

Tenda

User Guide

www.tendacn.com



Wireless N300 ADSL2+/3G Modem Router

Copyright Statement

Tenda is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd. If you would like to know more about our product information, please visit our website at <http://www.tendacn.com>.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Contents

Chapter 1 Product Overview	1 -
1.1 Package Contents	1 -
1.2 Hardware Overview	1 -
1.2.1 LEDs on Front Panel	1 -
1.2.2 Buttons & Ports on Back Panel.....	3 -
1.2.3 Label.....	4 -
Chapter 2 Get Started	5 -
2.1 Install Considerations.....	5 -
2.2 What You Need Before You Start.....	5 -
A. To access the Internet with a phone cable:	5 -
B. To access the Internet with an Ethernet cable:.....	6 -
C. To access the Internet via a 3G mobile connection:	7 -
Chapter 3 Quick Internet Setup	1 -
3.1 Hardware Install.....	1 -
A. To access the Internet with a phone cable:	1 -
B. To access the Internet with an Ethernet cable.....	2 -
C. To access the Internet via a 3G mobile connection:	4 -
3.2 Connect to Your Device	5 -
3.2.1 Configure Your PC	5 -
3.2.2 Join Your Wireless Network	5 -
3.3 Internet Setup	9 -
3.3.1 Web Login	9 -
3.3.2 Internet Setup & Wireless Setup	12 -
Chapter 4 Advanced Settings	16 -
4.1 Device Info.....	17 -
4.2 Advanced Setup.....	20 -
4.2.1 Layer2 Interface	21 -
4.2.2 WAN Service.....	23 -
4.2.3 USB Application.....	58 -
4.2.4 LAN Setup	61 -
4.2.5 NAT.....	64 -
4.2.6 Security	70 -
4.2.7 Parental Control	74 -
4.2.8 Quality of Service	76 -
4.2.9 Routing	78 -
4.2.10 DNS	81 -
4.2.11 DSL	83 -
4.2.12 UPnP.....	85 -

4.2.13 Interface Grouping	- 85 -
4.2.14 IP Tunnel.....	- 87 -
4.2.15 Certificate.....	- 88 -
4.2.16 Multicast	- 91 -
4.2.17 IPTV	- 93 -
4.3 Wireless.....	- 93 -
4.3.1 Basic	- 94 -
4.3.2 Security	- 94 -
4.3.3 MAC Filter	- 96 -
4.3.4 Wireless Bridge	- 98 -
4.3.5 Station Info.....	- 99 -
4.4 Diagnostics.....	- 99 -
4.5 Management.....	- 100 -
4.5.1 Settings.....	- 101 -
4.5.2 System Logs.....	- 102 -
4.5.3 TR-069 Client.....	- 103 -
4.5.4 Internet Time	- 104 -
4.5.5 Access Control	- 104 -
4.5.6 Update Firmware	- 106 -
4.5.7 Reboot.....	- 106 -
Appendix 1 Configure Your PC	- 1 -
Windows 7	- 1 -
Windows XP	- 3 -
Appendix 2 FAQs	- 5 -
Appendix 3 VPI/VCI List	- 1 -
Appendix 4 Regulatory Compliance Information	- 10 -

About This Manual

Thank you for choosing Tenda! Please read this User Guide before you start! This User Guide instructs you to install and configure your device.

Conventions

Unless otherwise specified, "This (this)/The (the) device", "This (this)/The (the) product" and "Device (device)", etc. mentioned herein all refer to Tenda Wireless N300 ADSL2+/3G Modem Router D303.

Unless otherwise specified, this User Guide is exemplified of IPv4.

Technical Support

Website: <http://www.tendacn.com>

TEL: (86 755) 2765 7180

Email: support@tenda.com.cn

Chapter 1 Product Overview

1.1 Package Contents

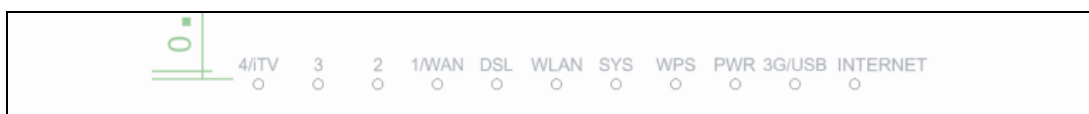
Unpack the package. Your box should contain the following items:

- D303
- Power Adapter
- Two Phone Cables
- Ethernet Cable
- ADSL Splitter
- Install Guide
- Resource CD

If any of the parts are incorrect, missing, or damaged, contact your dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

1.2 Hardware Overview

1.2.1 LEDs on Front Panel



LED	Status	Description
4/iTV 3 2 1/WAN	Solid	The corresponding port is connected correctly.
	Blinking	The corresponding port is transmitting data.
	Off	The corresponding port is connected improperly or malfunctioning.
DSL	Solid	DSL connection is established successfully.

