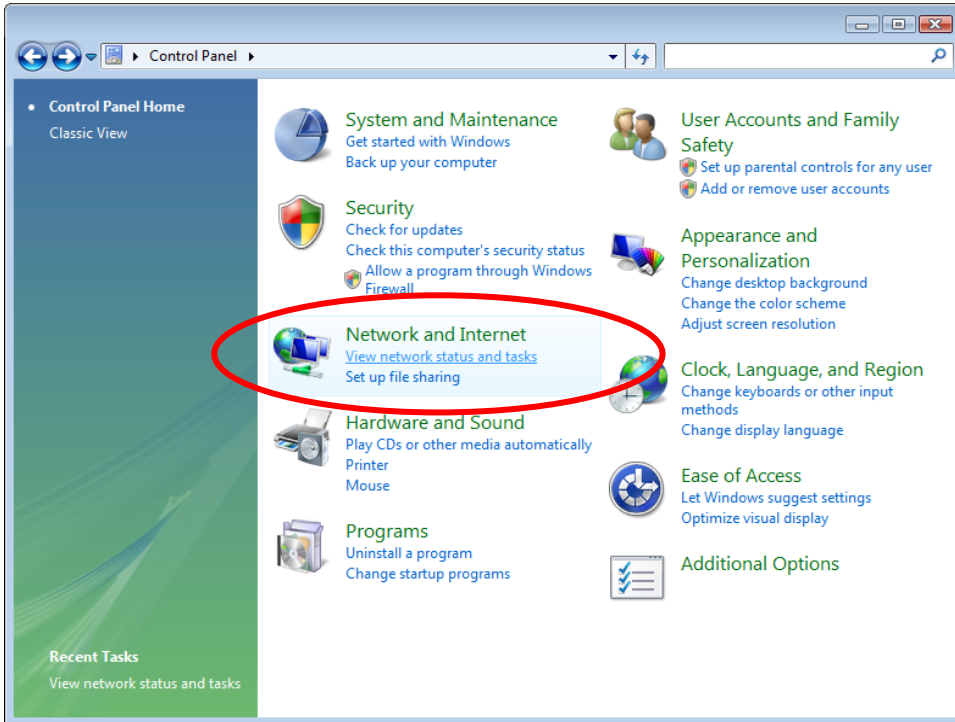
4. Check **"Obtain an IP address automatically"** and **"Obtain DNS server address automatically"** then click on **"OK"** to continue.



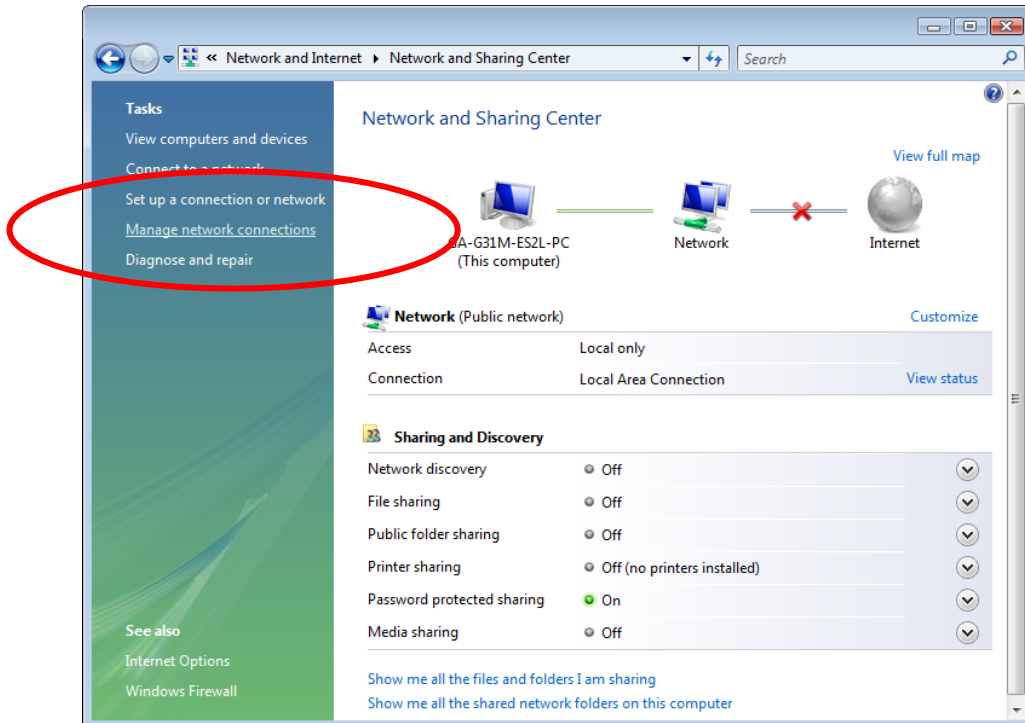
5. Click **"Show icon in notification area when connected"** (see screen image in 3. above) then Click on **"OK"** to complete the setup procedures.

For Windows Vista-32/64

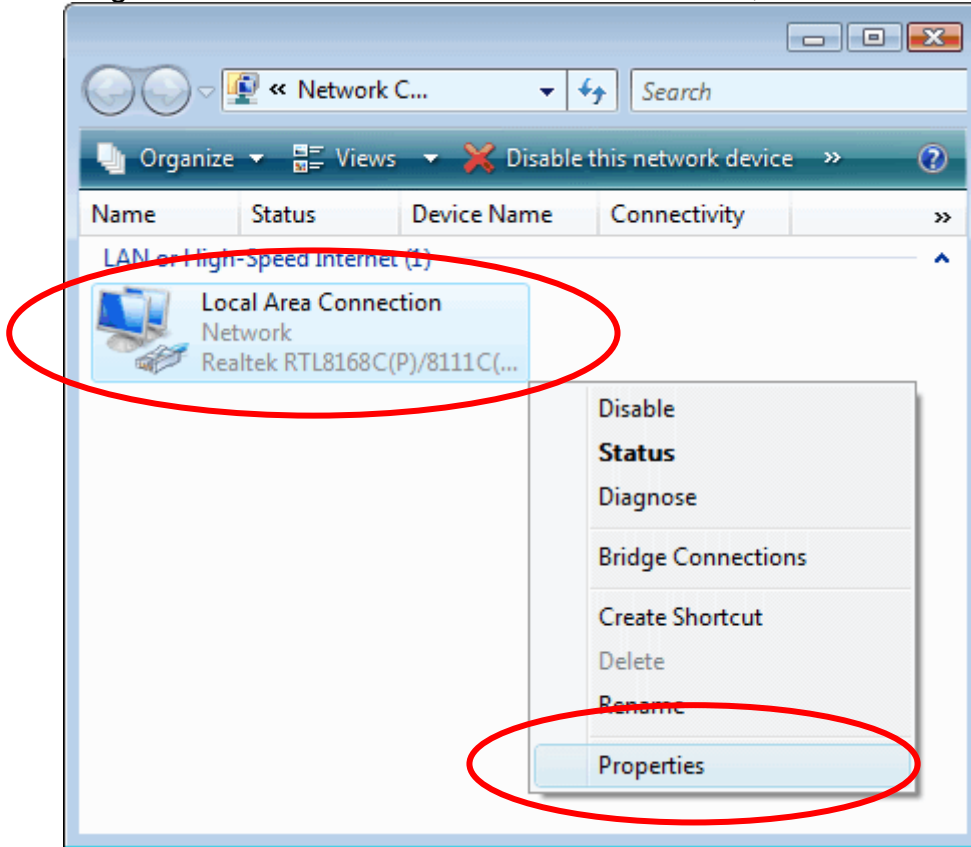
1. Click on “Start” -> “Control Panel” -> “View network status and tasks”.



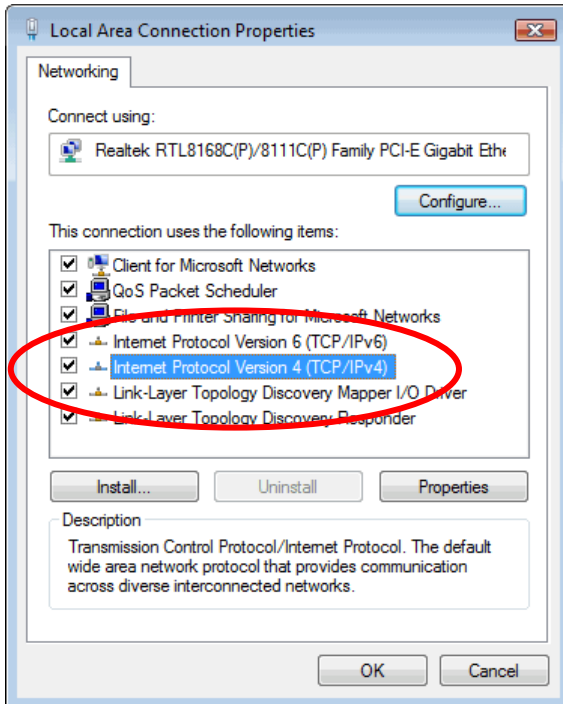
2. In the Manage network connections, click on “Manage network connections” to continue.



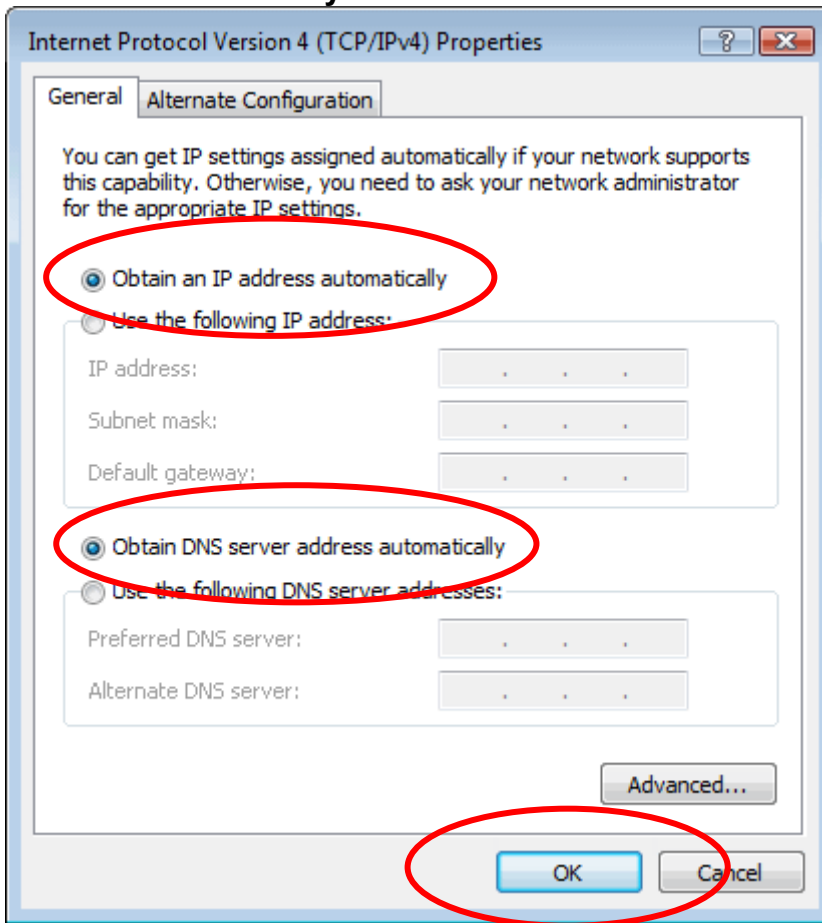
3. Single RIGHT click on "Local Area connection", then click "Properties".



4. The screen will display the information "User Account Control" and click "Continue" to continue.
5. Double click on "Internet Protocol Version 4 (TCP/IPv4)".

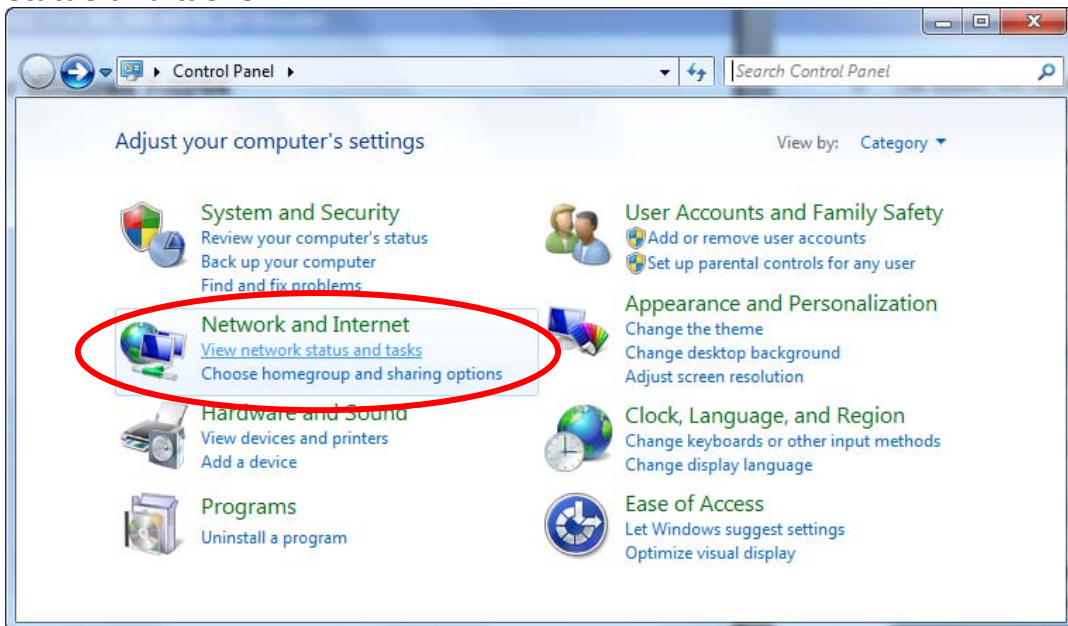


6. Check **"Obtain an IP address automatically"** and **"Obtain DNS server address automatically"** then click on **"OK"** to continue.

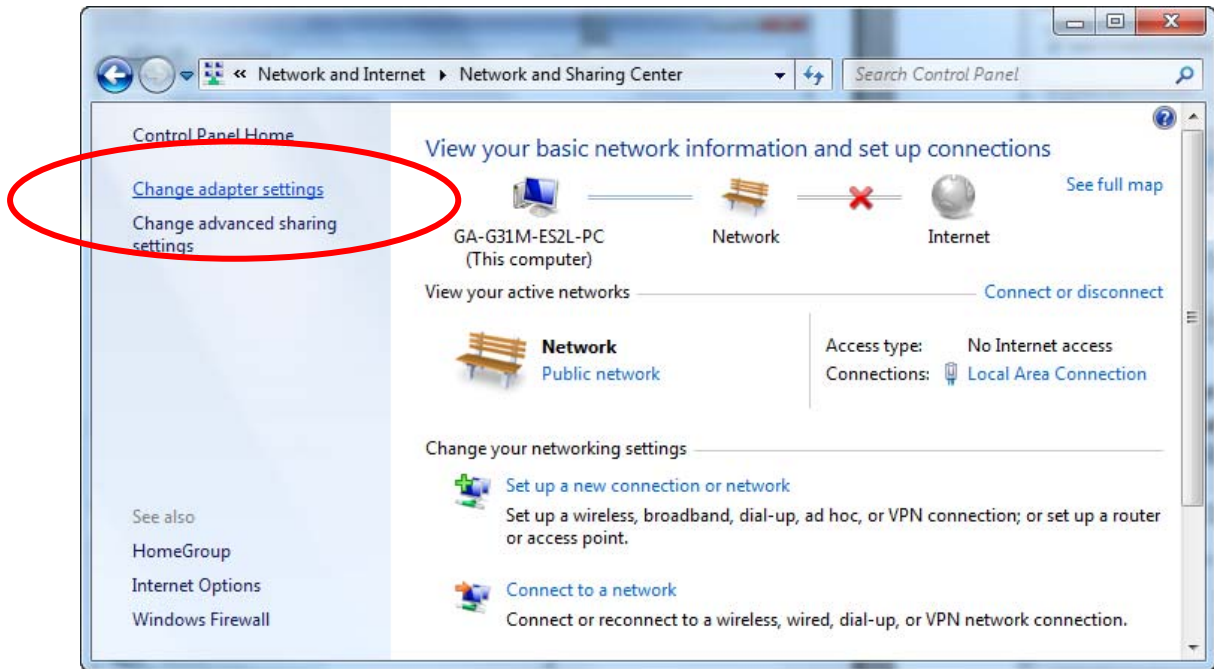


For Windows 7-32/64

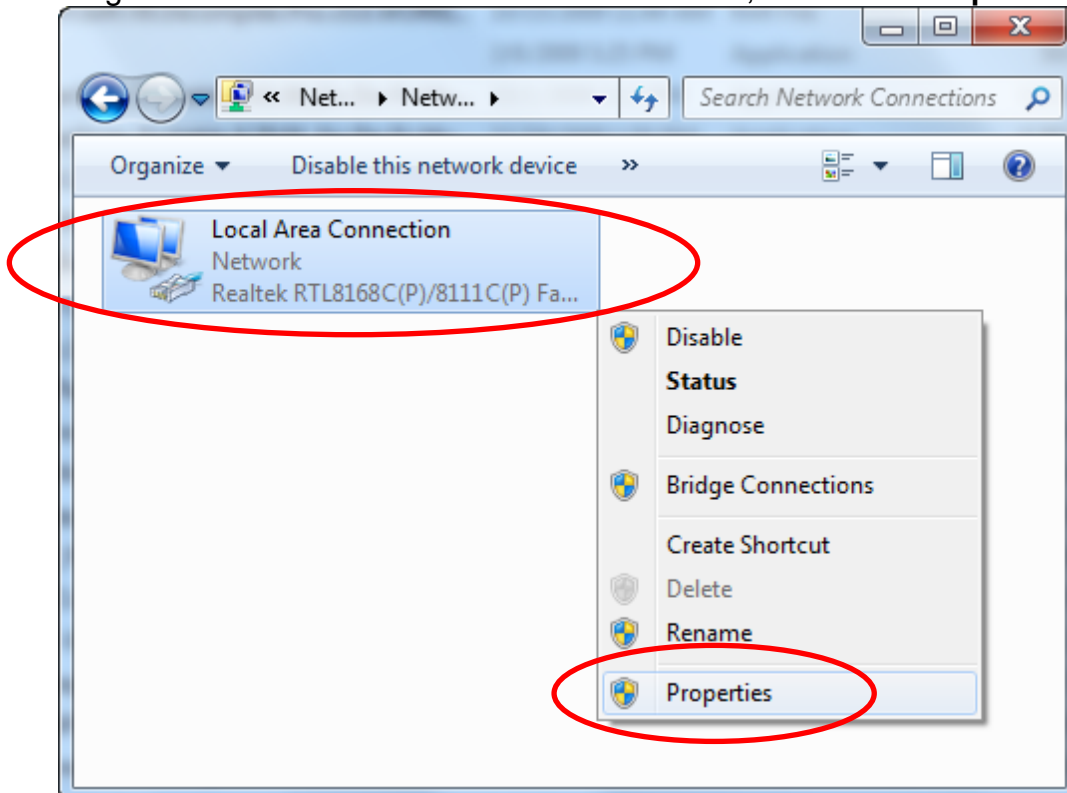
1. Click on **"Start"** -> **"Control Panel"** (in Category View) -> **"View network status and tasks"**.



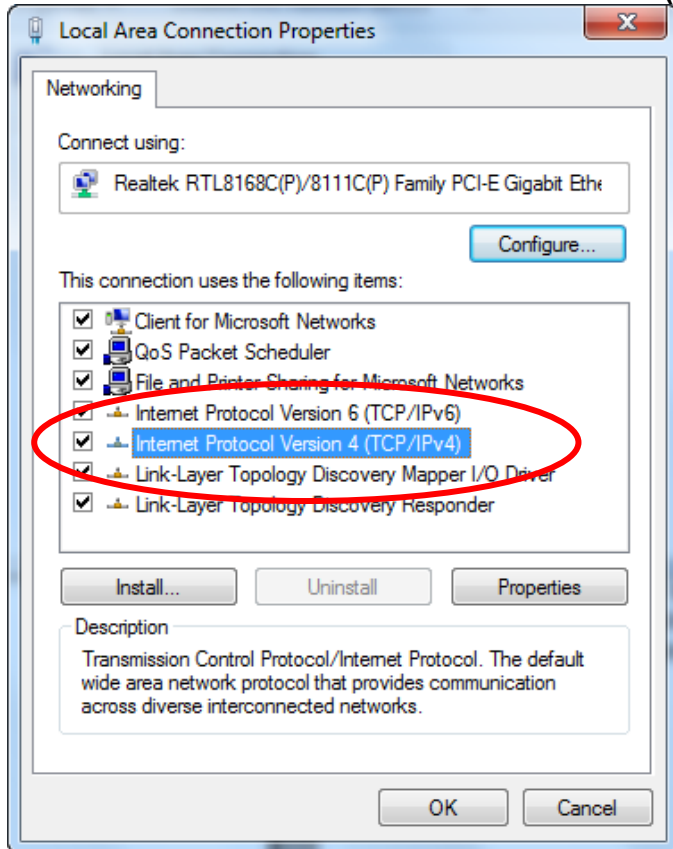
2. In the Control Panel Home, click on **“Change adapter settings”** to continue.