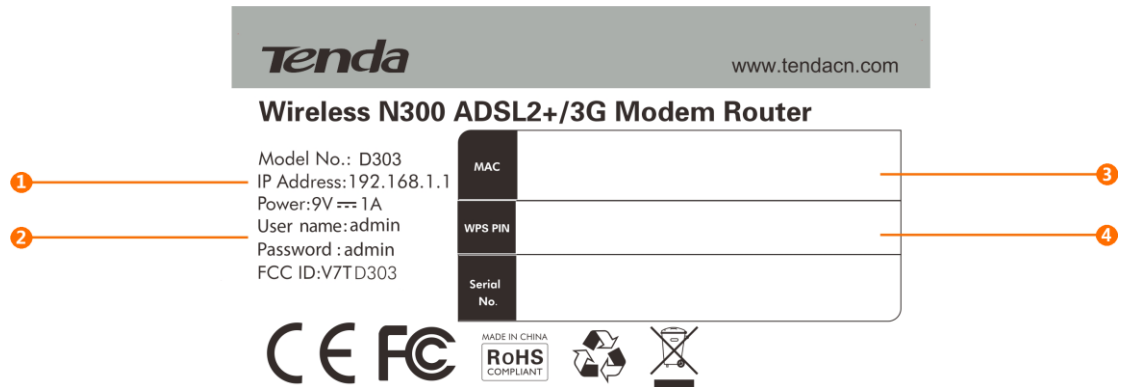
	Blinking	The device is negotiating with DSLAM.
	Off	No phone cable is connected to the DSL port or phone cable is connected improperly.
WLAN	Solid	Wireless radio is on.
	Blinking	The wireless interface is transmitting data.
	Off	Wireless radio is off.
SYS	Blinking	System is functioning properly.
	Solid/Off	System is malfunctioning.
WPS	Solid	Clients have successfully joined your wireless network using the WPS feature during the first two minutes.
	Blinking	WPS-PBC is enabled and your wireless network is accessible to WPS-PBC enabled clients.
	Off	No clients join your wireless network using the WPS feature during the first two minutes.
PWR	Solid	The device is receiving electrical power.
	Off	Electric power is not supplied to the device or the device is malfunctioning.
3G/USB	Solid	The device has identified an attached USB storage device or has successfully joined a 3G network.
	Blinking	Connecting to 3G network...
	Off	The USB port is not connected or has not identified an attached USB storage device or the device fails to join a 3G network.
INTERNET	Solid	The device has obtained an IP address for Internet access.
	Off	The device fails to obtain an IP address for Internet access.

1.2.2 Buttons & Ports on Back Panel



Interface/Button	Description
DSL	For connecting to a phone cable
1	This RJ45 port is a WAN/LAN Interchangeable port. It works as a LAN port for connecting to a PC, switch and router, etc. when the device accesses the Internet via a phone cable and a WAN port for connecting to ISP when when the device accesses the Internet via an Ethernet cable. Note: The device is preset to access the Internet via a phone cable.
2/3	Local (LAN) Ethernet ports for cabling the device to local computers, switches, etc.
4	This port works as an IPTV/LAN interchangeable port. It works as a LAN port for cabling the device to a local computer, switch, router, etc. with IPTV disabled and as an IPTV-specific port with IPTV enabled. Note: The IPTV feature is disabled by default.
USB	For connecting to a 3G modem, USB printer or storage device
WPS/RST	This is a WPS/RST interchangeable button. <ul style="list-style-type: none"> ➤ Pressing this button for 3 seconds enables the WPS-PBC feature on the device (The WPS LED on the device blinks and clients can join the device's wireless network with via WPS-PBC). ➤ Pressing this button for 10 seconds resets the device to factory default settings.
PWR	Power Receptacle for connecting to the included power adapter.
ON/OFF	For turning on/off the device

1.2.3 Label



1 IP Address: Default Login IP address. This IP address is to be used to access the device's settings through a web browser.

2 User name/Password: Default Web Login user name and password

3 MAC: Physical address of the device's LAN port. The device's default SSID (wireless network name) is Tenda_XXXXXX (where XXXXXX is the last 6 characters of this MAC address).

4 WPS PIN: The device's WPS PIN code

Chapter 2 Get Started

2.1 Install Considerations

The operating distance or range of your wireless connection can vary significantly, depending on the physical placement of your device. For best performance, place your device:

- ✧ Near the center of the area where your computers, smart phones and other devices operate, and preferably within line of sight to your wireless devices.
- ✧ In an elevated location such as a high shelf, keeping the number of walls and ceilings between this device and your other devices such as computers and smart phones to a minimum.
- ✧ Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves or PCs.
- ✧ Away from any large metal surfaces, such as a solid metal door or aluminum studs.
- ✧ Away from other materials such as glass, insulated walls, fish tanks, mirrors, brick and concrete that can also affect your wireless signal.

2.2 What You Need Before You Start

Prepare the following according to how you access the Internet.

A. To access the Internet with a phone cable:

Before you start the installation process, you need to prepare the following:

Item	Number	Description
D303	1	Find it in your package
Power Adapter	1	Find it in your package
ADSL Splitter	1	The ADSL Splitter is not required if you do not need to install a telephone and the device at the same time.
Phone cable from the incoming Internet side	1	Provided by ISP

Ethernet Cable	1	Find it in your package
Phone Cable	2	Find it in your package
PC	1	With installed Web browser such as IE8 (or higher) or Google
Broadband Receipt	1	<p>Including VPI/VCI (optional), Internet connection type and corresponding information (indispensable; for details, see below)</p> <ul style="list-style-type: none"> ➤ PPPOE or PPPOA: User Name_____, Password_____ ➤ Dynamic IP/DHCP (No information required) ➤ Static IP or IPOA: IP Address_____._____._____._____ Subnet Mask_____._____._____._____ Default Gateway_____._____._____._____ Preferred DNS Server IP_____._____._____._____ Alternate DNS Server IP (optional)_____._____._____._____

B. To access the Internet with an Ethernet cable:

Before you start the installation process, you need to prepare the following:

Item	Number	Description
D303	1	Find it in your package
Power Adapter	1	Find it in your package
Ethernet cable from the incoming Internet side	1	Provided by ISP
Ethernet Cable	1	Find it in your package
PC	1	With installed Web browser such as IE8 (or higher) or Google
Broadband Receipt	1	<p>Including Internet connection type and corresponding information (indispensable; for details, see below)</p> <ul style="list-style-type: none"> ➤ PPPoE: User Name_____, Password_____ ➤ Dynamic IP/DHCP (No information required) ➤ Static IP: IP Address_____._____._____._____ Subnet Mask_____._____._____._____ Default Gateway_____._____._____._____ Preferred DNS Server IP_____._____._____._____ Alternate DNS Server IP (optional)_____._____._____._____

		Default Gateway _____. Preferred DNS Server IP _____. Alternate DNS Server IP (optional) _____
--	--	--

C. To access the Internet via a 3G mobile connection:

Item	Number	Description
D303	1	Find it in your package.
Power Adapter	1	Find it in your package.
3G modem	1	You need to buy a 3G modem and apply 3G Internet service from your local 3G ISP.
Ethernet Cable	1	Find it in your package.
PC	1	With installed Web browser such as IE8 (or higher) or Google

Chapter 3 Quick Internet Setup

3.1 Hardware Install

Install your device according to how you access the Internet.

A. To access the Internet with a phone cable:

Step 1: Connect to the Internet.

1. Connect the phone cable from the incoming Internet side to the **LINE** port of the ADSL splitter.
2. Connect the **MODEM** port of the ADSL splitter to the **DSL** port of your device with a phone cable.
3. Connect the **PHONE** port of the ADSL splitter and your telephone with another phone cable.

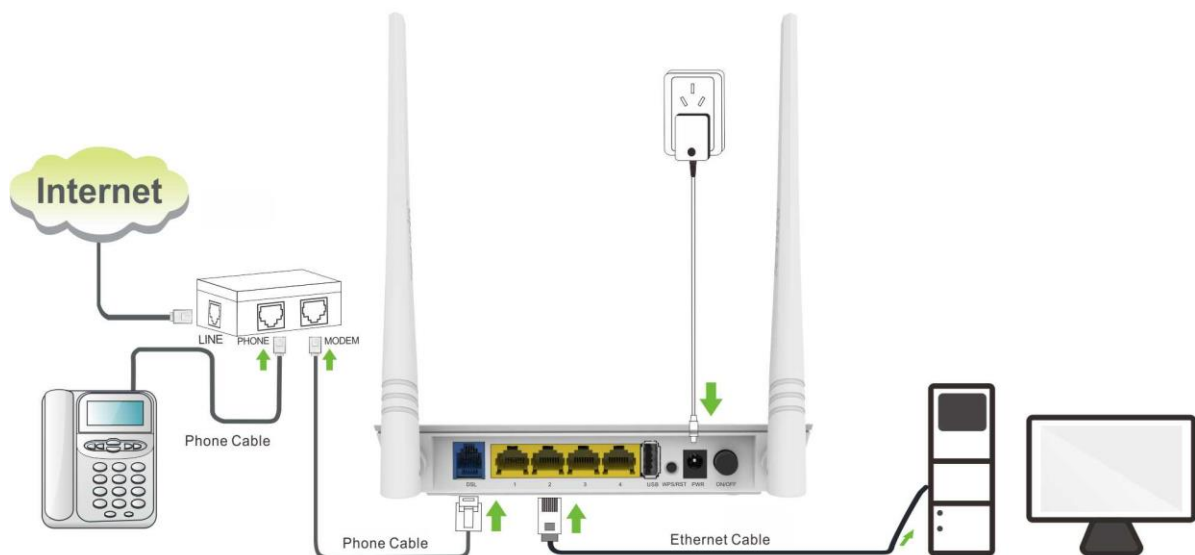
Step 2: Connect your device's port **1, 2, 3** or **4** and your PC's NIC port using an Ethernet cable.



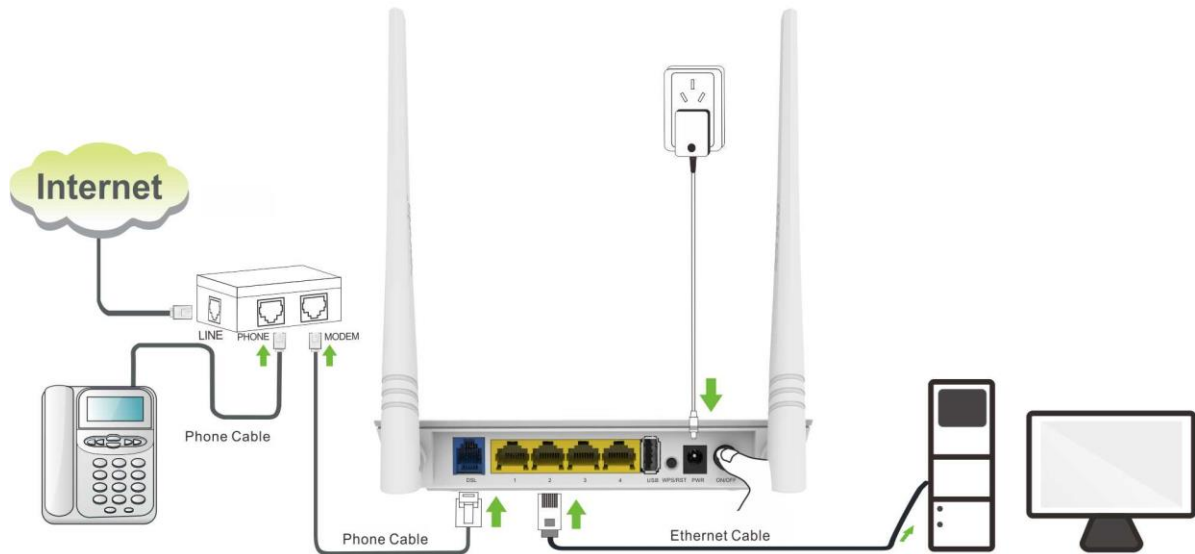
Tip:

With IPTV enabled (By default, the IPTV feature is disabled.), port **4** can only connect to an IPTV set-top box.