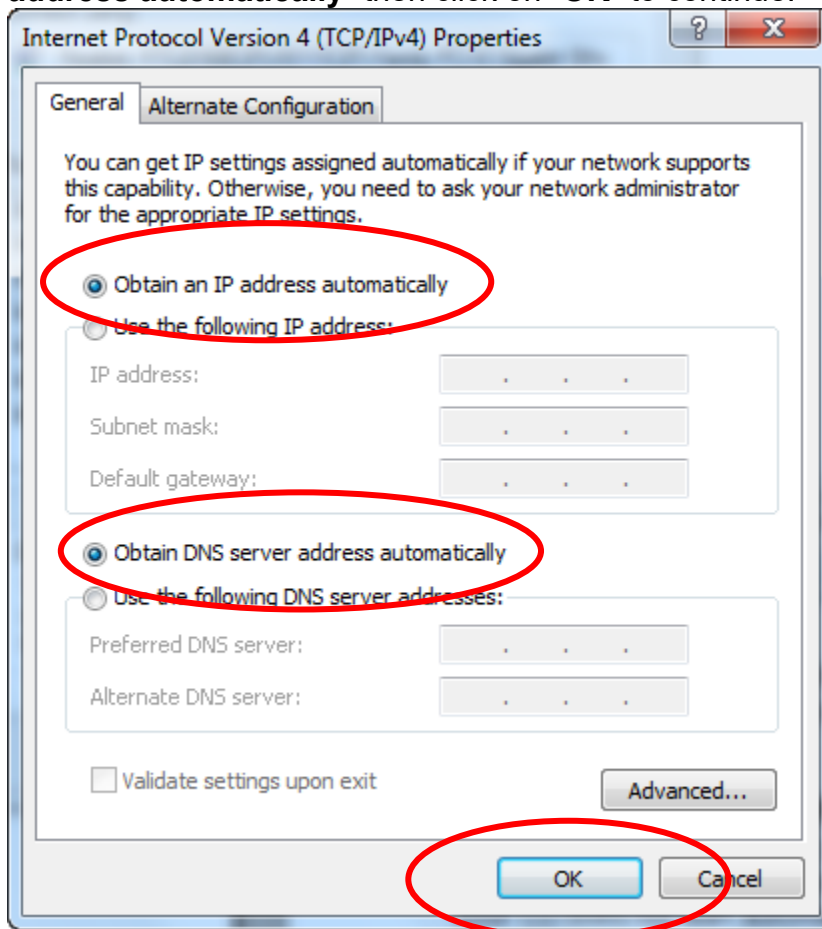
3. Single RIGHT click on **“Local Area connection”**, then click **“Properties”**.



4. Double click on "**Internet Protocol Version 4 (TCP/IPv4)**".



5. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.

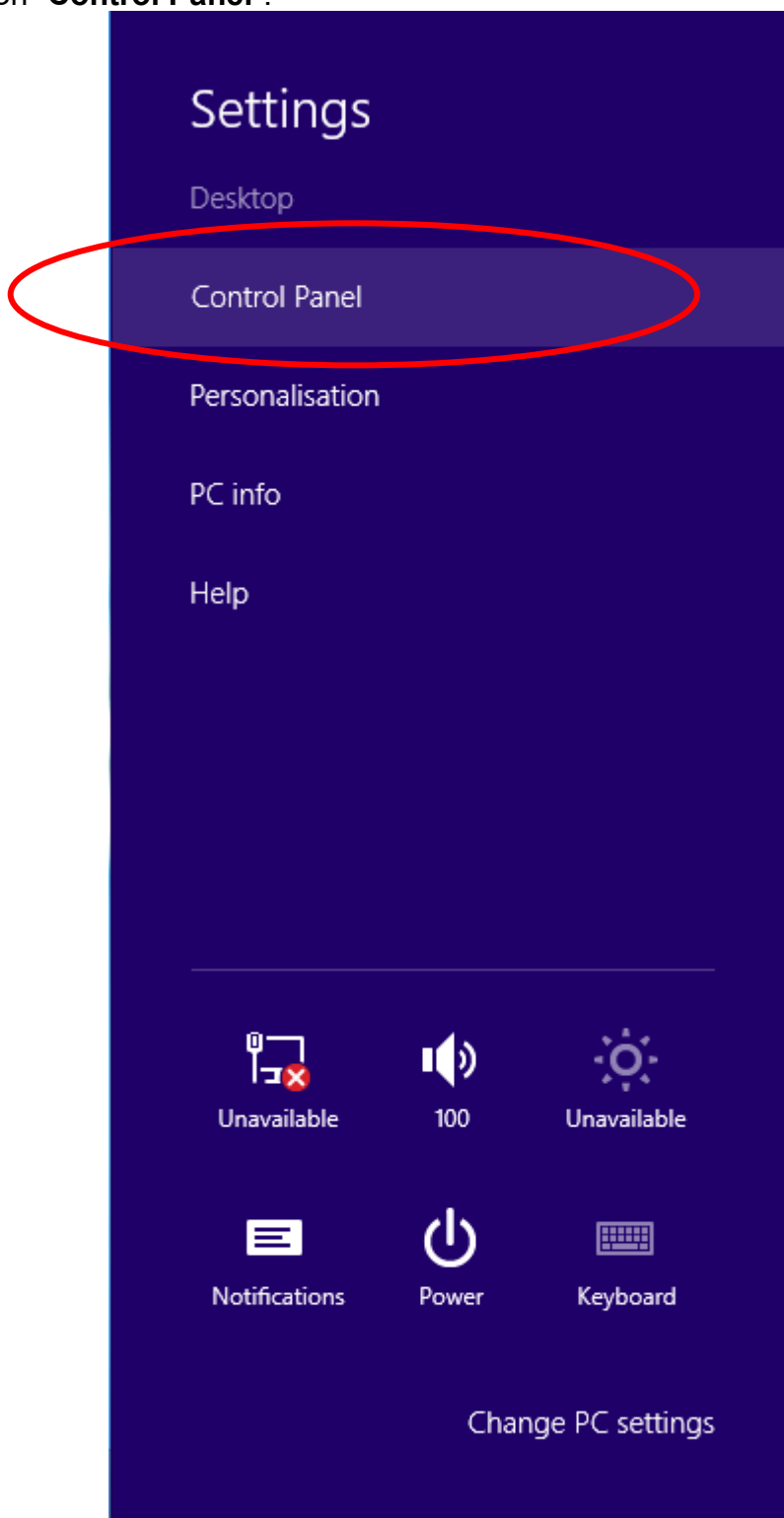


For Windows 8-32/64

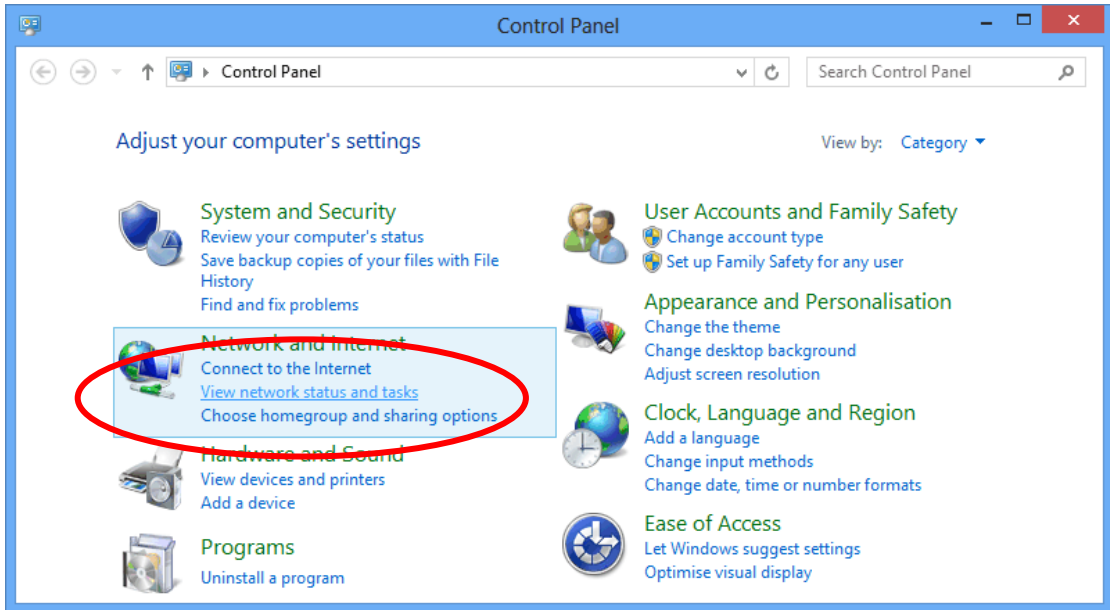
1. Move the mouse or tap to the upper right corner and click on **“Settings”**.



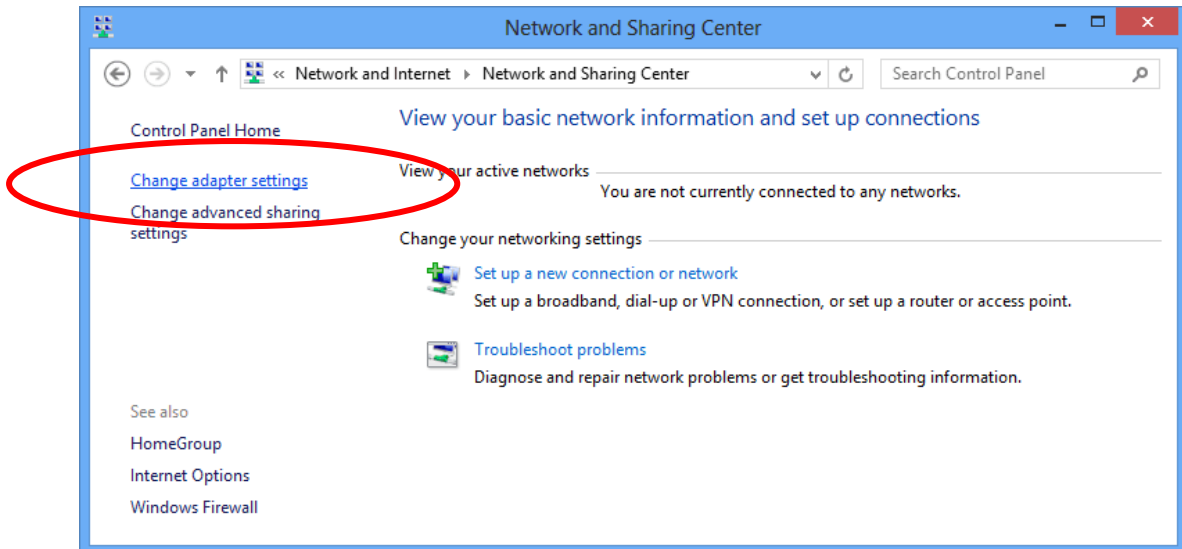
2. Click on **“Control Panel”**.



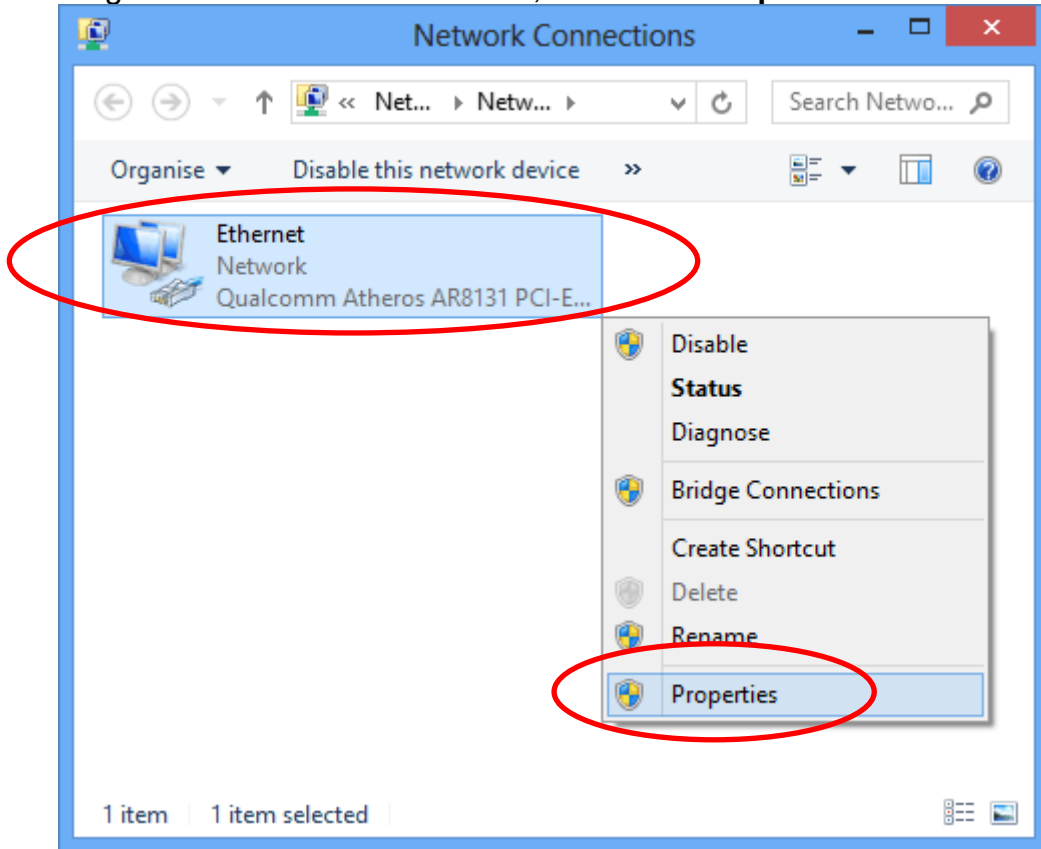
3. Click on **“View network status and tasks”**.



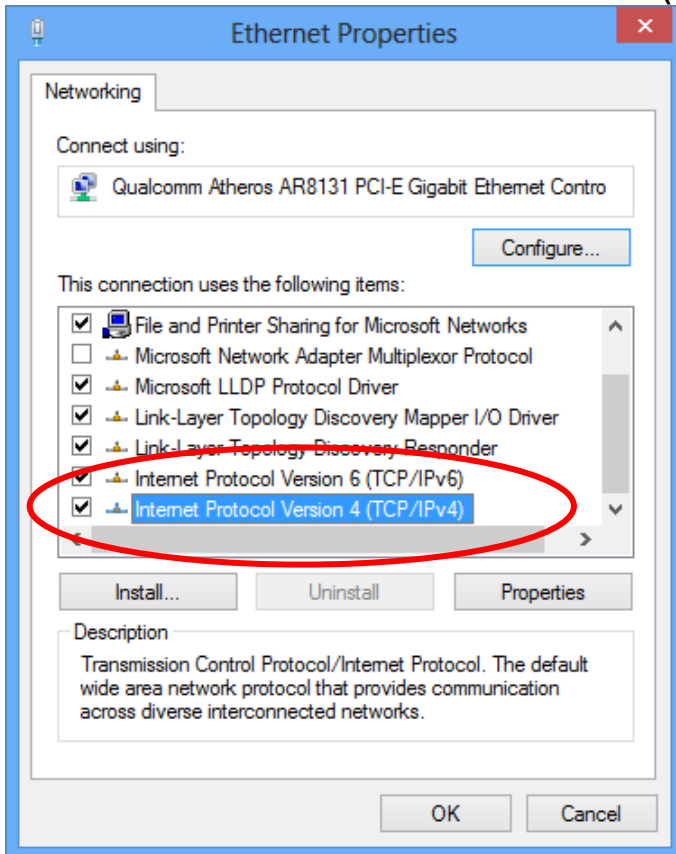
4. In the Control Panel Home, click on **“Change adapter settings”** to continue.



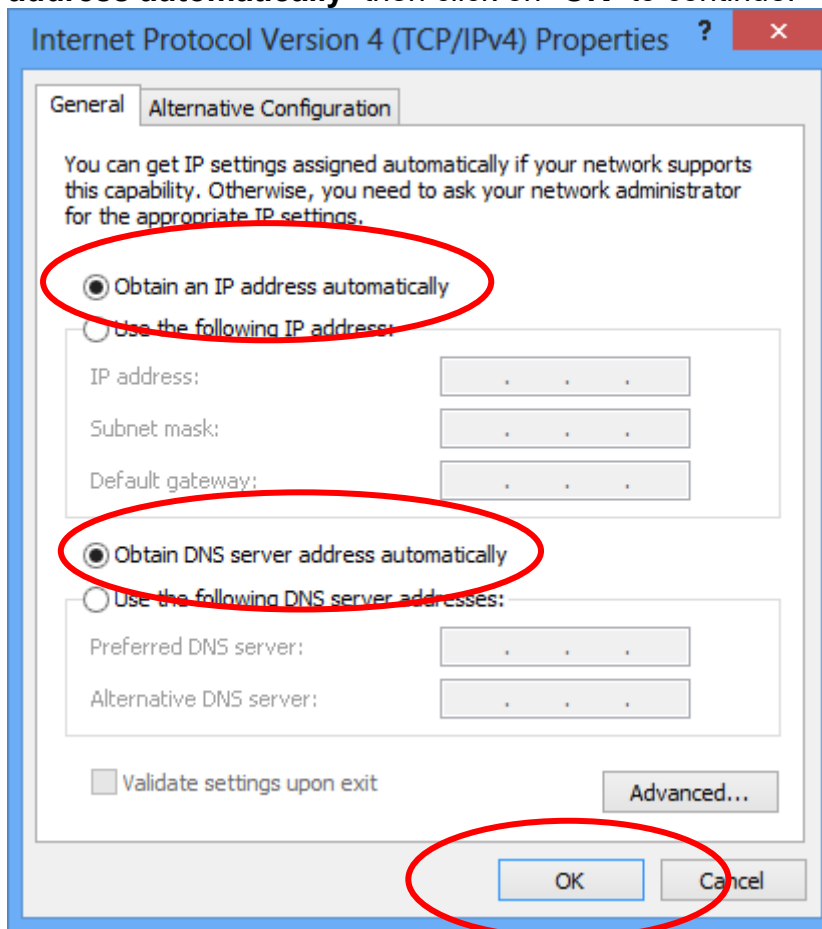
5. Single RIGHT click on **"Ethernet"**, then click **"Properties"**.



6. Double click on **"Internet Protocol Version 4 (TCP/IPv4)"**.



7. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.



4 Utility CD execution

Connecting the Hardware

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

1. Before you begin to execute utility CD Installations, please ensure the VDSL2 Router has been powered on.
2. Please insert the supplied CD into your CD-ROM drive.
3. The CD should auto-start, displaying the window shown in 4. below. If your CD does not start automatically, go to Windows Explorer, Select your CD drive and double click "**Autorun.exe**".
4. To configure the Internet configuration, please click the "**Advanced Configuration**".

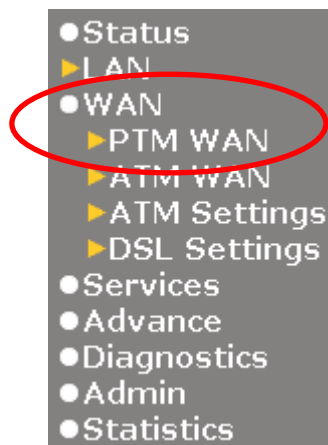


5. Please enter the User Name: **admin** and Password: **admin** and then click on **OK** button.



VDSL WAN Configuration (VDSL Line User)

1. From the left-hand menu, click on *WAN* -> *PTM WAN*.



Examples

8-1. PPPoE

From the *Channel Mode* drop-down list, select *PPPoE* setting.

Enable Enable NAPT

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.

Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.

Configure IPv6 WAN setting determined by your ISP if any.