Step 3: Connect the device to a power outlet.



Step 4: Press the **ON/OFF** button to turn on the device.



Step 5: Check the device's LEDs, make sure the **PWR** and **DSL** LEDs are always on, the **WLAN** LED and the LED of a corresponding port that is connected to a PC are always on or blinking.



B. To access the Internet with an Ethernet cable

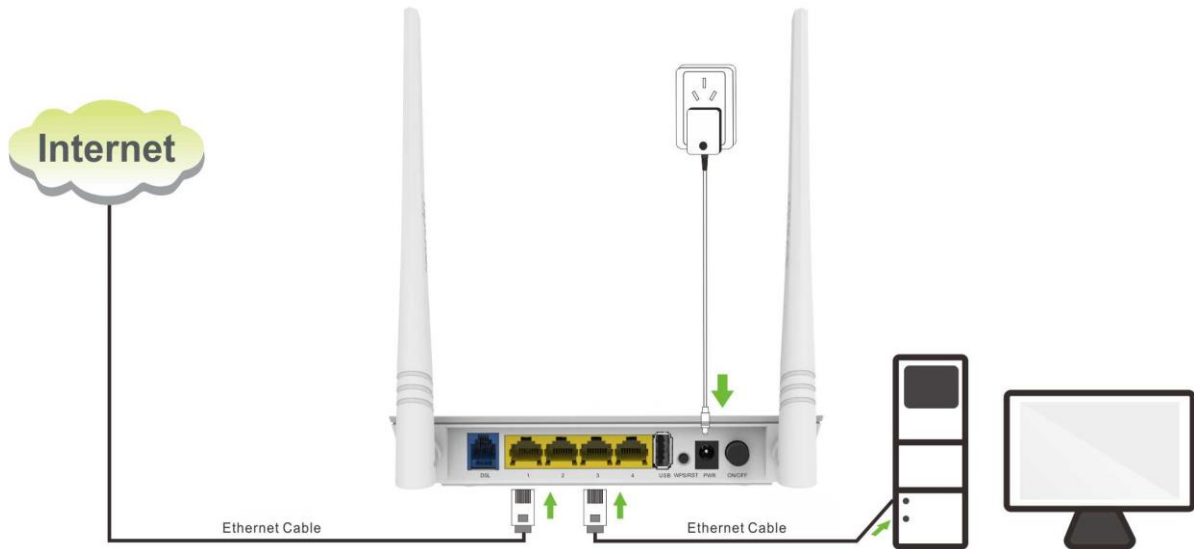
Step 1: Connect the Ethernet cable from the incoming Internet side to port **1** on your device.

Step 2: Connect your device's port **2, 3** or **4** and your PC's NIC port using an Ethernet cable.

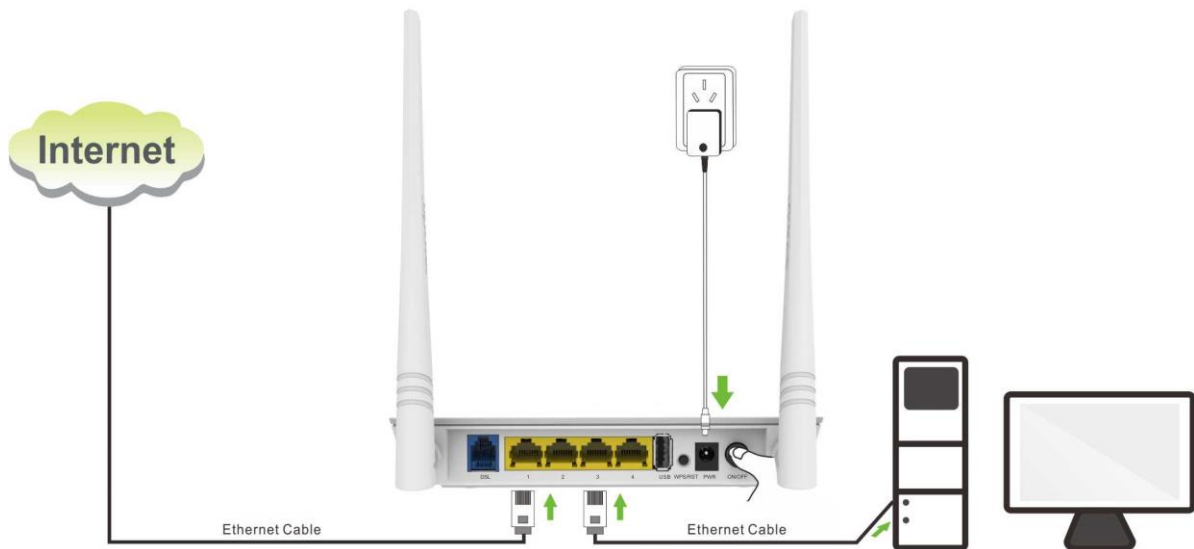


Tip: With IPTV enabled (By default, the IPTV feature is disabled.), port **4** can only connect to an IPTV set-top box.

Step 3: Connect the device to a power outlet.



Step 4: Press the **ON/OFF** button to turn on the device.



Step 5: Check the device's LEDs, make sure the **PWR** LED is always on, the **SYS** LED is blinking, the **WLAN** LED, the **1/WAN** LED and the LED of a corresponding port that is connected to a PC are always on or blinking.



C. To access the Internet via a 3G mobile connection:

Step 1: Insert the 3G modem in the device's USB port.

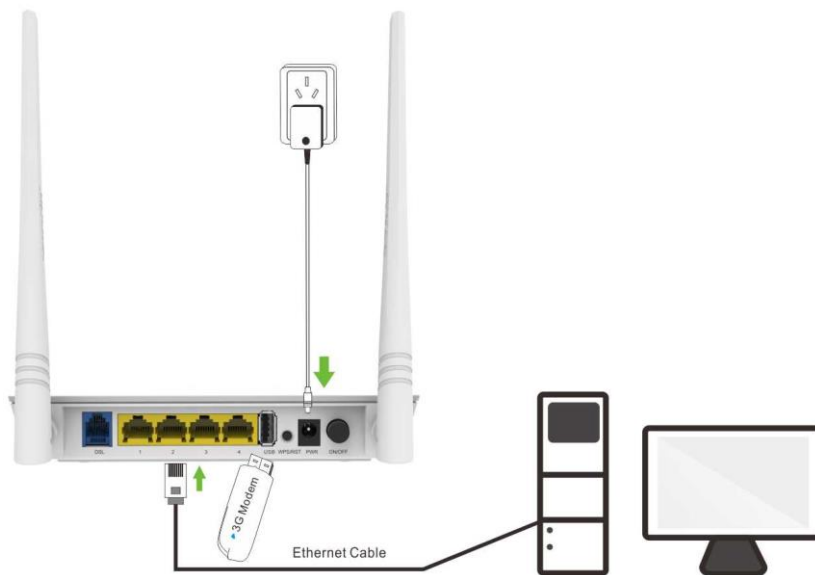
Step 2: Connect your device's port 1, 2, 3 or 4 and your PC's NIC port using an Ethernet cable.



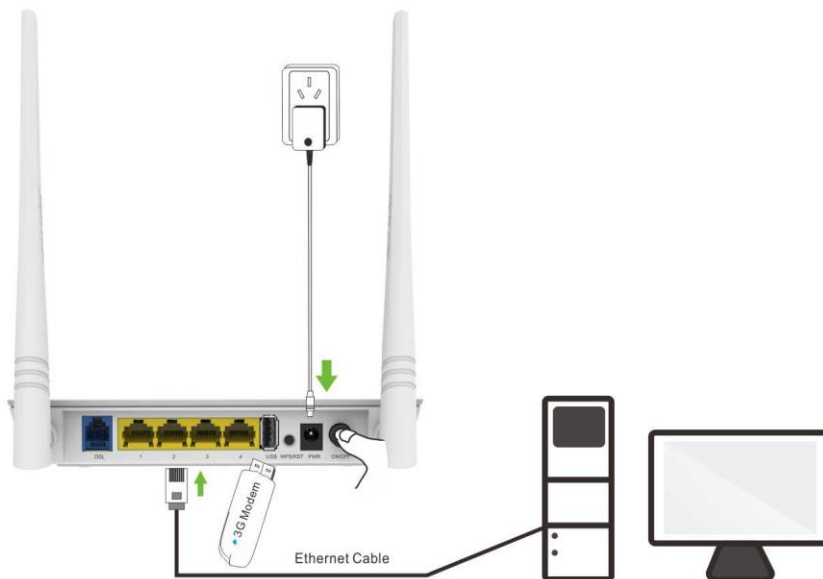
Tip:

With IPTV enabled (By default, the IPTV feature is disabled.), port 4 can only connect to an IPTV set-top box.

Step 3: Connect the device to a power outlet.



Step 4: Press the ON/OFF button to turn on the device.



Step 5: Check the device's LEDs, make sure they act as below:

The **WLAN** LED, **3G/USB** LEDs and the LED of a corresponding port that is connected to a PC are always on or blink;

The **SYS** LED blinks;

The **PWR** LED is always on.



Tip:

If the 3G/USB LED blinks for a while and then lights off, it indicates that the device fails to join a 3G network and is automatically unmounting and remounting the 3G modem for 3G connection. The device will not stop this process until it successfully joins a 3G network.

3.2 Connect to Your Device

If you access the Internet via a wired connection, follow instructions in [3.2.1 Configure Your PC](#) and then skip to [3.3 Internet Setup](#).

3.2.1 Configure Your PC

If your computer is set to a static or fixed IP address (This is uncommon), change it to "Obtain an IP address automatically" and "Obtain DNS server address automatically" from the device. See [Appendix 1 Configure Your PC](#) if you are not clear.

3.2.2 Join Your Wireless Network



Follow corresponding instructions below according to your OS.



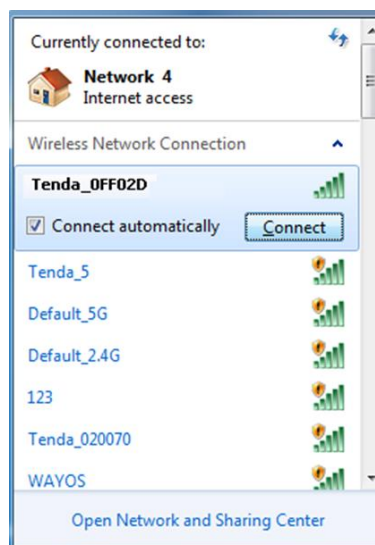
Tip:

- The device's SSID (wireless network) is "Tenda_XXXXXX" by default (where "XXXXXX" is the last six characters of the device's MAC address in the label).
- To join your wireless network, the PC you use must have an installed wireless network adapter. If not, install one.