If you are happy with your settings, click *Apply Changes*

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0

Enable VLAN:

VLAN ID:

802.1p_Mark

Channel Mode: PPPoE

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069

IP Protocol: IPv4/IPv6

PPP Settings: User Name: Password:

Type: Continuous Idle Time (sec):

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

Apply Changes

Delete

8-2. Bridged

From the Channel Mode drop-down list, select Bridged setting.

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

If you are happy with your settings, click Apply Changes

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

Channel Mode: Bridged ▾

Enable NAPT:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

802.1p_Mark

Enable QoS:

Apply Changes Delete

Now you can load your PPPoE Client Software onto your PC.
Now you can load your PPPoE Client Software with user name and password which determined by your ISP onto your PC.

8-3. IPoE by DHCP

From the *Channel Mode* drop-down list, select *IPoE*

Enable Enable NAPT

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.

From the Type ratio, click DHCP.

Configure IPv6 WAN setting determined by your ISP if any.

If you are happy with your settings, click Apply Changes

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

Channel Mode: IPoE ▾

Enable NAPT:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

802.1p_Mark

Enable QoS:

IP Protocol: IPv4/IPv6 ▾

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

Apply Changes Delete

8-4. IPoE by Fixed IP

From the *Channel Mode* drop-down list, select *IPoE* setting.

Enable Enable NAPT

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.

From the Type ratio, click Fixed IP.

Enter Local IP Address, Subnet Mask and Remote IP Address which was given by Telecom or by your Internet Service Provider (ISP).

Configure IPv6 WAN setting determined by your ISP if any.

If you are happy with your settings, click Apply Changes

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

802.1p_Mark ▾

Channel Mode: IPoE ▾

Enable WAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

IP Protocol: IPv4/IPv6 ▾

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

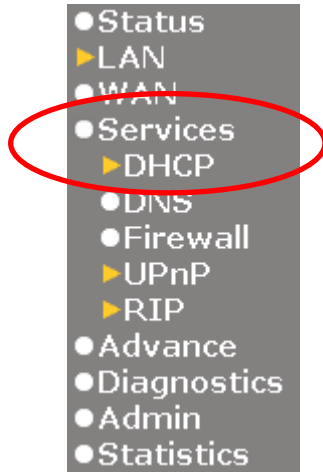
Request Options:

Request Address

Request Prefix

Apply Changes

From the left-hand Service menu, click on Services -> DHCP.



From the Type ratio, click Set Manually.

Enter DNS setting determined by your ISP.

If you are happy with your settings, click *Apply Changes*

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: **seconds (-1 indicates an infinite lease)**

Domain Name:

Gateway Address:

DNS option: Use DNS Relay Set Manually

DNS1:

DNS2:

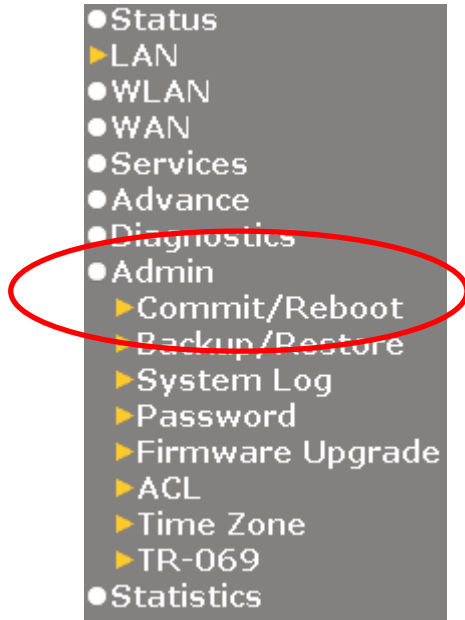
DNS3:

Click OK

Change setting successfully!

OK

2. From the left-hand menu, click on *Admin -> Commit/Reboot*.



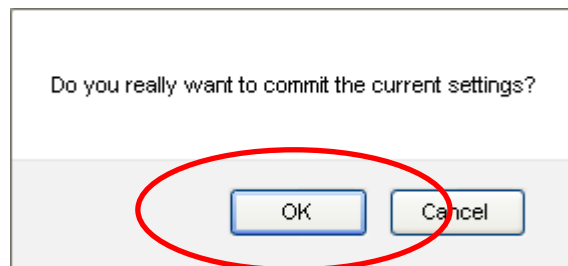
3. Click on *Commit and Reboot*.

Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

4. Click on *OK*.



5. System rebooting, Please wait ...

System rebooting, Please wait ... 58

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

DSL WAN Configuration (ADSL Line User)

1. From the left-hand menu, click on *WAN* -> *ATM WAN*.



Examples

8-1. PPPoE

Enter VCI and VPI setting determined by your ISP.

Select the Encapsulation determined by your ISP.

From the *Channel Mode* drop-down list, select *PPPoE* setting.

Enable Enable NAPT

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.

Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.

Configure IPv6 WAN setting determined by your ISP if any.

If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:

Encapsulation: LLC VC-Mux

Channel Mode:

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type:

Enable VLAN: Disable

VLAN ID(0-4095):

802.1p_Mark:

Enable

IP Protocol:

PPP Settings: User Name:

Password:

Type:

Idle Time (sec):

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6

Client:



Request Options:

Request Address

Request Prefix

8-2. PPPoA

Enter VCI and VPI setting determined by your ISP.
 Select the Encapsulation determined by your ISP.
 From the *Channel Mode* drop-down list, select *PPPoA* setting.

Enable Enable NAPT

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.

Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.

Configure IPv6 WAN setting determined by your ISP if any.

If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:
 Encapsulation: LLC VC-Mux
 Channel Mode:

Enable NAPT:
 Enable QoS:

Admin Status: Enable Disable

Connection Type:

Enable VLAN: Disable Enable
 VLAN ID(0-4095):
 802.1p_Mark:

IP Protocol:

PPP Settings: User Name: Password:
 Type: Idle Time (sec):

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

 Request Prefix

8-3. Bridged

Enter VCI and VPI setting determined by your ISP.
 Select the Encapsulation determined by your ISP.
 From the Channel Mode drop-down list, select 1483 Bridged setting.
 From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.
 If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:
 Encapsulation: LLC VC-Mux
 Channel Mode:

Enable NAPI:
 Enable QoS:

Admin Status: Enable Disable

Connection Type:

Enable VLAN: Disable Enable
 VLAN ID(U-4095):
 802.1p_Mark:

Now you can load your PPPoE Client Software onto your PC.
 Now you can load your PPPoE Client Software with user name and password which determined by your ISP onto your PC.

8-4. 1483 MER by DHCP

Enter VCI and VPI setting determined by your ISP.
 Select the Encapsulation determined by your ISP.
 From the *Channel Mode* drop-down list, select *1483 MER*

Enable Enable NAPT

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.

From the Type ratio, click DHCP.

Configure IPv6 WAN setting determined by your ISP if any.

If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

Encapsulation: LLC VC-Mux

Channel Mode: 1483 MER

Enable NAPT:
Enable QoS:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069

Enable VLAN: Disable Enable

 VLAN ID(0-4095):

 802.1p_Mark:

IP Protocol: IPv4/IPv6

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address: **Remote IP Address:**

Subnet Mask: **Unnumbered**

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

8-5. 1483 MER by Fixed IP

Enter VCI and VPI setting determined by your ISP.

Select the Encapsulation determined by your ISP.

Enable Enable NAPT

From the *Connection Type* drop-down list, select *INTERNET_TR069* setting.

From the *Channel Mode* drop-down list, select *1483 MER* setting.

From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.

From the Type ratio, click Fixed IP.

Enter Local IP Address, Subnet Mask and Remote IP Address which was given by Telecom or by your Internet Service Provider (ISP).

Configure IPv6 WAN setting determined by your ISP.

If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:

Encapsulation: LLC VC-Mux

Channel Mode:

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type:

Enable VLAN: Disable Enable

VLAN ID(0-4095):

802.1p_Mark:

IP Protocol:

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

IPv6 WAN Setting:

Address Mode: Slaac Static

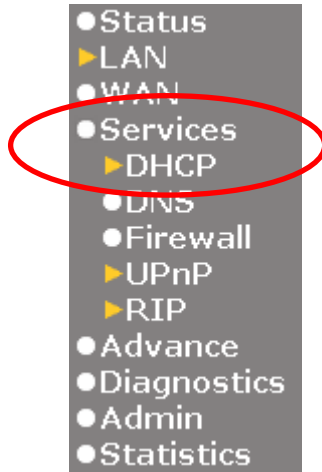
Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

From the left-hand Service menu, click on Services -> DHCP.



From the Type ratio, click Set Manually.

Enter DNS setting determined by your ISP.

If you are happy with your settings, click *Apply Changes*

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: **seconds (-1 indicates an infinite lease)**

Domain Name:

Gateway Address:

DNS option: Use DNS Relay Set Manually

DNS1:

DNS2:

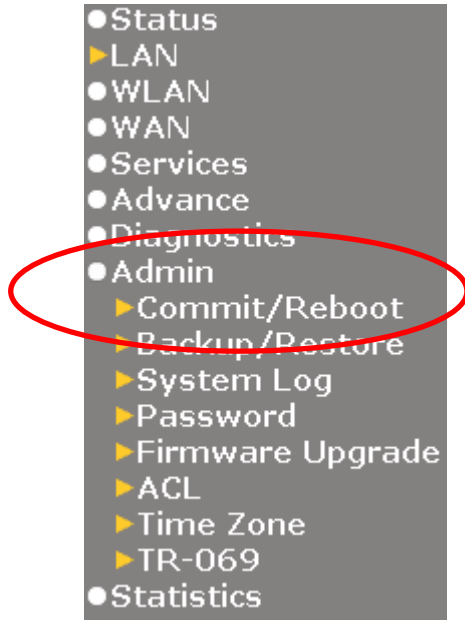
DNS3:

Click OK

Change setting successfully!

OK

2. From the left-hand menu, click on *Admin -> Commit/Reboot*.



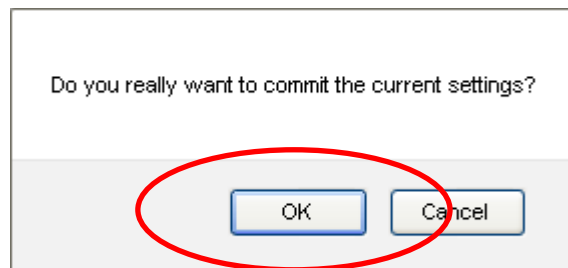
3. Click on *Commit and Reboot*.

Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

4. Click on *OK*.



5. System rebooting, Please wait ...

System rebooting, Please wait ...
58

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

6. Click on " **Exit** " to exit this program.



7. Now, the VDSL2 Router has been configured completely, and suitable for Internet Connections.

5 Getting Started with the Web pages

The VDSL2 Router includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through your web browser from any PC connected to the device via the LAN ports.

Accessing the Web pages

To access the Web pages, you need the following:

- A PC or laptop connected to the LAN 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 following URL in the web address (or location) box, and press [Enter] on your keyboard:

http://192.168.1.1

The Status homepage for the web pages is displayed:

Router Status

This page shows the current status and some basic settings of the device.

System						
Alias Name	VDSL Modem/Router					
Uptime	1:17					
Firmware Version	R104R1B_STD_30_131217					
DSP Version	v117d927					
Name Servers						
IPv4 Default Gateway						
IPv6 Default Gateway						
DSL						
Operational Status	ACTIVATING.					
Upstream Speed	0 kbps					
Downstream Speed	0 kbps					
LANConfiguration						
IP Address	192.168.1.1					
Subnet Mask	255.255.255.0					
DHCP Server	Enabled					
MAC Address	001333e4f5d6					
WANConfiguration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
ppp1_ptm0_0	---	---	PPPoE			down 0sec / 0sec
ppp0_vc0_0	8/35	LLC	PPPoE			down 0sec / 0sec

Figure 1: Homepage

The first time that you click on an entry from the left-hand menu, a login box is displayed. You must enter your username and password to access the pages.

A login screen is displayed:



Figure 2: Login screen

1. Enter your user name and password. The first time you log into the program, use these defaults:

User Name: **admin**
 Password: **admin**



Note

You can change the password at any time or you can configure your device so that you do not need to enter a password. See *Password*.

2. Click on OK. You are now ready to configure your device.

This is the first page displayed each time you log in to the Web pages. This page contains links to the following pages:

- Addressing; links to the *Addressing* page that controls your device's network address. See *Addressing*.
- Internet Access; links to the *Internet Access* page that controls how your device connects to the Internet. See *Internet Access*.



Note

If you receive an error message or the *Welcome* page is not displayed, see *Troubleshooting Suggestions*.

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:

Table 1. LED Indicators

LED	Behavior
<i>POWER</i>	Solid green to indicate that the device is turned on. If this light is not on, check the power cable attachment.
<i>ETH</i>	Flashing on/off while the device is booting. After about 10-15 seconds, solid green to indicate that the device can communicate with your LAN.
<i>Link</i>	Flashing on/off while data is being transmitted. Solid green to indicate that the device has successfully established a connection with your ISP.
<i>INTERNET</i>	Flashing on/off while data is being transferred. Solid green when a valid IP address has been assigned to the device by the ISP.

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.yahoo.com>). The LED labeled *INTERNET* should blink rapidly and then appear solid as the device connects to the site.

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. For details, see *Internet Access*. If the LEDs still do not illuminate as expected or the web page is not displayed, see *Troubleshooting Suggestions* 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
<i>LINE Port IP Address</i>	Unnumbered interface: 192.168.1.1 Subnet mask: 255.255.255.255	This is the temporary public IP address of the WAN port on the device. It is an unnumbered interface that is replaced as soon as your ISP assigns a 'real' IP address. See <i>Internet Access</i> .

Option	Default Setting	Explanation/Instructions
<i>LAN Port IP Address</i>	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 <i>LAN</i> .
<i>DHCP (Dynamic Host Configuration Protocol)</i>	DHCP server enabled with the following pool of addresses: 192.168.1.33 through 192.168.1.254	The VDSL2 Router 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 <i>Services -> DHCP Settings</i> .
<i>NAT (Network Address Translation)</i>	NAT enabled	Your computers' private IP addresses (see DHCP above) will be translated to your public IP address whenever the PCs access the Internet. See <i>Services -> Firewall</i> .

6 Overview

The *Overview* page displays useful information about the setup of your device, including:

- details of the device's Internet access settings
- version information about your device

To display this page:

From the left menu, click on *Status - Device*. The following page is displayed:

Router Status

This page shows the current status and some basic settings of the device.

System						
Alias Name	VDSL Modem/Router					
Uptime	1:17					
Firmware Version	R104R1B_STD_30_131217					
DSP Version	v117d927					
Name Servers						
IPv4 Default Gateway						
IPv6 Default Gateway						
DSL						
Operational Status	ACTIVATING.					
Upstream Speed	0 kbps					
Downstream Speed	0 kbps					
LANConfiguration						
IP Address	192.168.1.1					
Subnet Mask	255.255.255.0					
DHCP Server	Enabled					
MAC Address	001333e4f5d6					
WANConfiguration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
ppp1_ptm0_0	---	---	PPPoE			down 0sec / 0sec
ppp0_vc0_0	8/35	LLC	PPPoE			down 0sec / 0sec

Figure 3: Overview page

The information displayed on this page is explained in detail in the following sections.

Internet access settings

This section displays details of the settings that allow your device to access the Internet. These details include:

IP address and subnet mask:	The IP address and subnet mask assigned to your WAN interface. This address is used temporarily until your ISP assigns a real IP address (via DHCP or PPP – see <i>Internet Access</i>).
Default gateway:	The address of the ISP server through which your Internet connection will be routed.
DNS servers:	The Domain Name System (DNS) servers used by your ISP to map domain names to IP addresses.

Your ISP assigns all of these settings. In most cases, you **will not** need to make changes to these settings in order for your Internet connection to work. If your ISP does ask you to change any of these settings, follow the instructions for manually configuring your device in *Internet Access*.

About VDSL2 Router

This section displays details of your device's hardware and firmware versions. If you need to contact your ISP's support team, they may need to know which hardware/firmware versions you are using in order to answer your query.

Your hardware version details contain information about the make and model of your device and its exact hardware components.

Your firmware version details contain information about the software program running on your device. They then make the latest updated version available to you via the Internet. For details of how to update your firmware, see *Admin -> Upgrade Firmware*.

7 Status

You can view statistics on the processing of IP packets on the networking interfaces. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

Device Info

This page shows the current status and some basic settings of the device.

1. From the left *Status* menu, click on *Device*. The following page is displayed:
2. To display updated statistics showing any new data since you opened this page, click *Refresh*.

Router Status

This page shows the current status and some basic settings of the device.

System	
Alias Name	VDSL Modem/Router
Uptime	1:17
Firmware Version	R104R1B_STD_30_131217
DSP Version	v117d927
Name Servers	
IPv4 Default Gateway	
IPv6 Default Gateway	
DSL	
Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps
LANConfiguration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	001333e4f5d6

WANConfiguration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
ppp1_ptm0_0	---	---	PPPoE			down 0sec / 0sec
ppp0_vc0_0	8/35	LLC	PPPoE			down 0sec / 0sec

Refresh

IPv6

This page shows the ADSL line statistic information.

1. From the left *Status* menu, click on *IPv6* The following page is displayed:
2. To display updated statistics showing any new data since you opened this page, click *Refresh*.

IPv6 Status

This page shows the current system status of IPv6.

LAN Configuration					
IPv6 Address					
IPv6 Link-Local Address					
				fe80::2e0:4cff:fe86:7001/64	
Prefix Delegation					
Prefix					
WAN Configuration					
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Status
Refresh					

8 Local Network Configuration

The *Addressing* page displays information about your LAN IP address and allows you to change the address and subnet mask assigned to your device.



Note

You should only change the addressing details if your ISP asks you to, or if you are familiar with network configuration. In most cases, you will not need to make any changes to this configuration.

Changing the LAN IP address and subnet mask

1. From the left menu, click on *LAN*. The following page is displayed:

LAN Interface Settings

This page is used to configure the LAN interface of your Router. Here you may change the setting for IP addresses, subnet mask, etc..

Interface Name:	br0
IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input type="checkbox"/> Secondary IP	
IGMP Snooping:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
<input type="button" value="Apply Changes"/>	

2. From the left-hand *LAN* menu, click on *LAN*.
3. Type a new IP Address and Subnet Mask.
4. Click *Apply Changes*.

LAN Interface Settings

This page is used to configure the LAN interface of your Router. Here you may change the setting for IP addresses, subnet mask, etc..

Interface Name:	br0
IP Address:	<input type="text" value="10.0.0.2"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input type="checkbox"/> Secondary IP	
IGMP Snooping:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
<input type="button" value="Apply Changes"/>	

5. The primary IP address is being changed to 10.0.0.2 netmask 255.255.255.0. Then please go to <http://10.0.0.2> to continue. Your browser communicates with the web server via the LAN connection, and changing the IP address may disrupt this.

You may also need to renew your DHCP lease:

Windows 95/98

- a. Select **Run...** from the **Start** menu.
- b. Enter **winipcfg** and click **OK**.
- c. Select your ethernet adaptor from the pull-down menu
- d. Click **Release All** and then **Renew All**.
- e. **Exit** the winipcfg dialog.

Windows NT/Windows 2000/Windows XP

- a. Bring up a command window.
- b. Type **ipconfig /release** in the command window.
- c. Type **ipconfig /renew**.
- d. Type **exit** to close the command window.

Linux

- a. Bring up a shell.
- b. Type **pump -r** to release the lease.
- c. Type **pump** to renew the lease.

**Note**

If you change the LAN IP address of the device while connected through your Web browser, you will be disconnected. You must open a new connection by entering your new LAN IP address as the URL.

Adding the Secondary LAN IP address and subnet mask

1. From the left-hand *LAN* menu, click on *LAN*.
2. Check on *Secondary IP*.
3. Type the Secondary IP Address and Subnet Mask.
4. Click *Apply Changes*.

LAN Interface Settings

This page is used to configure the LAN interface of your Router. Here you may change the setting for IP addresses, subnet mask, etc..

Interface Name:	br0
IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input checked="" type="checkbox"/> Secondary IP	
IP Address:	<input type="text" value="192.168.100.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
IGMP Snooping:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

5. Change setting successfully!
6. Click OK.

Change setting successfully!