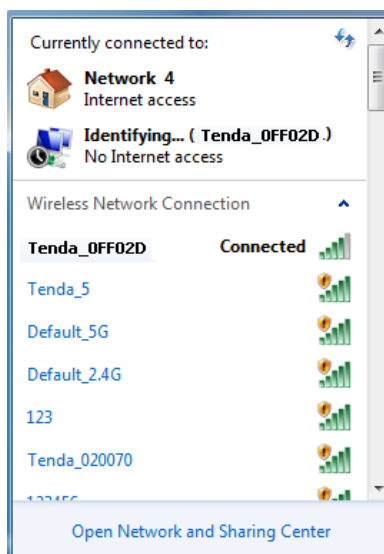
Windows 7

Step 1: Click  or  from the bottom right of your desktop.

Step 2: Double click the name of the wireless network (SSID) you wish to join and then follow onscreen instructions.

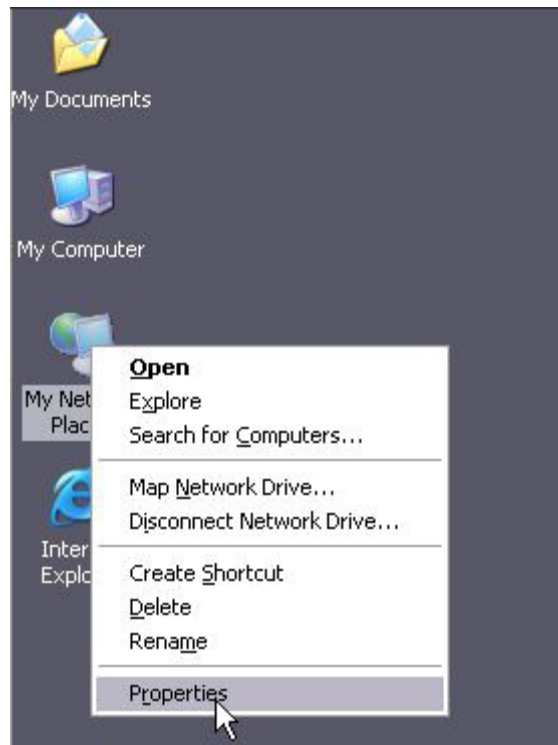


When **Connected** appears next to the selected wireless network (SSID), you have successfully connected to it.

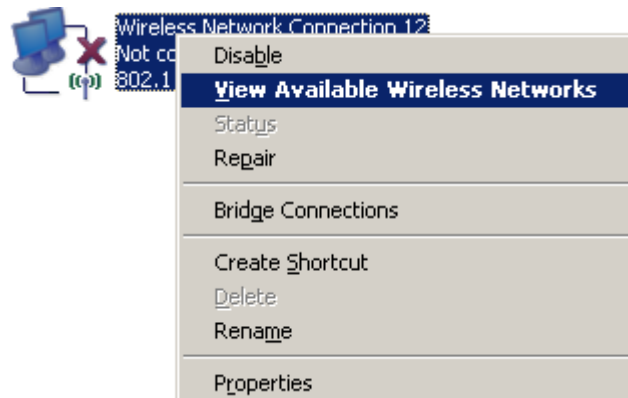


Windows XP

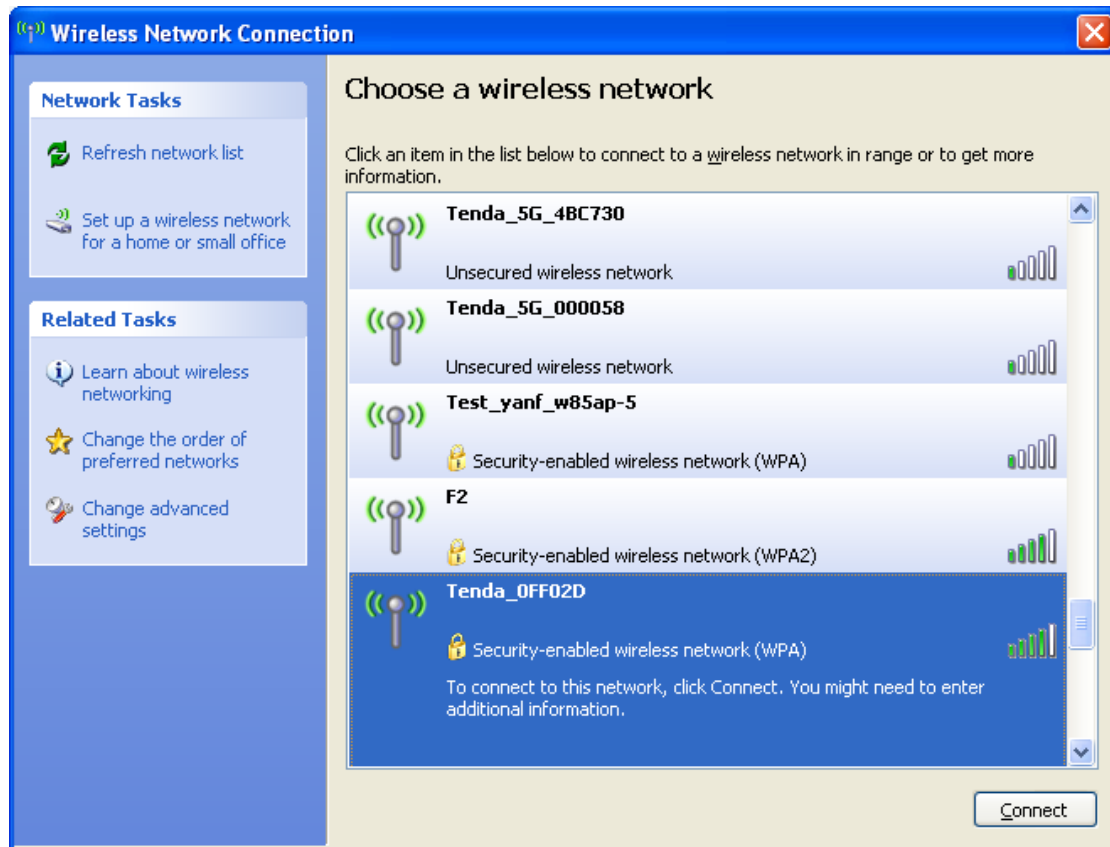
Step 1: Right click **My Network Places** and select **Properties**.



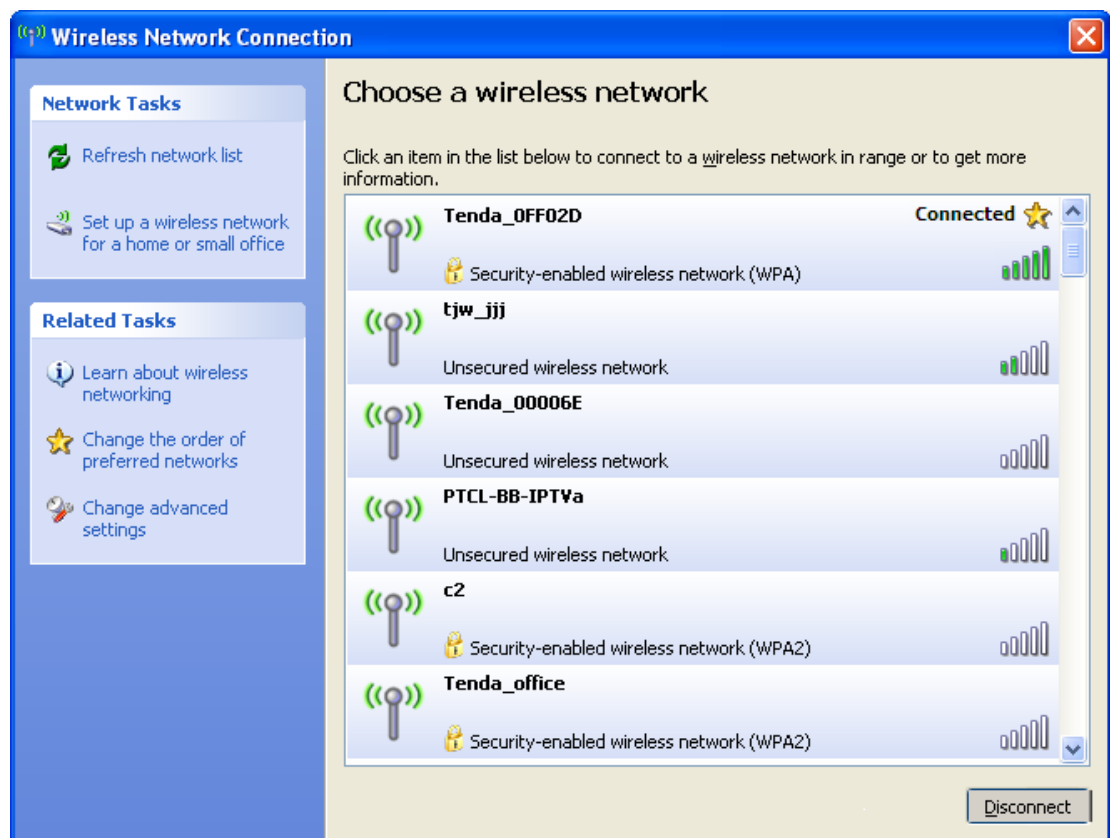
Step 2: Right click **Wireless Network Connection** and select **View available wireless networks**.



Step 3: Double click the name of the wireless network (SSID) you wish to join and then follow onscreen instructions.



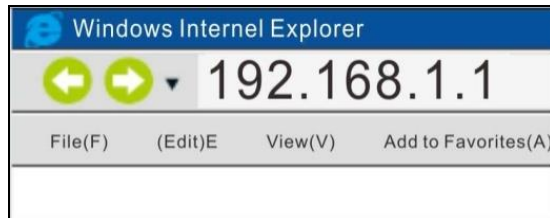
When **Connected** appears next to the selected wireless network (SSID), you have successfully connected to it.