Change IP Pool Range and Subnet mask

1. From the left-hand *Services* menu, click on *DHCP*.

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range:	<input type="text" value="192.168.1.33"/> - <input type="text" value="192.168.1.254"/>	
	<input type="button" value="Show Client"/>	
Subnet Mask:	<input type="text" value="255.255.255.0"/>	
Max Lease Time:	<input type="text" value="86400"/> seconds (-1 indicates an infinite lease)	
Domain Name:	<input type="text" value="domain.name"/>	
Gateway Address:	<input type="text" value="192.168.1.1"/>	
DNS option:	<input checked="" type="radio"/> Use DNS Relay <input type="radio"/> Set Manually	
<input type="button" value="Apply Changes"/>	<input type="button" value="MAC-Based Assignment"/>	<input type="button" value="STB Data Pool"/>

2. Change the *IP Pool Range/Subnet Mask* and then click *Apply Changes* button.

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: seconds (-1 indicates an infinite lease)

Domain Name:

Gateway Address:

DNS option: Use DNS Relay Set Manually

3. Change setting successfully!
4. Click OK.

Change setting successfully!

9 PTM WAN

This chapter describes how to configure the way that your device connects to the Internet. Your ISP determines what type of Internet access you should use and provides you with any information that you need in order to configure the Internet access to your device.

The device supports four methods of obtaining the WAN IP address:

Option	Description
Bridged	Choose this option to have the device to be a AP
IPoE Fixed IP	Choose this option if you are a leased line user with a fixed IP address.
IPoE DHCP Client	Choose this option if you are connected to the Internet through a Cable modem line.
PPPoE	Choose this option if you are connected to the Internet through a DSL line
DS-Lite	Choose this option if you are connected to the DS-Lite Server
6rd	Choose this option if you are connected to the 6rd Server

- From the left-hand *Network Settings* -> *PTM WAN* menu. The following page is displayed:

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID: 802.1p_Mark ▾

Channel Mode: PPPoE ▾

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

IP Protocol: IPv4/IPv6 ▾

PPP Settings: User Name: Password:

Type: Continuous ▾ Idle Time (sec):

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Option	Description
Enable VLAN	Enable or disable VLAN
VLAN ID	Enter the VLAN ID

802.1p_Mark		Choose the 802.1p_Mark
Channel Mode	Bridged	Choose this option to have the device to be a AP
	IPoE Fixed IP	Choose this option if you are a leased line user with a fixed IP address.
	IPoE DHCP Client	Choose this option if you are connected to the Internet through a Cable modem line.
	PPPoE	Choose this option if you are connected to the Internet through a DSL modem line
	DS-Lite	Choose this option if you are connected to the DS-Lite Server
	6rd	Choose this option if you are connected to the 6rd Server
Enable NAPT		Enable or disable NAPT
Enable IGMP		Enable or disable IGMP
Enable Default Route		Enable or disable Default Route
Enable Admin Status		Enable or disable Admin Status
IP Protocol		IPv4/IPv6, IPv4 or IPv6
Local IP Address		Check with your ISP provider
Subnet Mask		Check with your ISP provider
Remote IP Address		Check with your ISP provider
User Name		User name for PPPoE registration recognized by the Internet service provider
Password		Password for PPPoE registration recognized by the Internet service provider
Connection Type	Continuous	The connection is always on
	Connect on Demand	Enter the minutes after which the session must be disconnected, if no activity takes place
	Manual	Manually connect
Idle Time		Enter the minutes after which the session must be disconnected
IPv6 WAN Address Mode		Check with your ISP provider
Enable DHCPv6 Client		Check with your ISP provider
Port Mapping		Port Mapping configuration

Configuring PTM WAN IPoE Static IP connection

If you are a leased line user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP.

If your ISP wants you to connect to the Internet using Static IP, follow the instructions below.

6. From the left-hand *WAN Settings* -> *PTM WAN* menu. The following page is displayed:
7. From the *Channel Mode* drop-down list, select *IPoE* setting.
8. Enable *Enable NAPT*
9. Select proper *Connection Type*
10. Enable *Fixed IP*
11. Enter *Local IP Address, WAN Subnet Mask and Remote IP Address* which was given by Telecom or by your Internet Service Provider (ISP).
12. Click *Apply Changes*.

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

Channel Mode: IPoE ▾

Enable NAPT:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

802.1p_Mark

Enable QoS:

IP Protocol: IPv4/IPv6 ▾

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

- Request Address
- Request Prefix

13. From the left-hand menu, click on *Services* -> *DHCP*.

- Status
- ▶ LAN
- WLAN
- WAN
- Services
 - ▶ DHCP
 - DNS
 - Firewall
 - ▶ UPnP
 - ▶ RIP
 - ▶ Samba
- Advance
- Diagnostics
- Admin
- Statistics

- From the Type ratio, click Set Manually.
- Enter DNS setting determined by your ISP.
- If you are happy with your settings, click *Apply Changes*

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: **seconds (-1 indicates an infinite lease)**

Domain Name:

Gateway Address:

DNS option: Use DNS Relay Set Manually

- Click OK.

Change setting successfully!

Configuring PTM WAN IPoE DHCP Client connection

Dynamic Host Configuration Protocol (DHCP), Dynamic IP (Get WAN IP Address automatically). If you are connected to the Internet through a Cable modem line, then a dynamic IP will be assigned.

If your ISP wants you to connect to the Internet using DHCP Client, follow the instructions below.

1. From the left-hand *WAN Settings* -> *PTM WAN* menu. The following page is displayed:
2. From the *Channel Mode* drop-down list, select *IPoE* setting.
3. Enable *Enable NAPT*
4. Select proper *Connection Type*
5. Enable *DHCP*
6. Click *Apply Changes*.

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

Channel Mode: IPoE ▾

Enable NAPT:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

802.1p_Mark

Enable QoS:

IP Protocol: IPv4/IPv6 ▾

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

Configuring PTM WAN PPPoE connection

If your ISP's Internet service uses PPPoE you need to set up a PPP login account. The first time that you login to the Internet, your ISP will ask you to enter a username and password so they can check that you are a legitimate, registered Internet service user. Your device stores these authentication details, so you will not have to enter this username and password every time you login.

If your ISP wants you to connect to the Internet using PPP, follow the instructions below.

1. From the left-hand *WAN Settings* -> *PTM WAN* menu. The following page is displayed:
2. From the *Channel Mode* drop-down list, select *PPPoE* setting.
3. Enable *Enable NAPT*
4. Select proper *Connection Type*
5. Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.
6. Click *Apply Changes*.

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

802.1p_Mark

Channel Mode: PPPoE ▾

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

IP Protocol: IPv4/IPv6 ▾

PPP Settings: User Name: Password:
Type: Continuous ▾ Idle Time (sec):

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

Configuring PTM WAN DS-Lite connection

If you are a leased line with DS-Lite user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP.

If your ISP wants you to connect to the Internet using DS-Lite, follow the instructions below.

1. From the left-hand *WAN Settings* -> *PTM WAN* menu. The following page is displayed:
2. From the *Channel Mode* drop-down list, select *DS-Lite* setting.
3. Enable *Enable NAPT*
4. Select proper *Connection Type*
5. Enter *Local IPv6 Address*, *Remote IPv6 End point Address* and *Gateway IPv6 Address* which was given by Telecom or by your Internet Service Provider (ISP).
6. Click *Apply Changes*.

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

Channel Mode: DS-Lite ▾

Enable NAPT:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

802.1p_Mark

Enable QoS:

DS-Lite WAN config:

Local IPv6 Address:

Remote IPv6 End point Address:

Gateway IPv6 Address:

Apply Changes

Delete

Configuring PTM WAN 6rd connection

If you are a leased line with 6rd user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP.

If your ISP wants you to connect to the Internet using 6rd, follow the instructions below.

1. From the left-hand *WAN Settings* -> *PTM WAN* menu. The following page is displayed:
2. From the *Channel Mode* drop-down list, select *6rd* setting.
3. Enable *Enable NAPT*
4. Select proper *Connection Type*
5. Enter *Board Router v4 Address*, *6rd IPv4 Mask Len*, *6rd Prefix* (EX:"2001:db8::") and *6rd Prefix length* which was given by Telecom or by your Internet Service Provider (ISP).
6. Click *Apply Changes*.

PTM WAN

This page is used to configure the parameters for PTM WAN of your Router.

ptm0_0 ▾

Enable VLAN:

VLAN ID:

802.1p_Mark

Channel Mode: 6rd ▾

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type: INTERNET_TR069 ▾

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

6rd Config:

Board Router v4 Address:

6rd IPv4 Mask Len:

6rd Prefix (EX:"2001:db8::"):

6rd Prefix length:

10 ATM WAN

This chapter describes how to configure the way that your device connects to the Internet. Your ISP determines what type of Internet access you should use and provides you with any information that you need in order to configure the Internet access to your device.

Your device needs the following address information in order to access the Internet:

ATM PVC	<p>To configure ATM PVC, enter the VPI and VCI provided by ISP. Select the Service Type Index, Service Category and enter the following information:</p> <ul style="list-style-type: none">• Peak Cell Rate• Sustainable Cell Rate• Maximum Burst Size
Channel Mode	<p>To configure the connection type, select the protocol and encapsulation type as indicated by ISP. Supported Protocol types are:</p> <ul style="list-style-type: none">• RFC1483 Bridged• RFC1483 MER• PPPoE• PPPoA• RFC1483 Routed <p>Supported Encapsulation types are:</p> <ul style="list-style-type: none">• VCMUX• LLC/SNAP
WAN IP Settings	<p>To configure WAN IP settings, enter the information as indicated by ISP. Enable/Disable the Access Concentrator option. Either enter the WAN IP or select the option to automatically obtain IP address.</p> <p>Check as applicable the following two options:</p> <ul style="list-style-type: none">• Enable NAT• Add default Route
Broadband Username and Password	<p>To configure Broadband Username and Password, enter the user name and password details. Also set the session establishment condition as one of the following:</p> <ul style="list-style-type: none">• Continuous

- Connect on demand. Enter the minutes after which the session must be disconnected, if no activity takes place.
- Manual. Enter the minutes after which the session must be disconnected, if no activity takes place.

In most cases, you **will not** need to configure your device with these addresses because your ISP is likely to use an Internet access type which automatically assigns addresses to your device. For more information, see *Types of Internet Access*.

Types of DSL WAN Internet Access

The types of DSL WAN Internet access available are as follows:

- PPP Internet access – your device uses a Point to Point Protocol (PPP) to carry data between your ISP and your computer. To use PPP Internet access, you must enter a PPP login username and password the first time to log on. The IP addresses required to access your ISP's Internet service are automatically configured.
Your device supports PPPoE (over Ethernet).
- PPP Internet access – your device uses a Point to Point Protocol (PPP) to carry data between your ISP and your computer. To use PPP Internet access, you must enter a PPP login username and password the first time to log on. The IP addresses required to access your ISP's Internet service are automatically configured.
Your device supports PPPoA (over ATM).
- Bridged Internet access – your device uses a Bridge mode with your PPPoE Client Software to carry data between your ISP and your computer. To use Bridged Internet access with your PPPoE Client Software, you must enter a PPP login username and password the first time to log on. The IP addresses required to access your ISP's Internet service are automatically configured.
Your device supports RFC 1483 Bridged Mode).

Configuring your PPPoE DSL connection

If your ISP's Internet service uses PPPoE you need to set up a PPP login account. The first time that you login to the Internet, your ISP will ask you to enter a username and password so they can check that you are a legitimate, registered Internet service user. Your device stores these authentication details, so you will not have to enter this username and password every time you login.

Your ISP may also tell you to set unique path and circuit numbers (called VPI and VCI) in order to connect your device to the ISP's Internet service. In most cases, your device will use default settings, so you may not need to enter these values.



Note

Your ISP will provide you with the login details and VPI/VCI values necessary to set up a PPP login account.

If your ISP wants you to connect to the Internet using PPP, follow the instructions below.

7. From the left *WAN* menu, click on *ATM WAN*. The following page is displayed:
8. Enter VCI and VPI setting determined by your ISP.
9. Select the Encapsulation determined by your ISP.
10. From the *Channel Mode* drop-down list, select *PPPoE* setting.
11. Enable *Enable NAPT*
12. Select proper *Connection Type*
13. From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.
14. Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.
15. Configure IPv6 WAN setting determined by your ISP.
16. If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:

Encapsulation: LLC VC-Mux Channel Mode: ▼

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type: ▼

Enable VLAN: Disable Enable

VLAN ID(0-4095):

802.1p_Mark: ▼

IP Protocol: ▼

PPP Settings: User Name:

Password:

Type: ▼ Idle Time (sec):

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

17. Your configuration is complete.
18. Now you are ready to Surf the Internet !!!

Configuring your PPPoA DSL connection

If your ISP's Internet service uses PPPoA you need to set up a PPP login account. The first time that you login to the Internet, your ISP will ask you to enter a username and password so they can check that you are a legitimate, registered Internet service user. Your device stores these authentication details, so you will not have to enter this username and password every time you login.

Your ISP may also tell you to set unique path and circuit numbers (called VPI and VCI) in order to connect your device to the ISP's Internet service. In most cases, your device will use default settings, so you may not need to enter these values.



Note

Your ISP will provide you with the login details and VPI/VCI values necessary to set up a PPP login account.

If your ISP wants you to connect to the Internet using PPP, follow the instructions below.

1. From the left *WAN* menu, click on *ATM WAN*. The following page is displayed:

2. Enter VCI and VPI setting determined by your ISP.
3. Select the Encapsulation determined by your ISP.
4. From the *Channel Mode* drop-down list, select *PPPoA* setting.
5. Enable *Enable NAPT*
6. Select proper *Connection Type*
7. From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.
8. Enter *User Name/Password* provided by your ISP. Type them in the relevant boxes.
9. Configure IPv6 WAN setting determined by your ISP.
10. If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: **VCI:**
Encapsulation: LLC VC-Mux **Channel Mode:**

Enable NAPT: **Enable QoS:**

Admin Status: Enable Disable

Connection Type:

Enable VLAN: Disable Enable
 VLAN ID(0-4095):
802.1p Mark:

IP Protocol:

PPP Settings: User Name: **Password:**

Type: **Idle Time (sec):**

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

11. Your configuration is complete.
12. Now you are ready to Surf the Internet !!!

Configuring your Bridged DSL connection

1. From the left *WAN* menu, click on *ATM WAN*. The following page is displayed:
2. Enter VCI and VPI setting determined by your ISP.
3. Select the Encapsulation determined by your ISP.
4. From the *Channel Mode* drop-down list, select *1483 Bridged* setting.
5. Select proper *Connection Type*
6. If you are happy with your settings, click *Add*

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:

Encapsulation: LLC VC-Mux Channel Mode: ▼

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type: ▼

Enable VLAN: Disable Enable

VLAN ID(0-4095):

802.1p_Mark:

7. Now you can load your PPPoE Client Software onto your PC.
8. Now you can load your PPPoE Client Software with *user name* and *password* which determined by your ISP onto your PC.

Configuring your 1483 MER by DHCP

1. From the left *WAN* menu, click on *ATM WAN*. The following page is displayed:
2. Enter VCI and VPI setting determined by your ISP.
3. Select the Encapsulation determined by your ISP.
4. From the *Channel Mode* drop-down list, select *1483 MER* setting.
5. Enable *Enable NAPT*
6. Select proper *Connection Type*
7. From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.
8. From the *Type ratio*, click *DHCP*.
9. IPv6 WAN setting determined by your ISP.
10. If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:

Encapsulation: LLC VC-Mux Channel Mode:

Enable NAPT:

Enable QoS:

Admin Status: Enable Disable

Connection Type:

Enable VLAN: Disable Enable

VLAN ID(0-4095):

802.1p_Mark:

IP Protocol:

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

11. Your configuration is complete.
12. Now you are ready to Surf the Internet !!!

Configuring your 1483 MER by Fixed IP

1. From the left *WAN* menu, click on *ATM WAN*. The following page is displayed:

2. Enter VCI and VPI setting determined by your ISP.
3. Select the Encapsulation determined by your ISP.
4. From the *Channel Mode* drop-down list, select *1483 MER* setting.
5. Enable *Enable NAPT*
6. Select proper *Connection Type*
7. From the *IP Protocol* drop-down list, select the IP Protocol, IPv4, IPv6 or dual stacks IPv4/IPv6 determined by your ISP.
8. From the *Type ratio*, click *Fixed IP*.
9. Enter *Local IP Address*, *Subnet Mask* and *Remote IP Address* which was given by Telecom or by your Internet Service Provider (ISP).
10. IPv6 WAN setting determined by your ISP.
11. If you are happy with your settings, click Add

DSL WAN Configuration

This page is used to configure the parameters for DSL WAN of your Router.

VPI: VCI:

Encapsulation: LLC VC-Mux Channel Mode:

Enable NAPT:

Admin Status: Enable Disable

Enable QoS:

Connection Type:

Enable VLAN: Disable Enable

VLAN ID(0-4095):

802.1p_Mark:

IP Protocol:

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

Unnumbered

IPv6 WAN Setting:

Address Mode: Slaac Static

Enable DHCPv6 Client:

Request Options:

Request Address

Request Prefix

1. From the left *Service* menu, click on *DHCP*.
2. Check on Set Manually ratio.
3. Enter DNS setting determined by your ISP.
4. Click *Apply Changes* button.

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: —

Subnet Mask:

Max Lease Time: **seconds (-1 indicates an infinite lease)**

Domain Name:

Gateway Address:

DNS option: Use DNS Relay Set Manually

DNS1:

DNS2:

DNS3:

5. Click *OK* button.

Change setting successfully!

6. Your configuration is complete.

7. Now you are ready to Surf the Internet !!!

ATM Settings

The page is for ATM PVC QoS parameters setting. The DSL device support 4 QoS mode —CBR/rt-VBR/nrt-VBR/UBR.

1. From the left-hand *WAN* menu, click on *ATM*. The following page is displayed:

ATM Settings

This page is used to configure the parameters for the ATM of your Router. Here you may change the setting for VPI, VCI, QoS etc ...

VPI: VCI: QoS:

PCR: CDVT: SCR: MBS:

Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
--------	-----	-----	-----	-----	------	-----	-----

Field	Description
-------	-------------

VPI	Virtual Path Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through to the ATM switch.
QoS	Quality of Server, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are: –UBR (Unspecified Bit Rate): When UBR is selected, the SCR and MBS fields are disabled. –CBR (Constant Bit Rate): When CBR is selected, the SCR and MBS fields are disabled. –nrt-VBR (non-real-time Variable Bit Rate): When nrt-VBR is selected, the SCR and MBS fields are enabled. –rt-VBR (real-time Variable Bit Rate): When rt-VBR is selected, the SCR and MBS fields are enabled.
PCR	Peak Cell Rate, measured in cells/sec., is the cell rate which the source may never exceed.
SCR	Sustained Cell Rate, measured in cells/sec., is the average cell rate over the duration of the connection.
MBS	Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.

Function Button	Description
Apply Changes	Set new PVC OoS mode for the selected PVC. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.
Undo	Discard your settings.

DSL Settings

The DSL setting page allows you to select any combination of DSL training modes.

1. From the left-hand *WAN* menu, click on *DSL Settings*. The following page is displayed:

DSL Settings

This page is used to configure the parameters for the bands of your Router.

DSL Modulation:

- G.Dmt
- ADSL2
- ADSL2+
- VDSL2

VDSL2 Profile:

- 8a
- 8b
- 8c
- 8d
- 12a
- 12b
- 17a
- 30a

ADSL Capability:

- Enable Bitswap
- Enable SRA

Apply Changes

Field	Description
ADSL modulation	Choose preferred xdsl standard protocols. G.lite : G.992.2 Annex A G.dmt : G.992.1 Annex A T1.413 : T1.413 issue #2 ADSL2 : G.992.3 Annex A ADSL2+ : G.992.5 Annex A
AnnexL Option	Enable/Disable ADSL2/ADSL2+ Annex L capability.
AnnexM Option	Enable/Disable ADSL2/ADSL2+ Annex M capability.
VDSL2	Choose preferred xdsl standard protocols: 8a/8b/8c/8d/12a/12b/17a/30a
ADSL Capability	"Bitswap Enable" : Enable/Disable bitswap capability. "SRA Enable" : Enable/Disable SRA (seamless rate adaptation) capability.
Function Button	Description
Tone Mask	Choose tones to be masked. Mased tones will not carry any data.
Apply Changes	Click to save the setting to the configuration and the modem will be retrained.

11 DHCP Settings

You can configure your network and DSL device to use the Dynamic Host Configuration Protocol (DHCP). This page provides DHCP instructions for implementing it on your network by selecting the role of DHCP protocol that this device wants to play. There are two different DHCP roles that this device can act as: DHCP Server and DHCP Relay. When acting as DHCP server, you can setup the server parameters at the **DHCP Server** page; while acting as DHCP Relay, you can setup the relay at the **DHCP Relay** page.

DHCP Server Configuration

1. From the left-hand *Services* menu, click on *DHCP*.
2. From *DHCP Mode* check radio, click on *DHCP Server*.
3. Type a new IP Pool Range, Subnet Mask, Max Lease Time, Domain Name and Gateway Address.
4. Click on *Apply Changes*.

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: -

Subnet Mask:

Max Lease Time: seconds (-1 indicates an infinite lease)

Domain Name:

Gateway Address:

DNS option: Use DNS Relay Set Manually

Field	Description
IP Pool Range	Specify the lowest and highest addresses in the pool.
Max Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 86400 seconds (1 day). The value -1 stands for the infinite lease.
Domain Name	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.
MAC-Based Assignment	Configure the static IP base on MAC Address. You can assign/delete the static IP.

5. Click *OK* button.

Change setting successfully!



DHCP Relay Configuration

1. From the left-hand *Services* menu, click on *DHCP*.
2. From *DHCP Mode* check ratio, click on *DHCP Relay*.
3. Type DHCP server IP Addresses.
4. Click on *Apply Changes*.

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

This page is used to configure the DHCP Server IP Address for DHCP Relay.

DHCP Server IP Address:

Field	Description
DHCP Server Address	Specify the IP address of your ISP's DHCP server. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.
Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

5. Click *OK* button.

Change setting successfully!

6. You need to renew your DHCP lease:

Windows 95/98

- a. Select **Run...** from the **Start** menu.
- b. Enter **winipcfg** and click **OK**.
- c. Select your ethernet adaptor from the pull-down menu
- d. Click **Release All** and then **Renew All**.
- e. **Exit** the winipcfg dialog.

Windows NT/Windows 2000/Windows XP

- a. Bring up a command window.
- b. Type **ipconfig /release** in the command window.
- c. Type **ipconfig /renew**.
- d. Type **exit** to close the command window.

Linux

- a. Bring up a shell.
- b. Type **pump -r** to release the lease.
- c. Type **pump** to renew the lease.

DHCP None Configuration

1. From the left-hand *Services* menu, click on *DHCP*.
2. From *DHCP Mode* check ratio, click on *None*.
3. Click on *Apply Changes*.

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode: None DHCP Relay DHCP Server

Apply Changes

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

4. Click *OK* button.

Change setting successfully!

OK

12 DHCPv6 Settings

You can configure your network and DSL device to use the Dynamic Host Configuration Protocol (DHCP). This page provides DHCP instructions for implementing it on your network by selecting the role of DHCP protocol that this device wants to play. There are two different DHCP roles that this device can act as: DHCP Server and DHCP Relay. When acting as DHCP server, you can setup the server parameters at the **DHCP Server** page; while acting as DHCP Relay, you can setup the relay at the **DHCP Relay** page.

DHCP Server (Manual) Configuration

1. From the left-hand *Advance* menu, click on *IPv6 - DHCPv6*.
2. From *DHCPv6 Mode* check radio, click on *DHCP Server (Manual)*.
3. Type a new IP Pool Range and Prefix Length.
4. Click on *Apply Changes*.

DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: None DHCP Relay
 DHCP Server (Manual) DHCP Server (Auto)

Enable the DHCPv6 Server if you are using this device as a DHCPv6 server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

IP Pool Range: -

Prefix Length:

Valid Lifetime: **seconds**

Preferred Lifetime: **seconds**

Renew Time: **seconds**

Rebind Time: **seconds**

Client DUID:

Domain:

Domain Search Table:

Select	Domain
<input type="checkbox"/>	

Name Server IP:

Name Server Table:

Select	Name Server
<input type="checkbox"/>	

Field	Description
IP Pool Range	Specify the lowest and highest addresses in the pool.
Prefix Length	Configure Prefix Length
Valid Lifetime	Configure Valid Lifetime
Preferred Lifetime	Configure Preferred Lifetime
Renew Time	Configure Renew Time
Rebind Time	Configure Rebind Time
Client DUID	Configure Client DUID
Domain Name	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

5. Click *OK* button.

Change setting successfully!



DHCP Server (Auto) Configuration

1. From the left-hand *Services* menu, click on *DHCPv6*.
2. From *DHCPv6 Mode* check ratio, click on *DHCP Server (Auto)*.
3. Click on *Apply Changes*.

DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: None DHCP Relay
 DHCP Server (Manual) DHCP Server (Auto)

Auto Config by Prefix Delegation for DHCPv6 Server:

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

4. Click *OK* button.

Change setting successfully!

DHCP Relay Configuration

1. From the left-hand *Services* menu, click on *DHCP*.
2. From *DHCPv6 Mode* check ratio, click on *DHCP Relay*.
3. Configure the *Upper Interface* (server link).
4. Click on *Apply Changes*.

DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: None DHCP Relay
 DHCP Server (Manual) DHCP Server (Auto)

This page is used to configure the upper interface (server link) for DHCPv6 Relay.

Upper Interface:

ptm0_0 ▼

Apply Changes

Field	Description
Upper Interface	Configure the upper interface (server link)

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

5. Click *OK* button.

Change setting successfully!

OK

6. You need to renew your DHCP lease:

Windows 95/98

- a. Select **Run...** from the **Start** menu.
- b. Enter **winipcfg** and click **OK**.
- c. Select your ethernet adaptor from the pull-down menu
- d. Click **Release All** and then **Renew All**.
- e. **Exit** the winipcfg dialog.

Windows NT/Windows 2000/Windows XP

- a. Bring up a command window.
- b. Type **ipconfig /release** in the command window.
- c. Type **ipconfig /renew**.
- d. Type **exit** to close the command window.

Linux

- a. Bring up a shell.
- b. Type **pump -r** to release the lease.
- c. Type **pump** to renew the lease.

DHCP None Configuration

1. From the left-hand *Services* menu, click on *DHCP*.
2. From *DHCPv6 Mode* check ratio, click on *None*.
3. Click on *Apply Changes*.

DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: None DHCP Relay
 DHCP Server (Manual) DHCP Server (Auto)

Apply Changes

Function Button	Description
Apply Changes	Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

4. Click *OK* button.

Change setting successfully!

OK

13 DNS Configuration

This page is used to configure the DNS server ip addresses for DNS Relay.

DHCP Server Configuration - Attain DNS Automatically

1. From the left *Services* menu, click on *DNS -> DNS Server*.
2. From check ratio, click on *Attain DNS Automatically*.
3. Click on *Apply Changes*.

DNS Configuration

This page is used to configure the DNS Server IP addresses.

- Attain DNS Automatically
 Set DNS Manually

Apply Changes

Field	Description
Attain DNS Automatically	Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.
Set DNS Manually	Select this item to configure up to three DNS IP addresses.

Function Button	Description
Apply Changes	Set new DNS relay configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

4. Click *OK* button.

Change setting successfully!

OK

DHCP Server Configuration - Set DNS Manually

1. From the left *Services* menu, click on *DNS -> DNS Server*.
2. From check ratio, click on *Set DNS Manually*.
3. Enter the IP Address of DNS.
4. Click on *Apply Changes*.

DNS Configuration

This page is used to configure the DNS Server IP addresses.

Attain DNS Automatically
 Set DNS Manually

IPv4 WAN Interface Binding:

DNSv4 1:

DNSv4 2:

DNSv4 3:

IPv6 WAN Interface Binding:

DNSv6 1:

DNSv6 2:

DNSv6 3:

Field	Description
IPv4 WAN Interface Binding	Enable or disable IPv4 WAN Interface Binding
DNSv4 1/2/3	Select this item to configure up to three DNSv4 IP addresses.
IPv6 WAN Interface Binding	Enable or disable IPv6 WAN Interface Binding
DNSv6 1/2/3	Select this item to configure up to three DNSv6 IP addresses.

Function Button	Description
Apply Changes	Set new DNS relay configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

5. Click *OK* button.

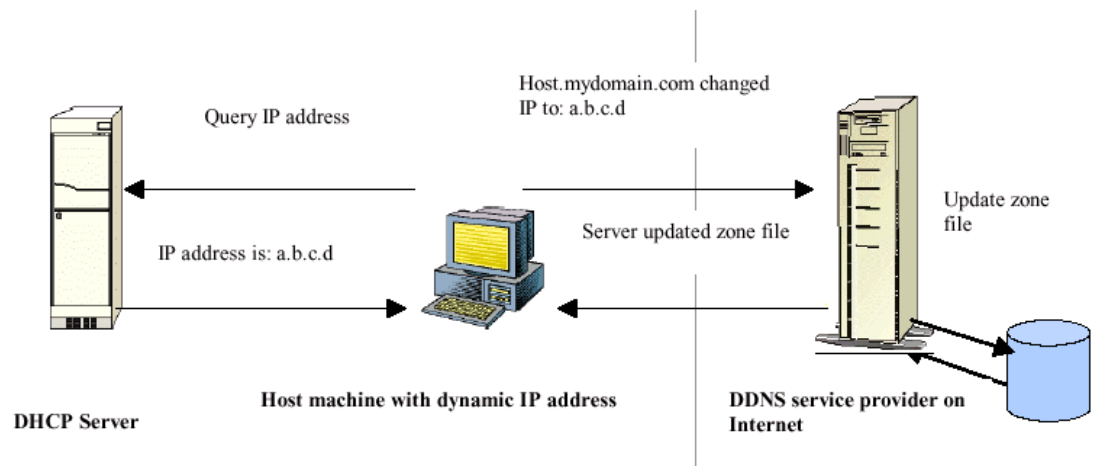
Change setting successfully!

OK

14 Dynamic DNS Configuration

Overview of Dynamic DNS

If some host has a dynamic IP address that keeps changing frequently, it is difficult to keep updating the IP record that is associated with the domain name of this host in the zone files. This will result in non-accessibility of this host on the Internet. Dynamic DNS service allows to keep mapping of a dynamic IP address of such host to a static hostname. Dynamic DNS services are provided by many websites. The host needs to register with some website and get a domain name. When the IP address of the host changes, it just needs to send a message to the website that's providing dynamic DNS service to this host. For this to work, an automated update client needs to be implemented. These update clients send update messages to the servers whenever there is some change in the IP address of that host. Then, the server updates the entries for that host and replies back with some return code.



Above Figure explains one such scenario in which a host gets a dynamic IP address for itself from a DHCP server. As the host has registered with one of the dynamic DNS service providers on the Internet, it sends an update message to the service provider with host name and changed IP address. The service provider updates the new IP address of the host in the zone files that have entry for that host name and replies back with some return code. The return code communicates the success or failure of the update message. This process is repeated every time the host's IP address changes.

If the dynamic DNS service provider is notified of the same IP address again and again, then it considers it an abuse and might block the host name. To avoid this scenario, the IP address that was successfully updated to the ISP is stored on the unit. Whenever we receive an IP address change notification, the new IP address is compared with the IP address that was stored on the last update. If they differ, then only an

update request is sent. However, when the system comes up there is no way of knowing what was the IP address on last successful update before the system went down. You need to give the command "system config save" periodically to save this IP address on Flash.

Registering With Dynamic DNS Service Provider

Currently, VDSL2 Router supports two Dynamic DNS service providers, www.tzo.com and www.dyndns.com. To use their Dynamic DNS service, you first need to visit the Web site of a service provider and register. While registering, you need to provide your username, password, and hostname as mandatory parameters. A service provider may also prompt you to fill some optional parameters.

Configuring IP Interfaces

You need to create a Dynamic DNS interface per IP interface and can only create one Dynamic DNS interface service on one IP interface. For more information on creating IP interfaces, refer to section Creating IP interfaces.



Note

www.dyndns.org provides three kinds of services - Dynamic DNS, Custom DNS and Static DNS. You can create different domains in these systems. Custom DNS service is a full DNS solution for newly purchased domains or domains you already own. A web-based interface provides complete control over resource records and your entire domain, including support for dynamic IPs and automated updates. Static DNS service points a DNS hostname in some domain owned by dyndns.org to the user's ISP-assigned static or pseudo-static IP address.

DynDNS service points a fixed hostname in some domain owned by dyndns.org to the user's ISP-assigned dynamic IP address. This allows more frequent update of IP addresses, than allowed by Static DNS.

Dynamic DNS Configuration – DynDNS.org

1. From the left *Services* menu, click on *DNS -> Dynamic DNS*.
2. Check the *Enable* check box.
3. From *DDNS provider* drop-down list, select *DynDNS.org*.
4. Enter the *Hostname*.
5. Enter the *Username*.
6. Enter the *Password*.
7. Click *Add* button.

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

Enable:

DDNS Provider:

Hostname:

Interface:

DynDns Settings:

User Name:

Password:

TZO Settings:

Email:

Key:

Field	Description
Enable	Check this item to enable this registration account for the DNS server.
DDNS provider	There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO . A charge may occur depends on the service you select.
Hostname	Domain name to be registered with the DDNS server.
Username	User-name assigned by the DDNS service provider.
Password	Password assigned by the DDNS service provider.

Function Button	Description
Add	Click Add to add this registration into the configuration.
Remove	Select an existing DDNS registration by clicking the radio button at the Select column of the Dynamic DNS Table . Click Remove button to remove the selected registration from the configuration.

8. Configure Dynamic DNS setting successfully!

Dynamic DNS Table:

Select	State	Hostname	User Name	Service	Status
<input type="radio"/>	Enable	test.dyndns.org	test	dyndns	Cannot connecting to provider

Dynamic DNS Configuration – TZO

1. From the left-hand *Services* menu, click on *DNS -> Dynamic DNS*.
2. From *DDNS provider* drop-down list, select *TZO*.
3. Enter the *Hostname*.
4. From *Interface* drop-down list, select proper one.
5. Check the *Enable* check box.
6. Enter the *Hostname*, *Email* and *Password*.
7. Click *Add* button.

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

Enable:

DDNS Provider:

Hostname:

Interface

DynDns Settings:

User Name:

Password:

TZO Settings:

Email:

Key:

Field	Description
Enable	Check this item to enable this registration account for the DNS server.
DDNS provider	There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO . A charge may occurs depends on the service you select.
Hostname	Domain name to be registered with the DDNS server.
Email	Email that applied for the DDNS service provider.
Key	Key assigned by the DDNS service provider.
Function Button	Description
Add	Click Add to add this registration into the configuration.
Modify	Click Modify to modify this registration into the configuration.
Remove	Select an existing DDNS registration by clicking the radio button at the Select column of the Dynamic DNS Table . Click Remove button to remove the selected registration from the configuration.

8. Configure Dynamic DNS setting successfully!

Dynamic DNS Table:

Select	State	Hostname	User Name	Service	Status
<input type="radio"/>	Enable	test.tzo.net	test@gmail.com	tzo	Cannot connecting to provider

15 IP/Port Filtering

Firewall contains several features that are used to deny or allow traffic from passing through the device.

The IP/Port filtering feature allows you to deny/allow specific services or applications in the forwarding path.

IP/Port Filtering

1. From the left *Services* menu, click on *Firewall -> IP/Port Filtering*.

IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action Deny Allow
Incoming Default Action Deny Allow

Direction: **Protocol:** **Rule Action** Deny Allow
Source IP Address: **Subnet Mask:** **Port:** -
Destination IP Address: **Subnet Mask:** **Port:** -

Current Filter Table:

Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action
--------	-----------	----------	-------------------	-------------	------------------------	------------------	-------------

Fields on the first setting block	Description
Outgoing Default Action	Specify the default action on the LAN to WAN forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN forwarding path.
Function Button	Description
Apply Changes	Click to save the setting of default actions to the configuration.
Fields on the second setting block	Description

Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic forwarding direction.
Protocol	There are 3 options available: TCP, UDP and ICMP.
Source IP Address	The source IP address assigned to the traffic on which filtering is applied.
Source Subnet Mask	Subnet-mask of the source IP.
Source Port	Starting and ending source port numbers.
Destination IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Destination Subnet Mask	Subnet-mask of the destination IP.
Destination Port	Starting and ending destination port numbers.
Function Button	Description
Add	Click to save the rule entry to the configuration.
Delete Selected	Delete selected filtering rules from the filter table. You can click the checkbox at the Select column to select the filtering rule.
Delete All	Delete all filtering rules from the filter table.

16 MAC Filtering

The MAC filtering feature allows you to define rules to allow or deny frames through the device based on source MAC address, destination MAC address, and traffic direction.

Configuring MAC filtering to Deny for outgoing access

2. From the left *Services* menu, click on *Firewall -> MAC Filtering*.
3. From the *Direction* drop-down list, select *Outing* setting
4. From the *Rule Action* check ratio, select *Deny*
5. Enter the MAC Address that you want to deny for outgoing access in the *Source MAC Address*
6. Click *Add*

MAC Filtering for bridge mode

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action Deny Allow
Incoming Default Action Deny Allow Apply Changes

Direction: Outgoing ▾
Source MAC Address: 001333000001
Destination MAC Address:
Rule Action Deny Allow Add

Current Filter Table:

Select	Direction	Source MAC Address	Destination MAC Address	Rule Action
Delete Selected Delete All				

7. Configure MAC filtering setting successfully!

Current Filter Table:

Select	Direction	Source MAC Address	Destination MAC Address	Rule Action
<input type="checkbox"/>	Outgoing	00-13-33-00-00-01	-----	Deny
Delete Selected Delete All				

Fields on the first setting block	Description
Outgoing Default Action	Specify the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN bridging/forwarding path.
Function Button	Description
Apply Changes	Click to change the setting of default actions to the configuration.

Fields on the second setting block	Description
Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic bridging/forwarding direction.
Source MAC Address	The source MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.
Destination MAC Address	The destination MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.
Function Button	Description
Delete Selected	Delete selected filtering rules from the filter table. You can click the checkbox at the Select column to select the filtering rule.
Delete All	Delete all filtering rules from the filter table.

17 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Your device has built in advanced Security features that protect your network by blocking unwanted traffic from the Internet.

If you simply want to connect from your local network to the Internet, you do not need to make any changes to the default Security configuration. You only need to edit the configuration if you wish to do one or both of the following:

- allow Internet users to browse the user pages on your local network (for example, by providing an FTP or HTTP server)
- play certain games which require accessibility from the Internet

This chapter describes how to configure Security to suit the needs of your network.

By default, the IP addresses of your LAN PCs are hidden from the Internet. All data sent from your LAN PCs to a PC on the Internet appears to come from the IP address of your device.

In this way, details about your LAN PCs remain private. This security feature is called *Port Forwarding*.

1. From the left *Services* menu, click on *Firewall -> Port Forwarding*.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding: Disable Enable

Enable Application:

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾

Current Port Forwarding Table:

Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface
--------	---------------	------------	----------	------------	--------	-------------	-------------	-----------

Port Forwarding for TCP with specified IP

Please follow example below to configure the Port Forwarding to Specified IP with TCP.

1. From the left *Services* menu, click on *Firewall -> Port Forwarding*.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding: Disable Enable

Enable Application:

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any

Current Port Forwarding Table:

Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface
--------	---------------	------------	----------	------------	--------	-------------	-------------	-----------

2. Check the option *Enable Port Forwarding* to enable the Enable Port Forwarding.
3. Click *Apply Changes*.
4. Enter any comment in *Comment* field.
5. Enter the IP Address and port you want to be forwarded in *IP Address / Local Port from / Local Port to* field.
6. From the *Protocol* drop-down list, select *TCP* setting.
7. Click *Add*.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding: Disable Enable

Enable Application:

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
HTTP	192.168.1.178	80	80	TCP				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any

Current Port Forwarding Table:

Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface
--------	---------------	------------	----------	------------	--------	-------------	-------------	-----------

8. Now the IP Address and port range that you created has been added and listed in the *Current Filter Table*.
9. Now the port range of the IP Address in the *Current Filter Table* can be access from Internet by TCP protocol.

Current Port Forwarding Table:

Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface
<input type="checkbox"/>	HTTP	192.168.1.178	TCP+UDP	80	Enable		----	---

Port Forwarding for UDP with specified IP

Please follow example below to configure the Port Forwarding to Specified IP with UDP.

1. From the left *Services* menu, click on *Firewall -> Port Forwarding*.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding:
 Disable
 Enable

Enable
Application:

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾

Current Port Forwarding Table:

Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface
--------	---------------	------------	----------	------------	--------	-------------	-------------	-----------

2. Check the option *Enable Port Forwarding* to enable the Enable Port Forwarding.
3. Click *Apply Changes*.
4. Enter any comment in *Comment* field.
5. Enter the IP Address and port you want to be forwarded in *IP Address / Local Port from / Local Port to* field.
6. From the *Protocol* drop-down list, select *UDP* setting.
7. Click *Add*.

Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Port Forwarding: Disable Enable

Enable Application:

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
UDP	192.168.1.178	69	69	UDP				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any
				Both				Any

8. Now the IP Address and port range that you created has been added and listed in the *Current Filter Table*.
9. Now the port range of the IP Address in the *Current Filter Table* can be access from Internet by UDP protocol.

Current Port Forwarding Table:

Select	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface
<input type="checkbox"/>	UDP	192.168.1.178	UDP	69	Enable		----	---

18 URL Blocking

The URL Blocking is the web filtering solution. The firewall includes the ability to block access to specific web URLs based on string matches. This can allow large numbers of URLs to be blocked by specifying a Keyword. The URL Blocking enforce a Web usage policy to control content downloaded from, and uploaded to, the Web.

Configuring URL Blocking of FQDN

1. From the left *Services* menu, click on *Firewall -> URL Blocking*.

URL Blocking Configuration

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable Apply Changes

FQDN: Add

URL Blocking Table:

Select	FQDN
Delete Selected Delete All	

Keyword: Add

Keyword Filtering Table:

Select	Filtered Keyword
Delete Selected Delete All	

Fields on the first setting block	Description
URL Blocking	Check this item to enable the URL Blocking feature.
Keyword	The filtered keyword such as yahoo. If the URL includes this keyword, the URL will be blocked to access.

Function Button	Description
-----------------	-------------

Apply Changes	Click to disable/enable the URL Blocking capability
Add FQDN	Add FQDN into URL Blocking table.
Delete Selected FQDN	Delete the selected FQDN from the URL Blocking table. You can click the checkbox at the Select column to select the Blocked FQDN.
Add Filtered Keyword	Add filtered keyword into Keyword Filtering table.
Delete Selected Keyword	Delete the selected keyword from the keyword Filtering table. You can click the checkbox at the Select column to select the filtered keyword.

2. From the *URL Blocking* check ratio, check on *Enable*
3. Click *Apply Changes*
4. Type the FQDN in the FQDN field.
5. Click *Add*

URL Blocking Configuration

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable

FQDN:

URL Blocking Table:

Select	FQDN
<input type="checkbox"/>	google.com

Keyword:

Keyword Filtering Table:

Select	Filtered Keyword
<input type="checkbox"/>	

6. Configure URL Blocking of FQDN setting successfully!

URL Blocking Table:

Select	FQDN
<input type="checkbox"/>	google.com

Configuring URL Blocking of Keyword

1. From the left *Services* menu, click on *Firewall -> URL Blocking*.

URL Blocking Configuration

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable Apply Changes

FQDN: Add

URL Blocking Table:

Select	FQDN
--------	------

Delete Selected Delete All

Keyword: Add

Keyword Filtering Table:

Select	Filtered Keyword
--------	------------------

Delete Selected Delete All

Fields on the first setting block	Description
URL Blocking	Check this item to enable the URL Blocking feature.
Keyword	The filtered keyword such as yahoo. If the URL includes this keyword, the URL will be blocked to access.

Function Button	Description
Apply Changes	Click to disable/enable the URL Blocking capability
Add FQDN	Add FQDN into URL Blocking table.
Delete Selected FQDN	Delete the selected FQDN from the URL Blocking table. You can click the checkbox at the Select column to select the Blocked FQDN.
Add Filtered Keyword	Add filtered keyword into Keyword Filtering table.
Delete Selected Keyword	Delete the selected keyword from the keyword Filtering table. You can click the checkbox at the Select column to select the filtered keyword.

2. From the *URL Blocking* check ratio, check on *Enable*
3. Click *Apply Changes*
4. Type the Keyword in the Keyword field.
5. Click *Add*

URL Blocking Configuration

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: Disable Enable

FQDN:

URL Blocking Table:

Select	FQDN
<input type="checkbox"/>	google.com

Keyword:

Keyword Filtering Table:

Select	Filtered Keyword
--------	------------------

6. Configure URL Blocking of Keyword setting successfully!

Keyword Filtering Table:

Select	Filtered Keyword
<input type="checkbox"/>	yao0

19 Domain Blocking

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Configuring Domain Blocking

1. From the left *Services* menu, click on *Firewall -> Domain Blocking*.

Domain Blocking Configuration

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Domain Blocking: Disable Enable

Domain:

Domain Blocking Configuration:

Select	Domain
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>

Fields on the first setting block	Description
Domain Blocking	Check this item to enable the Domain Blocking feature.
Domain	The Domain such as www.yahoo.com. If the URL includes this domain, the domain will be blocked to access.

Function Button	Description
Apply Changes	Click to disable/enable the URL Blocking capability
Add FQDN	Add FQDN into URL Blocking table.
Delete Selected	Delete the selected Domain Blocking from the Domain Blocking table. You can click the checkbox at the Select column to select the Blocked Domain.

2. From the *Domain Blocking* check ratio, check on *Enable*
3. Click *Apply Changes*
4. Type the Domain in the Domain field.
5. Click *Add*

Domain Blocking Configuration

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

Domain Blocking: Disable Enable

Domain:

Domain Blocking Configuration:

Select	Domain
--------	--------

6. Configure URL Blocking of FQDN setting successfully!

Domain Blocking Configuration:

Select	Domain
<input type="checkbox"/>	www.google.com

20 DMZ

A demilitarized zone (DMZ) is a host or small network that acts as neutral ground between the inside and outside network. It contains information that is useful to users of both the inside and outside network. For example, a company may wish to provide software patches to customers via an FTP server. However, it does not want FTP access to any hosts other than the FTP server. This is achieved by creating a DMZ network which is less restrictive than the internal network. Users attached to the outside network can access the DMZ, but they cannot access any other company data.

Configuring DMZ

1. From the left *Services* menu, click on *Firewall -> DMZ*.

DMZ Configuration

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ Host: Disable Enable

DMZ Host IP Address:

Fields on the first setting block	Description
DMZ Host	Check this item to enable the DMZ feature.
DMZ Host IP Address	IP address of the local host. This feature sets a local host to be exposed to the Internet.
Function Button	Description
Apply Changes	Click to change the setting to the configuration.

2. From the *DMZ Host* check ratio, check on *Enable*
3. Type the IP Address in the *DMZ Host IP Address* field.
4. Click *Apply Changes*

DMZ Configuration

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ Host: Disable Enable

DMZ Host IP Address:

5. Click *OK* button.

Change setting successfully!

21 UPnP

UPnP is an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, Wireless devices, and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet. UPnP is a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.

UPnP is more than just a simple extension of the plug and play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. This means a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS servers are optional and are used only if available on the network. Finally, a device can leave a network smoothly and automatically without leaving any unwanted state behind.

The DSL device supports a control point for Universal Plug and Play (UPnP) version 1.0, and supports two key features: **NAT Traversal** and **Device Identification**. This feature requires one active WAN interface. In addition, the host should support this feature. In the presence of multiple WAN interfaces, select an interface on which the incoming traffic is present.

With NAT Traversal, when an UPnP command is received to open ports in NAT, the application translates the request into system commands to open the ports in NAT and the firewall. The interface to open the ports on is given to UPnP when it starts up and is part of the configuration of the application.

For Device Identification, the application will send a description of the DSL device as a control point back to the host making the request.

From the web page you can enable or disable UPnP.

Configuring UPnP

1. From the left *Services* menu, click on *UPnP*. The following page is displayed:

UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP: Disable Enable

TR-064: Disable Enable

WAN Interface:

Fields on the first setting block	Description
UPnP	Enable/disable UPnP feature.
WAN Interface	Select WAN interface that will use UPnP from the drop-down lists.

Function Button	Description
Apply Changes	Click to save the setting to the configuration.

2. From the *UPnP* check ratio, check on *Enable*
3. Select a WAN Interface from the *WAN Interface* drop-down list.
4. Click *Apply Changes*

UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP: Disable Enable

TR-064: Disable Enable

WAN Interface:

5. Click *OK* button.

Change setting successfully!

A rectangular button with a thin border and the text "OK" centered inside.

UPnP Control Point Software on Windows ME

To install the control point software on Windows ME:

1. In the Control Panel, select "Add/Remove Programs".
2. In the "Add/Remove Programs Properties" dialog box, select the "Windows Setup" tab. In the "Components" list, double click on the "Communications" entry.
3. In the "Communications" dialog box, scroll down the "Components" list to display the UPnP entry. Select the entry, click "OK".
4. Click "OK" to finish the "Add/Remove Programs" dialog.
5. Reboot your system.

Once you have installed the UPnP software and you have rebooted (and your network includes the IGD system), you should be able to see the IGD controlled device on your network.

UPnP Control Point Software on Windows XP with Firewall

On Windows XP versions earlier than SP2, Firewall support is provided by the Windows XP Internet Connection Firewall. You cannot use the Windows XP Internet Connection Firewall support on a system that you intend to use as a UPnP control point. If this feature is enabled, although the control point system may display controlled devices in the list of network devices, the control point system cannot participate in UPnP communication. (This restriction also applies to controlled devices running on Windows XP systems earlier than SP2.)

On Windows XP SP2 and later, Firewall support is provided by Windows Firewall. Unlike earlier versions, Windows XP SP2 can be used on a system that you intend to use as a UPnP control point.

To turn off the Firewall capability on any version of Windows XP, follow the steps below:

1. In the Control Panel, select "Network and Internet Connections".
2. In the "Network and Internet Connections" dialog box, select "Network Connections".
3. In the "Network Connections" dialog box, right-click on the local area connection entry for your network; this will display a menu. Select the "Properties" menu entry.

4. In the "Local Area Connection Properties" dialog box, select the "Advanced" tab. Disable the Internet Connection Firewall by de-selecting the entry with the following label:

"Protect my computer and network by limiting or preventing access to the computer from the Internet".

5. Click "OK".

SSDP requirements

You must have SSDP Discovery Service enabled on your Windows XP system to use the UPnP Control point software.

SSDP Discovery Service is enabled on a default installation of Windows XP. To check if it is enabled on your system, look in Control Panel > Administrative Tools > Services).

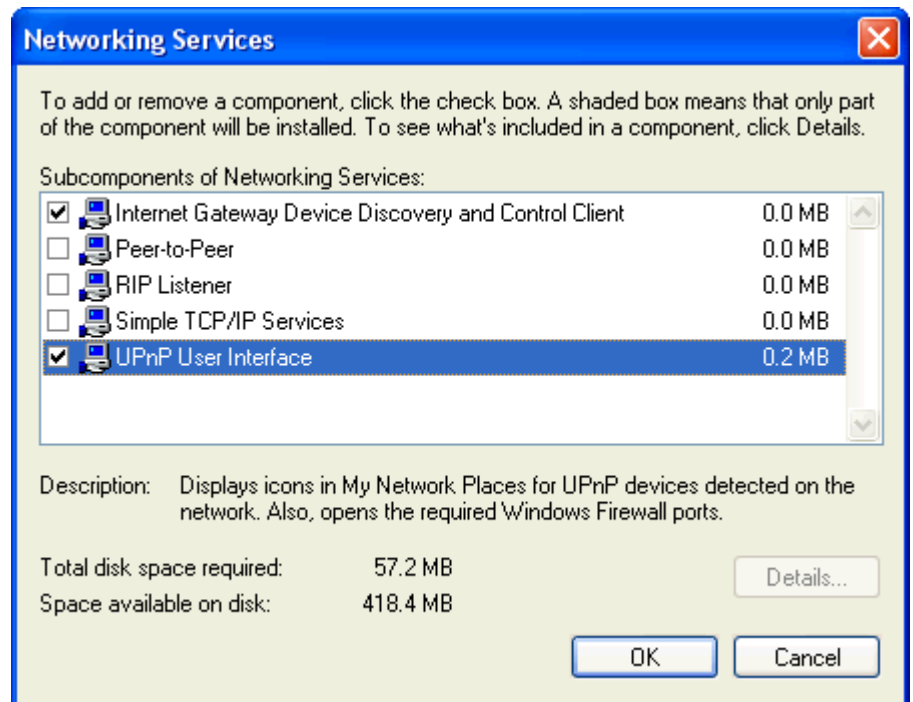
Installation procedure

To install the Control point software on Windows XP, follow the steps below:

1. In the Control Panel, select "Add/Remove Programs".
2. In the "Add or Remove Programs" dialog box, click the "Add / Remove Windows Components" button.
3. In the "Windows Component Wizard" dialog box, scroll down the list to display the "Networking Services" entry. Highlight (select) the entry, and click on the "Details" button.
4. The "Networking Services" window is displayed.

The subcomponents shown in the Networking Services window will be different depending on if you are using Windows XP, Windows XP (SP1), or Windows XP (SP2).

If you are using Windows XP SP2, the Networking Services window will display the following list of sub-components:



5. Select the following entries from the "Networking Services" window and then click "OK":

If you are using **Windows XP**, select:

- "Universal Plug and Play".

If you are using **Windows XP SP1**, select:

- "Internet Gateway Device discovery and Control Client".
- "Universal Plug and Play".

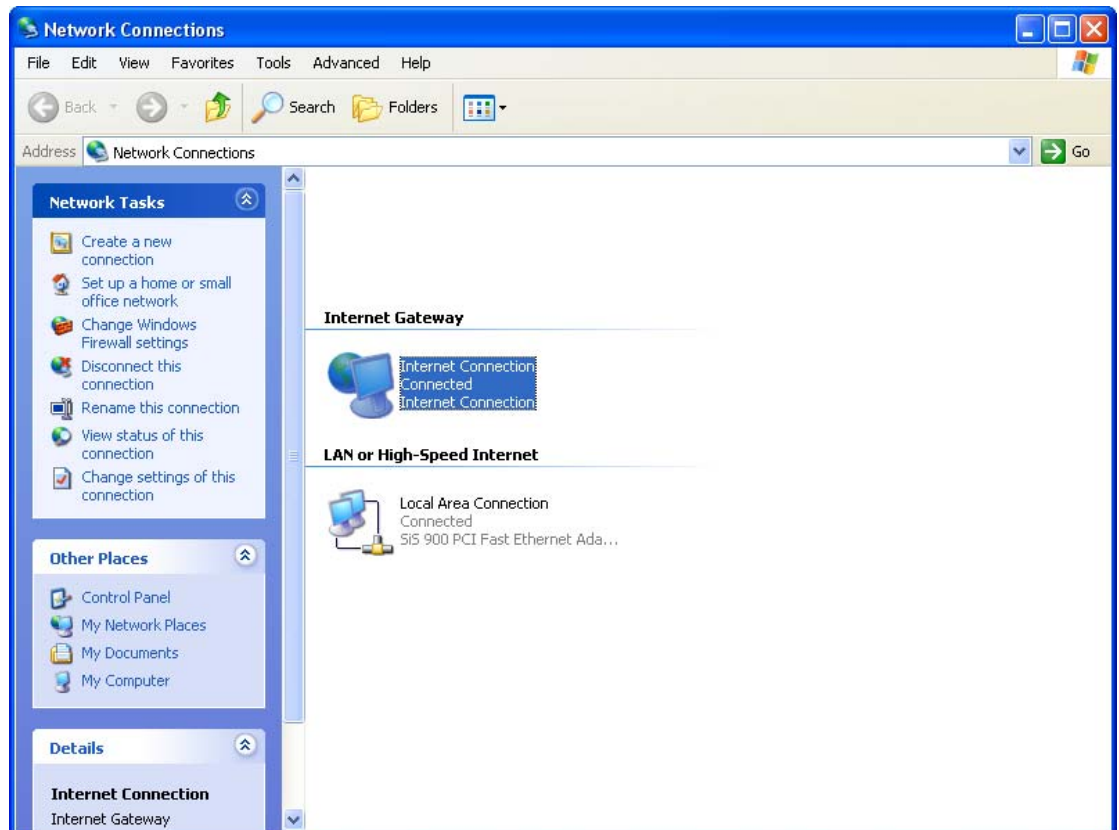
If you are using **Windows XP SP2**, select:

- "Internet Gateway Device discovery and Control Client".
- "UPnP User Interface".

6. Reboot your system.

Once you have installed the UPnP software and you have rebooted (and your network includes the IGD system), you should be able to see the IGD controlled device on your network.

For example, from the Network Connections window you should see the Internet Gateway Device:



22 RIP

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line.

Most small home or office networks do not need to use RIP; they have only one Router, such as the ADSL Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

-Your home network setup includes an additional Router or RIP-enabled PC (other than the ADSL Router). The ADSL Router and the Router will need to communicate via RIP to share their routing tables.

-Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.

-Your ISP requests that you run RIP for communication with devices on their network.

1. From the left *Advance* menu, click on *Route* -> *RIP*. The following page is displayed:

RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled Router to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device that use RIP, and the version of the protocol used.

RIP: Disable Enable

Apply Changes

Interface:

br0

Receive Mode:

None

Send Mode:

None

Add

RIP Config Table:

Select

Interface

Receive Mode

Send Mode

Delete Selected

Delete All

Fields on the first setting block	Description
RIP	Enable/disable RIP feature.

Fields on the second setting block:	Description
Interface	The name of the interface on which you want to enable RIP.
Receive Mode	Indicate the RIP version in which information must be passed to the DSL device in order for it to be accepted into its routing table.
Send Mode	Indicate the RIP version this interface will use when it sends its route information to other devices.

Function buttons for the second setting block in this page	Description
Add	Add a RIP entry and the new RIP entry will be display in the table
Delete Selected Entry	Delete a selected RIP entry. The RIP entry can be selected on the Select column of the RIP Config Table .
Delete All Entry	Delete All RIP entry.

23 ARP Table

This ARP Table shows a list of learned MAC addresses.

ARP Table

1. From the left *Advance* menu, click on *ARP Table*.

ARP Table

This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.1.178	00-24-1d-c4-b4-c0
192.168.1.33	f8-db-7f-dc-84-99

Refresh

24 Bridging

You can enable/disable Spanning Tree Protocol and set MAC address aging time in this page.

Bridging

1. From the left *Advance* menu, click on *Bridging*.

Bridging Configuration

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time: (seconds)

802.1d Spanning Tree: Disabled Enabled

Fields on the first setting block	Description
Ageing Time	Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding DataBase (fdb).
802.1d Spanning Tree	Enable/disable the spanning tree protocol
Function buttons	Description
Apply Changes	Save this bridge configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section "Admin" for details.
Show MACs	List MAC address in forwarding table.

25 Routing

The Routing page enables you to define specific route for your Internet and network data.

Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the DSL device provide the most appropriate path for all your Internet traffic.

–On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the DSL device. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.

–On the DSL device itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to setup through the configuration.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

Static Route

1. From the left *Advance* menu, click on *Routing*. The following page is displayed:

Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text"/>
Interface:	<input type="text" value="ppp0"/> ▼
<input type="button" value="Add Route"/> <input type="button" value="Update"/> <input type="button" value="Delete Selected"/> <input type="button" value="Show Routes"/>	

Static Route Table:

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
--------	-------	-------------	-------------	----------	--------	-----------

Fields on the first setting block	Description
Enable	Check to enable the selected route or route to be added.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
Interface	The WAN interface to which a static routing subnet is to be applied.
Function buttons	Description
Add Route	Add a user-defined destination route.
Update	Update the selected destination route on the Static Route Table .
Delete Selected	Delete a selected destination route on the Static Route Table .
Show Routes	Click this button to view the DSL device's routing table. The IP Route Table displays, as shown in Figure.

IP Route Table

This table shows a list of destination routes commonly accessed by your network.

Destination	Subnet Mask	NextHop	Iface
192.168.1.1	255.255.255.255	*	e1

26 SNMP

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The DSL device can be managed locally or remotely by SNMP protocol.

SNMP

1. From the left *Advance* menu, click on *SNMP*. The following page is displayed:

SNMP Configuration

This page is used to configure the SNMP. Here you may change the settings for system description, trap ip address, community name, etc..

SNMP:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
System Description	<input type="text" value="System Description"/>
System Contact	<input type="text" value="System Contact"/>
System Name	<input type="text" value="VDSL Modem/Router"/>
System Location	<input type="text" value="System Location"/>
System Object ID	<input type="text" value="1.3.6.1.4.1.16972"/>
Trap IP Address	<input type="text" value="192.168.1.254"/>
Community name (read-only)	<input type="text" value="public"/>
Community name (write-only)	<input type="text" value="public"/>

Fields on the first setting block	Description
System Description	System description of the DSL device.
System Contact	Contact person and/or contact information for the DSL device.
System Name	An administratively assigned name for the DSL device.
System Location	The physical location of the DSL device.
Trap IP Address	Destination IP address of the SNMP trap.
Community name (read-only)	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.
Community name (write-only)	Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

Function buttons	Description
Apply Changes	Save SNMP configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section "Admin" for details.
Reset	Reset the configuration.

27 Remote Access

This page is used to enable/disable management services for the LAN and WAN.

Remote Access

1. From the left *Advance* menu, click on *Remote Access*. The following page is displayed:

Remote Access Configuration

This page is used to enable/disable management services for the LAN and WAN.

Service Name	LAN	WAN	WAN Port
TELNET	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="23"/>
FTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="21"/>
TFTP	<input type="checkbox"/>	<input type="checkbox"/>	
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="80"/>
SNMP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
PING	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Apply Changes

28 Others

Here you can set some other advanced settings.

Others

1. From the left *Advance* menu, click on *Others*. The following page is displayed:

Other Advanced Configuration

Here you can set some other advanced settings.

IP PassThrough: Lease Time: seconds
 Allow LAN access

29 IPv6

This page is used to configure IPv6

IPv6

This page is used to configure IPv6 enable/disable

1. From the left *Advance* menu, click on *IPv6* -> *IPv6*. The following page is displayed:

IPv6Configuration

This page be used to configure IPv6 enable/disable

IPv6: Disable Enable

Apply Changes

RADVD

This page is used to setup the RADVD's configuration of your Router.

1. From the left *Advance* menu, click on *IPv6* -> *RADVD*. The following page is displayed:

RADVD Configuration

This page is used to setup the RADVD's configuration of your Router.

MaxRtrAdvInterval:	<input type="text" value="600"/>
MinRtrAdvInterval:	<input type="text" value="198"/>
AdvCurHopLimit:	<input type="text" value="64"/>
AdvDefaultLifetime:	<input type="text" value="1800"/>
AdvReachableTime:	<input type="text" value="0"/>
AdvRetransTimer:	<input type="text" value="0"/>
AdvLinkMTU:	<input type="text" value="0"/>
AdvSendAdvert:	<input type="radio"/> off <input checked="" type="radio"/> on
AdvManagedFlag:	<input checked="" type="radio"/> off <input type="radio"/> on
AdvOtherConfigFlag:	<input type="radio"/> off <input checked="" type="radio"/> on
Enable ULA:	<input type="radio"/> off <input checked="" type="radio"/> on
ULA Prefix:	<input type="text" value="fc01::"/>
ULA Prefix Len:	<input type="text" value="64"/>
ULA Prefix Valid Time:	<input type="text" value="2592000"/>
ULA Prefix Preferred Time:	<input type="text" value="604800"/>
Prefix Mode:	<input type="text" value="Auto"/> ▼

Apply Changes

DHCPv6

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

1. From the left *Advance* menu, click on *IPv6 -> DHCPv6*. The following page is displayed:

DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

DHCPv6 Mode: None DHCP Relay
 DHCP Server (Manual) DHCP Server (Auto)

Auto Config by Prefix Delegation for DHCPv6 Server:

MLD Proxy

This page is used to configure MLD Proxy.

1. From the left *Advance* menu, click on *IPv6 -> MLD Proxy*.

MLD Proxy Configuration

This page be used to configure MLD Proxy.

MLD Proxy: Disable Enable
WAN Interface:

Fields on the first setting block	Description
MLD Proxy	Enable/disable the MLD Proxy
WAN Interface	Select a WAN Interface

Function buttons	Description
Apply Changes	Save this bridge configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section "Admin" for details.

- Click *OK* button.

Change setting successfully!

OK

MLD Snooping

This page is used to configure MLD Snooping.

- From the left *Advance* menu, click on *IPv6* -> *MLD Snooping*.

MLD Proxy Configuration

This page be used to configure MLD Proxy.

MLD Proxy:

Disable Enable

WAN Interface:

▼

Apply Changes

Fields on the first setting block	Description
MLD Snooping	Enable/disable the MLD Snooping

Function buttons	Description
Apply Changes	Save this bridge configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section "Admin" for details.

- Click *OK* button.

Change setting successfully!

OK

IPv6 Routing

This page is used to configure the IPv6 static routing information. Here you can add/delete static IP routes.

5. From the left *Advance* menu, click on *IPv6* -> *IPv6 Routing*.

IPv6 Static Routing Configuration

This page is used to configure the IPv6 static routing information. Here you can add/delete static IP routes.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text"/>
Interface:	<input type="text" value="ppp0"/> ▼

Static IPv6 Route Table:

Select	State	Destination	Next Hop	Metric	Interface
--------	-------	-------------	----------	--------	-----------

IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

1. From the left *Advance* menu, click on *IPv6 -> IP/Port Filtering*.

IPv6 IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action Deny Allow

Incoming Default Action Deny Allow

Apply Changes

Direction: **Protocol:** **Rule Action** Deny Allow

Source IP Address:

Source Prefix Length:

Destination IP Address:

Destination Prefix Length:

Source Port:

Destination Port:

Add

Current Filter Table:

Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action
--------	-----------	----------	-------------------	-------------	------------------------	------------------	-------------

Delete Selected

Delete All

30 Diagnostic

The DSL device supports some useful diagnostic tools.

Ping

Once you have your DSL device configured, it is a good idea to make sure you can ping the network. A ping command sends a message to the host you specify. If the host receives the message, it sends messages in reply. To use it, you must know the IP address of the host you are trying to communicate with and enter the IP address in the Host Address field. Click Go! To start the ping command, the ping result will then be shown in this page.

1. From the left *Maintenance* menu, click on *Diagnostic* -> *Ping*. The following page is displayed:

Ping Diagnostics

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

Host Address:

Go!

Fields	Description
Host Address	The IP address you want to ping.
Function buttons	Description
Go!	To start the ping command

2. Type the IP Address in the *Host* field.
3. Click *Ping*

Ping Diagnostics

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

Host Address:

8.8.8.8

Go!

4. Now you could see the result below:

PING 8.8.8.8 (8.8.8.8): 56 data bytes

64 bytes from 8.8.8.8: icmp_seq=0

64 bytes from 8.8.8.8: icmp_seq=1

64 bytes from 8.8.8.8: icmp_seq=2

--- ping statistics ---

3 packets transmitted, 3 packets received.

Back

ATM Loopback

In order to isolate the ATM interface problems, you can use ATM OAM loopback cells to verify connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC. ATM uses F4 and F5 cell flows as follows:

- F4: used in VPs
- F5: used in VCs

An ATM connection consists of a group of points. This OAM implementation provides management for the following points:

- Connection endpoint: the end of a VP/VC connection where the ATM cell are terminated
- Segment endpoint: the end of a connection segment

This page allows you to use ATM ping, which generates F5 segment and end-to-end loop-back cells to test the reachability of a segment endpoint or a connection endpoint.

1. From the left *Maintenance* menu, click on *Diagnostic* -> *ATM Loopback*. The following page is displayed:

ATM Loopback Diagnostics - Connectivity Verification

Connectivity verification is supported by the use of the ATM OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Select PVC:

Flow Type:

- F4 Segment
- F4 End-to-End
- F5 Segment
- F5 End-to-End

Loopback Location ID:

Go!

ADSL Tone Diagnostics

This page displays the ADSL Tone Diagnostic performance. Click Start button to start the ADSL diagnostic.

1. From the left *Maintenance* menu, click on *Diagnostic* -> *ADSL Tone*. The following page is displayed:
2. Click Start button to start the ADSL diagnostic.

DSL Tone Diagnostics

DSL Tone Diagnostics. Only ADSL2/ADSL2+/VDSL2 support this function.

Start

	Downstream	Upstream
Hlin Scale		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Band Status	U0	U1	U2	U3	U4	D1	D2	D3	D4
LATN									
SATN									
SNRM									

Upstream (Group Number=0)					
Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					

ADSL Connection Diagnostics

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

1. From the left *Maintenance* menu, click on *Diagnostic* -> *ADSL Connection*. The following page is displayed:
2. Click *RUN Diagnostic Test* button to start the ADSL diagnostic.

ADSL Connection Diagnostics

The Router is capable of testing your connection. The individual tests are listed below. If a test displays a fail status, click 'Go' button again to make sure the fail status is consistent.

Select the ADSL Connection:

Fields	Description
Select the ADSL Connection	The available WAN side interfaces are listed. You have to select one for the WAN side diagnostic.
Function buttons	Description
Go	To start the RUN Diagnostic Test

31 Commit/Reboot

Whenever you use the web console to change system settings, the changes are initially placed in temporary storage. To save your changes for future use, you can use the Commit/Reboot function. This function saves your changes from RAM to flash memory and reboot the system.

IMPORTANT! Do not turn off your modem or press the Reset button while this procedure is in progress.

Commit and Reboot

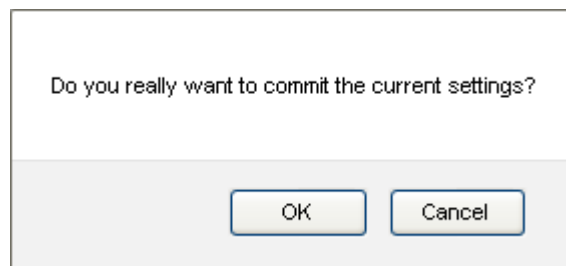
1. From the left *Admin* menu, click on *Commit/Reboot*. The following page is displayed:
2. Click on *Commit and Reboot*.

Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

3. Click on *OK*.



4. System rebooting, Please wait ... 60 seconds.

System rebooting, Please wait ...
49

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

32 Backup/Restore

You can save the current configuration of your Router to a file on your computer. This is highly recommended before you change any configuration settings on the Router or before you upgrade your firmware.

Backup settings

1. From the left *Maintenance* menu, click on *Admin -> Backup/Restore*. The following page is displayed:

Backup and Restore Settings

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

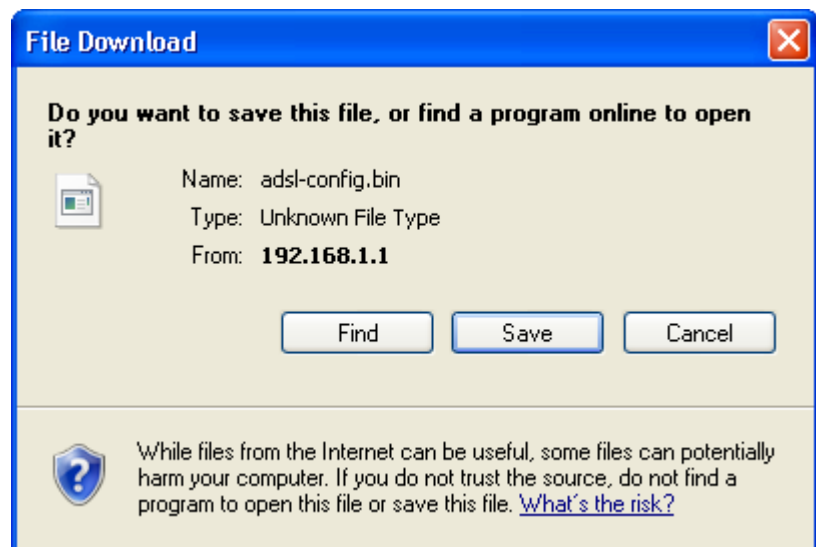
Backup Settings to File:

Restore Settings from File:

Reset Settings to Default:

Figure 4: Backup & Restore page

2. Click on *Save*.
3. Choose the *Save option* and select a suitable location and filename to save your backup file to.
4. Press *Save*



Restore settings

1. From the left *Maintenance* menu, click on *Update -> Backup/Restore*. The following page is displayed:
2. Click *Browse...* and browse to the location of your backup file
3. Click *Upload*

Backup and Restore Settings

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

Backup Settings to File:

Restore Settings from File:

Reset Settings to Default:

Figure 5: Backup & Restore page

4. Restore settings from config file successful!
5. The System is Restarting ...

Restore settings from config file successful! The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Resetting to Defaults

This page allows you to reset your device to its default factory settings.

The configuration settings of your device are stored in a configuration file. When you set up your device and access the web pages for the very first time, the configuration file contains a default factory configuration..

If you do make changes to the default configuration but then wish to revert back to the original factory configuration, you can do so by resetting the device to factory defaults.



Note

If you reset your device to factory defaults, all previous configuration changes that you have made are overwritten by the factory default configuration.

Software Reset:

1. From the left *Admin* menu, click on *Commit/Reboot*. The following page is displayed:
2. Click on *Reset*.

Backup and Restore Settings

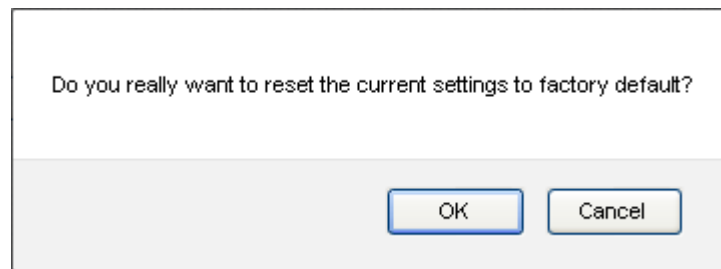
This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

Backup Settings to File:

Restore Settings from File:

Reset Settings to Default:

3. Click on *OK*.



4. System rebooting, Please wait ... 60 seconds.

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

33 System Log

This page can be used to set remote log server and show the system log.

System Log

- From the left-hand *Admin* menu, click on *System Log*. The following page is displayed:

System Log

System Log : Disable Enable

Log Level :

Display Level :

Save Log to File:

Clear Log:

System Log

Date/Time	Facility	Level	Message
-----------	----------	-------	---------

Option	Description
Enable Log	Enable/Disable the feature. Default: Disable
Log Level	Select one Log Level
Display Level	Select one Display Level
Mode	Select one Mode
Enable Remote Log	Enable: Send the system log to remote log server. To do this, make sure a secure syslog server is available. Default: Disable
Log Server IP Address	Enter the IP Address of remote log server.
Server UDP Port	Enter the UDP Port of remote log server.

2. Check the option *Enable*.
3. From the *Log Level* drop-down list, select a *Log Level*.
4. From the *Display Level* drop-down list, select a *Display Level*.
5. Click *Apply Changes*.

System Log

System Log : Disable Enable

Log Level : ▾

Display Level : ▾

Save Log to File:

Clear Log:

System Log

Date/Time	Facility	Level	Message
-----------	----------	-------	---------

6. Change setting successfully! Click on *OK* to confirm.

Change setting successfully!

34 Password

You can restrict access to your device's web pages using password protection. With password protection enabled, users must enter a username and password before gaining access to the web pages.

By default, password protection is enabled on your device, and the username and password set are as follows:

Username: **admin**

Password: **admin**

Username: **user**

Password: **user**

Setting your username and password



Note

Non-authorized users may try to access your system by guessing your username and password. We recommend that you change the default username and password to your own unique settings.

To change the default password:

1. From the left *Admin* menu, click on *Password*. The following page is displayed:

Password Configuration

This page is used to set the account to access the web server of your Router. Empty user name and password will disable the protection.

User Name:

admin ▾

Old Password:

New Password:

Confirmed Password:

Apply Changes

Reset

Figure 6: Currently Defined Administration Password: Setup page

2. This page displays the current username and password settings. Change your own unique password in the relevant boxes. They can be any combination of letters or numbers with a maximum of 30 characters. The default setting uses **admin** for the username and **admin** for password.
3. If you are happy with these settings, click **Apply Changes**. You will see following page that the new user has been displayed on the Currently Defined Users. You need to login to the web pages using your new username and new password.

Password Configuration

This page is used to set the account to access the web server of your Router. Empty user name and password will disable the protection.

User Name:

Old Password:

New Password:

Confirmed Password:

Figure 7: Administration Password

4. Click OK.

Change setting successfully!

5. Enter *User name* and new *Password*.
6. Click *OK*.

Connect to 192.168.1.1

DSL Router

User name:

Password:

Remember my password

35 Firmware Update

The *Firmware Update* page allows you to:

- manually download the latest firmware version from website and manually update your firmware. See *Manually updating firmware*.

About firmware versions

Firmware is a software program. It is stored as read-only memory on your device.

Your device can check whether there are later firmware versions available. If there is a later version, you can download it via the Internet and install it on your device.



Note

If there is a firmware update available you are strongly advised to install it on your device to ensure that you take full advantage of any new feature developments.

Manually updating firmware

You can manually download the latest firmware version from website to your PC's file directory.

Once you have downloaded the latest firmware version to your PC, you can manually select and install it as follows:

- From the left *Admin* menu, click on *Firmware Upgrade*. The following page is displayed:
- Click on the *Browse...* button.

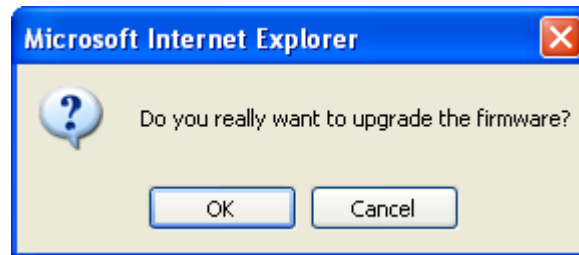
Firmware Upgrade

This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

Figure 8: Manual Update Installation section

(Note that if you are using certain browsers (such as Opera 7) the *Browse* button is labeled *Choose*.)

3. Use the *Choose file* box to navigate to the relevant directory where the firmware version is saved.
4. Once you have selected the file to be installed, click *Open*. The file's directory path is displayed in the *Select File*: text box.
5. Click *Upload*. The device checks that the selected file contains an updated version of firmware. A screen pops up, please click *OK*.



6. Firmware upgrading, Please wait 250 seconds.

Firmware upgrading, Please wait ... 242

Please note do NOT power off the device during the upload because it may crash the system.

- Firmware update has been update complete and it will bring you to the home page of the device:

Router Status

This page shows the current status and some basic settings of the device.

System	
Alias Name	VDSL Modem/Router
Uptime	4 min
Firmware Version	VNHA_201_STD_01_130603
DSP Version	v113d412
Name Servers	
IPv4 Default Gateway	
IPv6 Default Gateway	
DSL	
Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps
LANConfiguration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00e04c867001

WANConfiguration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
ppp1_vc0_0	0/33	LLC	PPPoE			down 0sec / 0sec
ppp0_ptm0_0	---	---	PPPoE			down 0sec / 0sec

3G Configuration				
Interface	Protocol	IP Address	Gateway	Status

Refresh

- From the left *Admin* menu, click on *Commit/Reboot*. The following page is displayed:
- Click on *Reset*.

Backup and Restore Settings

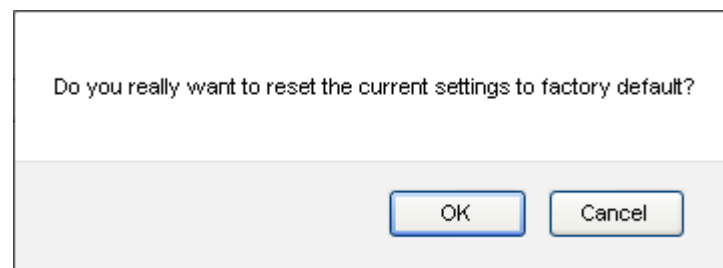
This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

Backup Settings to File:

Restore Settings from File:

Reset Settings to Default:

- Click on *OK*.



- System rebooting, Please wait ... 60 seconds.

The System is Restarting ...

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for a minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

36 ACL Configuration

You can specify which services are accessible from LAN or WAN side.

Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.

Using of such access control can be helpful in securing or restricting the Gateway management.

ACL Config

1. From the left *Firewall* menu, click on *ACL*. The following page is displayed:

ACL Configuration

This page is used to configure the IP Address for Access Control List. If ACL is enabled, only the IP address in the ACL Table can access CPE. Here you can add/delete the IP Address.

ACL Capability: Disable Enable

Enable:

Interface:

IP Address:

Subnet Mask:

ACL Table:

Select	State	Interface	IP Address
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>			

Figure 9: ACL Configuration page

37 Time Zone

Certain systems may not have a date or time mechanism or may be using inaccurate time/day information. The Simple Network Time Protocol feature provides a way to synchronize the device's own time of day setting with a remote time server as described in RFC 2030 (SNTP) and RFC 1305 (NTP).


SNTP Server and SNTP Client Configuration settings

1. From the left *Maintenance* menu, click on *Time*. The following page is displayed:


Time Zone Configuration

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Year Mon Day Hour Min Sec

Time Zone Select : 

Enable SNTP Client Update

SNTP Server : 
 (Manual Setting)

Fields	Description
Current Time	The current time of the specified time zone. You can set the current time by yourself or configured by SNTP.
Interval	The Interval of SNTP client to update the system clock
Time Zone Select	The time zone in which the DSL device resides.
SNTP server	The IP address or the host name of the SNTP server. You can select from the list or set it manually.

Function Button	Description
Apply Changes	Click to save the setting of default actions to the configuration.

2. Select proper Time Zone from *Time Zone Select* drop-down list.
3. Check on *Enable SNTP Client Update*.
4. Add NTP Server using IP Address.
5. Click on *Apply Changes*.

Time Zone Configuration

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Year Mon Day Hour Min Sec

Time Zone Select :

Enable SNTP Client Update

SNTP Server :
 (Manual Setting)

Figure 10: SNTP Server Configuration page

6. Click on *OK*.

Change setting successfully!

Time Zone	GMT +/- offset	Description	Daylight Saving Start	Daylight Saving End
IDLW	-1200	International Date Line West	Not applicable	Not applicable
NT	-1100	Nome	Not applicable	Not applicable
HST	-1000	Hawaii Standard	Not applicable	Not applicable
AKST	-900	Alaska Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
YST	-900	Yukon Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
PST	-800	US Pacific Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
MST	-700	US Mountain Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
CST	-600	US Central Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
EST	-500	US Eastern Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
AST	-400	Atlantic Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
NFST	-330	Newfoundland Standard	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
NFT	-330	Newfoundland	First Sunday of April at 2:00am	Last Sunday of October at 2:00am
BRA	-300	Brazil Standard	First Sunday of February at 2:00 am	Third Sunday of February at 2:00am
AT	-200	Azores	Not applicable	Not applicable
WAT	-100	West Africa	Last Sunday March at 1:00am	Last Sunday October at 1:00am
GMT	+000	Greenwich Mean	Last Sunday March at 1:00am	Last Sunday October at 1:00am
UTC	+000	Universal (Coordinated)	Last Sunday March at 1:00am	Last Sunday October at 1:00am
WET	+000	Western European	Last Sunday March at 1:00am	Last Sunday October at 1:00am

Time Zone	GMT +/- offset	Description	Daylight Saving Start	Daylight Saving End
CET	+100	Central European	Last Sunday March at 2:00am	Last Sunday October at 2:00am
MET	+100	Middle European	Last Sunday March at 2:00am	Last Sunday October at 2:00am
MEWT	+100	Middle European Winter	Last Sunday March at 2:00am	Last Sunday October at 2:00am
SWT	+100	Swedish Winter	Last Sunday March at 2:00am	Last Sunday October at 2:00am
BST	+100	British Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
EET	+200	Eastern Europe, Russia Zone 1	Last Sunday March at 2:00am	Last Sunday October at 2:00am
FST	+200	French Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
MEST	+200	Middle European Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
SST	+200	Swedish Summer	Last Sunday March at 2:00am	Last Sunday October at 2:00am
IST	+200	Israeli Standard	First Friday April at 2:00am	First Friday September at 2:00am
IDT	+300	Israeli Daylight	1st April at 2:00am	First Friday of September at 2:00am
BT	+300	Baghdad	1st April at 2:00am	1st October at 2:00am
IT	+330	Iran	21st March	23rd September
USZ3	+400	Russian Volga	Last Sunday March at 2:00am	Last Sunday in October at 2:00am
USZ4	+500	Russian Ural	Last Sunday of March at 2:00am	Last Sunday October at 2:00am
INST	+530	Indian Standard	Not applicable	Not applicable
USZ5	+600	Russian West-Siberian	Last Sunday March at 2:00am	Last Sunday October at 2:00am
NST	+630	North Sumatra	Not applicable	Not applicable
WAST	+700	West Australian Standard	Not applicable	Not applicable
USZ6	+700	Russia Yenisei	Last Sunday March at 2:00am	Last Sunday October at 2:00am
JT	+730	Java	Not applicable	Not applicable
CCT	+800	China Coast	Not applicable	Not applicable
ROK	+900	Korean Standard	Not applicable	Not applicable

Time Zone	GMT +/- offset	Description	Daylight Saving Start	Daylight Saving End
KST	+900	Korean Standard	Not applicable	Not applicable
JST	+900	Japan Standard	Not applicable	Not applicable
CAST	+930	Central Australian Standard	Last Sunday October at 2:00am	Last Sunday March at 2:00am
KDT	+1000	Korean Daylight	Not applicable	Not applicable
EAST	+1000	Eastern Australian Standard	Last Sunday October at 2:00am	Last Sunday March at 3:00am
GST	+1000	Guam Standard	Last Sunday March at 2:00am	Last Sunday October at 2:00am
CADT	+1030	Central Australian Daylight	Last Sunday October at 2:00am	Last Sunday March at 3:00am
IDLE	+1200	International Date Line East	Not applicable	Not applicable
NZST	+1200	New Zealand Standard	Last Sunday October at 2:00am	Last Sunday March at 2:00am
NZT	+1200	New Zealand	Last Sunday October at 2:00am	Last Sunday March at 2:00am

Time Zone abbreviations

38 TR-069

TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS). The CPE TR-069 configuration should be well defined to be able to communicate with the remote ACS.

TR-069 Configuration

1. From the left *Admin* menu, click on *TR-069*. The following page is displayed:

TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

TR069: Disabled Enabled

ACS:

URL:

User Name:

Password:

Periodic Inform: Disabled Enabled

Periodic Inform Interval:

Connection Request:

User Name:

Password:

Path:

Port:

Certificate Management:

CPE Certificate Password:

CPE Certificate:

CA Certificate:

Figure 11: TR-069 Configuration page

ACS Field	Description
URL	ACS URL. For example, http://10.0.0.1:80 https://10.0.0.1:443
User Name	The username the DSL device should use when connecting to the ACS.
Password	The password the DSL device should use when connecting to the ACS.
Periodic Inform	When this field is enabled, the DSL device will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in Periodic Inform Interval field; When this field is disabled, the DSL device will only send Inform RPC to the ACS server once at the system startup.
Periodic Inform Interval	Time interval in second to send Inform RPC.
Connection Request Field	Description
User Name	The username the remote ACS should use when connecting to this device.
Password	The password the remote ACS should use when connecting to this device.
Path	The path of the device ConnectionRequestURL. The device ConnectionRequestURL should be configured based on the Device_IP, Path and Port as follows: http://Device_IP:Port/Path
Port	The port of the device ConnectionRequestURL.

39 Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

Statistics - Interface

1. From the left *Statistics* menu, click on *Interface* The following page is displayed:
2. To display updated statistics showing any new data since you opened this page, click *Refresh*.

Interface Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0.5	26548	0	0	24551	0	0
ppp0_vc0_0	0	0	0	0	0	0
ppp1_ptm0_0	0	0	0	0	0	0

Statistics - ADSL

This page shows the packet statistics for transmission and reception regarding to network interface.

1. From the left *Statistics* menu, click on *ADSL*. The following page is displayed:
2. To display updated statistics showing any new data since you opened this page, click *Refresh*.

DSL Statistics

Mode	
TPS-TC	
Latency	
Status	HANDSHAKING.
Power Level	L0
Uptime	

	Downstream	Upstream
Trellis	Off	Off
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	0.0
Attainable Rate (Kbps)	0	0
G.INP	Off	Off
Rate (Kbps)	0	0
R (number of check bytes in RS code word)	0	0
N (RS codeword size)	0	0
L (number of bits in DMT frame)	0	0
S (RS code word size in DMT frame)	0.00	0.00
D (interleaver depth)	0	0
Delay (msec)	0.00	0.00
INP (DMT frame)	0.000	0.000
FEC errors	0	0
OH Frame	0	0
OH Frame errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	0	0
Total LOSS	--	--
Last Link Rate	0	0
Full Init	0	
Failed Full Init	0	
Synchronized time(Second)	0	
Synchronized number	0	

A Configuring your Computers

This appendix provides instructions for configuring the Internet settings on your computers to work with the VDSL2 Router.

Configuring Ethernet PCs

Before you begin

By default, the VDSL2 Router 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 VDSL2 Router to do so. See *Assigning static Internet information to your PCs* for instructions.

- If you have connected your LAN PCs via Ethernet to the VDSL2 Router, 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

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 labeled *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 labeled *Internet Protocol TCP/IP* is checked and click *Properties*.
5. In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
6. Click *OK* twice to confirm your changes, and then close the Control Panel.

Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

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 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 10.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click *Install...*
5. In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add...*
6. 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.
7. If prompted, click *OK* to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the VDSL2 Router:

8. In the *Control Panel*, double-click the Network and Dial-up Connections icon.
9. In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.
10. In the Local Area Connection Properties dialog box, select *Internet Protocol (TCP/IP)*, and then click *Properties*.
11. In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
12. 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 11.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click *Add...*
5. In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add...*
6. Select *Microsoft* in the Manufacturers box.
7. 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.

8. If prompted, click *OK* to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the VDSL2 Router:

9. In the *Control Panel*, double-click the Network and Dial-up Connections icon.
10. In *Network and Dial-up Connections window*, right-click the Network icon, and then select *Properties*.
11. In the *Network Properties* dialog box, select *TCP/IP*, and then click *Properties*.
12. In the TCP/IP Settings dialog box, click the radio button labeled **Server assigned IP address**. Also click the radio button labeled *Server assigned name server address*.
13. Click *OK* twice to confirm and save your changes, and then close the *Control Panel*.

Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. Double-click the Network icon.
3. If TCP/IP does not display as an installed component, click *Add...*

The *Select Network Component Type* dialog box displays.

4. Select *Protocol*, and then click *Add...*

The Select Network Protocol dialog box displays.

5. Click on *Microsoft* in the Manufacturers list box, and then click *TCP/IP* in the Network Protocols list box.
6. 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.

7. Click *OK* to restart the PC and complete the TCP/IP installation.

Next, configure the PCs to accept IP information assigned by the VDSL2 Router:

8. Open the Control Panel window, and then click the Network icon.
9. Select the network component labeled TCP/IP, and then click *Properties*.

If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

10. In the TCP/IP Properties dialog box, click the IP Address tab.
11. Click the radio button labeled *Obtain an IP address automatically*.
12. Click the DNS Configuration tab, and then click the radio button labeled *Obtain an IP address automatically*.
13. Click *OK* twice to confirm and save your changes.
You will be prompted to restart Windows.
14. Click *Yes*.

Windows NT 4.0 workstations

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. In the Control Panel window, double click the Network icon.
3. 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 9.

4. If TCP/IP does not display as an installed component, click *Add...*
5. 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.

6. 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 VDSL2 Router:

7. Open the Control Panel window, and then double-click the Network icon.
8. In the *Network* dialog box, click the *Protocols* tab.
9. In the *Protocols* tab, select *TCP/IP*, and then click *Properties*.
10. In the *Microsoft TCP/IP Properties* dialog box, click the radio button labeled *Obtain an IP address from a DHCP server*.
11. 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 VDSL2 Router 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 VDSL2 Router. By default, the LAN port is assigned the IP address *192.168.1.1*. (You can change this number or another number can be assigned by your ISP. See *Addressing* for more information.)
- 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.



Note

*Your PCs must have IP addresses that place them in the same subnet as the VDSL2 Router's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in *Addressing* to change the LAN port IP address accordingly.*

B IP Addresses, Network Masks, and Subnets

IP Addresses



Note

This section refers only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called *dotted decimal notation*. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information:

- *Network ID*
Identifies a particular network within the Internet or intranet
- *Host ID*
Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's *class* (see following section). The table below shows the structure of an IP address.

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the

scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

- The class can be determined easily from field1:
 field1 = 1-126: Class A
 field1 = 128-191: Class B
 field1 = 192-223: Class C
 (field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

Subnet masks



Definition mask

A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."

Subnet masks are used to define *subnets* (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field3 are part of the network ID, but note how the mask specifies that the first bit in field4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 1 to 126 hosts (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111.11111111.
11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 1 to 62.

**Note**

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:

Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

These are called default because they are used when a network is initially configured, at which time it has no subnets.

C Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the VDSL2 Router, 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 VDSL2 Router 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 VDSL2 Router. 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	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 192.168.1.1). 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 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.

Problem	Troubleshooting Suggestion
<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 VDSL2 Router is correct, then You can use the ping utility, 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" the user ID and "admin " as password. Otherwise, you can reset the device to the default configuration by pressing the Reset Default button on the Rare panel of the device (see <i>Rare Panel</i>). 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 your PC can communicate with the device's LAN IP address (by default 192.168.1.1). 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 VDSL2 Router.
<i>My changes to the web pages are not being retained.</i>	Be sure to use the <i>Confirm Changes/Apply</i> function after any changes.

Diagnosing Problem using IP Utilities

ping

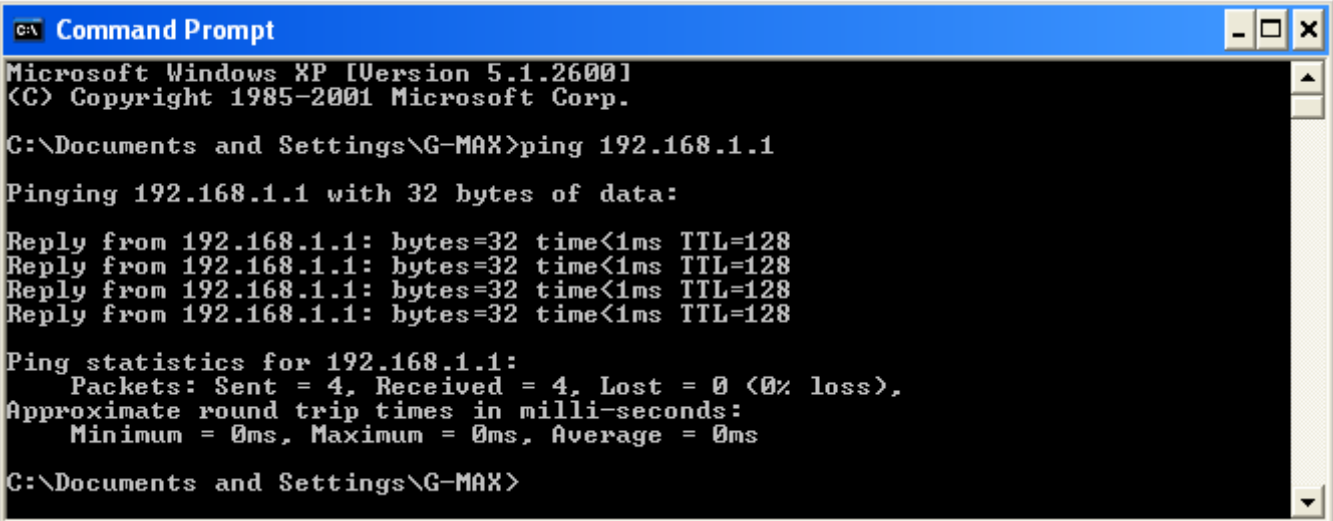
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer 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 192.168.1.1

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:

A screenshot of a Windows Command Prompt window. The title bar reads "C:\> Command Prompt". The window content shows the following text:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\G-MAX>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms 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:\Documents and Settings\G-MAX>
```

Figure 12: Using the ping Utility

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 VDSL2 Router is working (using the preconfigured default LAN IP address 192.168.1.1) 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

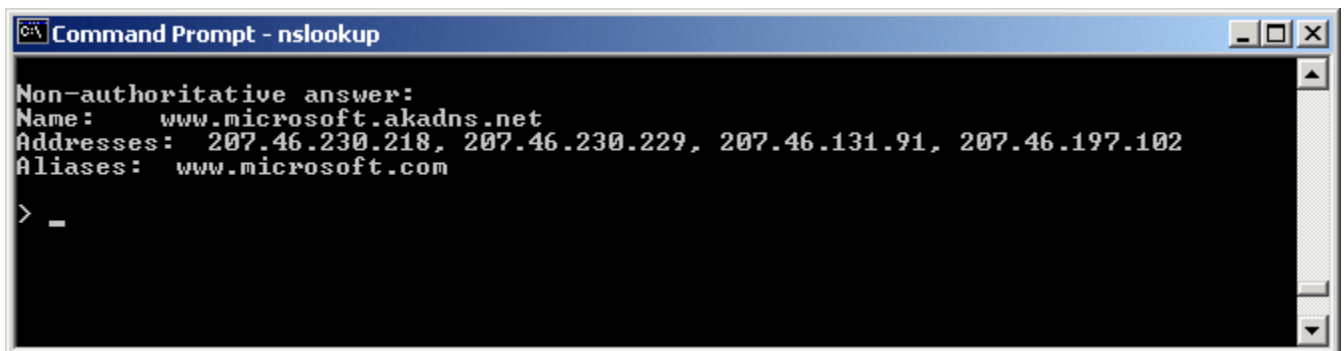
common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated 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
> _
```

Figure 13: Using the nslookup Utility

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.

D

Glossary

- 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 VDSL2 Router 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.

	<p>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.</p>
DHCP relay	<p>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 VDSL2 Router's interfaces can be configured as a DHCP relay. See <i>DHCP</i>.</p>
DHCP server	<p>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 <i>DHCP</i>.</p>
digital	<p>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 <i>analog</i>.</p>
DNS	<p>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, <i>www.yahoo.com</i> 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 <i>domain name</i>.</p>
domain name	<p>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 <i>DNS</i>.</p>
download	<p>To transfer data in the downstream direction, i.e., from the Internet to the user.</p>
DSL	<p>Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.</p>
encryption keys	<p>See <i>network keys</i></p>
Ethernet	<p>The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also <i>10BASE-T</i>, <i>100BASE-T</i>, <i>twisted pair</i>.</p>
FTP	<p>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.</p>
Gbps	<p>Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.</p>
host	<p>A device (usually a computer) connected to a network.</p>
HTTP	<p>Hyper-Text Transfer Protocol HTTP is the main protocol used to transfer data from web</p>

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 <i>TCP/IP</i> .
IP address	Internet Protocol address 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 <i>network ID</i> that identifies the particular network the host belongs to, and a <i>host ID</i> 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 <i>domain name</i> , <i>network mask</i> .
ISP	Internet Service Provider A company that provides Internet access to its customers, usually for a fee.
LAN	Local Area Network A network limited to a small geographic area, such as a home or small office.
LED	Light Emitting Diode An electronic light-emitting device. The indicator lights on the front of the VDSL2 Router are LEDs.
MAC address	Media Access Control address 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; <i>NN:NN:NN:NN:NN:NN</i> .
mask	See <i>network mask</i> .
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
NAT	Network Address Translation A service performed by many Routers that translates your network's publicly known IP address into a <i>private</i> 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.

network	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 <i>LAN</i> , or very large, such as the <i>Internet</i> .
network mask	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 <i>binary</i> , <i>IP address</i> , <i>subnet</i> .
NIC	Network Interface Card 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 <i>Ethernet</i> , <i>RJ-45</i> .
packet	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).
ping	Packet Internet (or Inter-Network) Groper 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.
port	A physical access point to a device such as a computer or Router, through which data flows into and out of the device.
PPP	Point-to-Point Protocol 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 VDSL2 Router uses two forms of PPP called PPPoA and PPPoE. See <i>PPPoA</i> , <i>PPPoE</i> .
PPPoA	Point-to-Point Protocol over ATM 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.
PPPoE	Point-to-Point Protocol over Ethernet 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.
protocol	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.
remote	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
RIP	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.
RJ-11	Registered Jack Standard-11 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.

RJ-45	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
routing	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.
SDNS	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See <i>DNS</i> .
subnet	A subnet is a portion of a network. The subnet is distinguished from the larger network by a <i>subnet mask</i> 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 <i>network mask</i> .
subnet mask	A mask that defines a subnet. See <i>network mask</i> .
TCP	See <i>TCP/IP</i> .
TCP/IP	Transmission Control Protocol/Internet Protocol 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.
Telnet	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.
TFTP	Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
TKIP	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.
triggers	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. 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.
twisted pair	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 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 (192.168.1.1).

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 <i>VC</i> .
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 <i>VC</i> .
WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the VDSL2 Router, 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 <i>HTTP</i> , <i>web site</i> , <i>WWW</i> .
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 <i>home page</i> . See <i>hyperlink</i> , <i>web site</i> .
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 <i>hyperlink</i> , <i>web page</i> .
WWW	World Wide Web

Also called *(the) Web*. Collective term for all web sites anywhere in the world that can be accessed via the Internet.

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 provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.