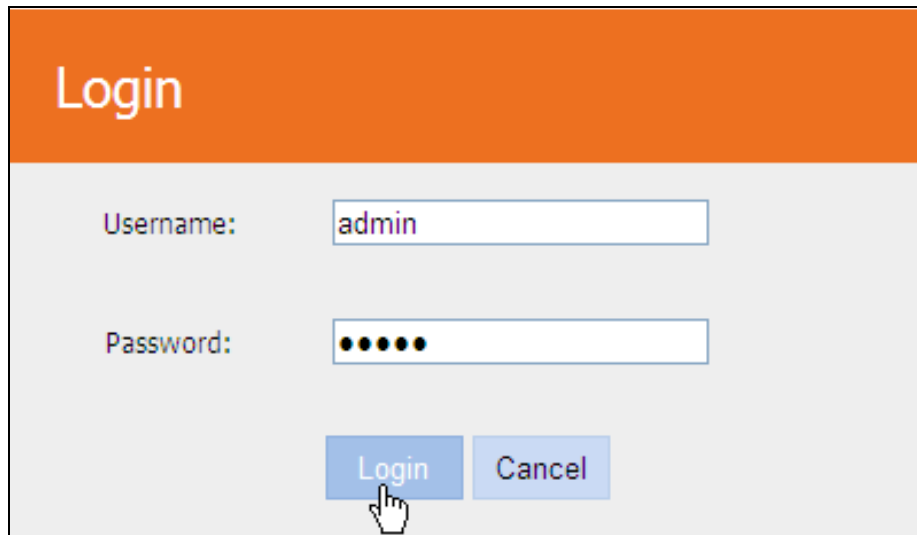
3.3 Internet Setup

3.3.1 Web Login

1. Launch a web browser, enter "192.168.1.1" and then press **Enter** or **Return**.



2. Enter user name and password (Both are preset to admin.) and click **Login**.



3. The home page displays.

Tenda E
easy life

DSL Wan/Lan1 Lan2 Lan3 Lan4/IPTV

Connected Disconnected

Connection Status ADSL/ETH:Unconfigured 3G:Connected

Primary Setup -- ADSL/ETH

Link Type Phone cable Ethernet cable

Country

ISP

VPI/VCI VPI (0-255) VCI (32-65535)

Connection Type

User Name (maxlength is 64)

Password (maxlength is 64)

Secondary Setup -- 3G Dial Enable 3G:

ISP:

APN:

Dial number:

Username:

Password:

Net Select:

Wireless Setup Enable Wireless:

Wireless SSID

Wireless Key

Wireless Key is made up of 8-63 ASCII or 64 hex characters.

Here you can view the connection status of each port and configure Internet and wireless settings. Also, you can click # **Advanced** to enter more configuration interfaces and click # **IPTV** to enter the IPTV configuration interface.

The following interface displays if you click # **Advanced**.

The screenshot shows the Tenda web interface. On the left is a navigation bar with a '1' indicating it is the focus of the first description. The main content area has a '2' indicating it is the focus of the second description. The 'Device Info' section contains the following data:

Board ID:	96318REF
Build Timestamp:	140228_1923
Software Version:	V5.2.1.3
Hardware Version:	V1.0.0
Bootloader (CFE) Version:	1.0.38-114.185
DSL PHY and Driver Version:	A2pG039d1.d24h
Wireless Driver Version:	6.30.102.7.cpe4.12L08.4
Uptime:	0D 0H 49M 15S

Below this is a note: "This information reflects the current status of your WAN connection." The 'WAN Connection' section contains the following data:

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Thu Jan 1 00:49:15 1970


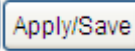

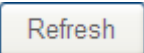

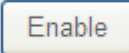
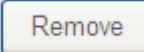
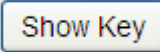
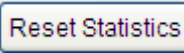
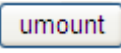
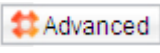
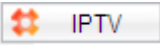
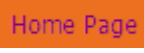
Description of the Web interface:

ID	Area	Description
1	Navigation Bar	Includes a list of different menus of features that can be selected and can be expanded to display all the components in configuration area.
2	Configuration Area	For users to configure and view parameters



Unsupported features do not appear in the navigation bar of the Web page. For actualities of features, refer to the actual firmware.

Explanation of Common Components in Web Interface:

Common Components	Description
 	Activate settings in the current page.
	Return to the previous configuration interface.
	Refresh the current page.
	Add a configuration rule.
	Enable a corresponding configuration rule.
	Delete a corresponding configuration rule.
	Display the security key.
	Reset (clear) statistics information.
	Unload the attached USB storage device.
	Click to enter more configuration interfaces.
	Click to enter IPTV configuration interface.
	Click to return to the device's home page.

3.3.2 Internet Setup & Wireless Setup

Select corresponding settings according to how you access the Internet.

A. Internet Setup (for Phone Cable) & Wireless Setup

- 1. Link Type:** Select **Phone Cable**.
- 2. Country/ISP/VPI/VCI:** Select your country and ISP, and system will automatically generate VPI/VCI settings.



If your ISP is included in the integrated list, select **Other** and then manually enter VPI and VCI settings (Consult your ISP if you don't know the VPI and VCI values.).

3. **Internet Setup:** Configure Internet settings according to the information in your broadband service receipt.

Primary Setup -- ADSL/ETH

Link Type Phone cable Ethernet cable

Country

ISP

VPI/VCI VPI (0-255) VCI (32-65535)

Connection Type

User Name (maxlength is 64)

Password (maxlength is 64)

4. **Wireless SSID/Wireless Key:** Configure your **Wireless SSID** and **Wireless key**.

Wireless Setup Enable Wireless:

Wireless SSID

Wireless Key

Wireless Key is made up of 8-63 ASCII or 64 hex characters.



Tip:

If you click **Save** without customizing the wireless SSID and wireless key, then the wireless SSID is Tenda_XXXXXX (where "XXXXXX" is the last six characters of the device's MAC address in the label attached to the device) and wireless key is 12345678.

5. Click **Save**.

If you access the Internet via a wired connection, you can now access the Internet when finishing the required settings. If you access the Internet via a wireless connection, follow instructions in **Join Your Wireless Network** to reconnect to the device.

B. Internet Setup (for Ethernet Cable) & Wireless Setup

1. **Link Type:** Select **Ethernet Cable**.
2. **Internet Setup:** Configure Internet settings according to the information in your broadband service receipt.

Primary Setup -- ADSL/ETH

Link Type Phone cable Ethernet cable

Connection Type

User Name (maxlength is 64)

Password (maxlength is 64)

3. Wireless SSID/Wireless Key: Configure your **Wireless SSID** and **Wireless key**.

Wireless Setup Enable Wireless:

Wireless SSID

Wireless Key

Wireless Key is made up of 8-63 ASCII or 64 hex characters.



Tip:

If you click **Save** without customizing the wireless SSID and wireless key, then the wireless SSID is Tenda_XXXXXX (where "XXXXXX" is the last six characters of the device's MAC address in the label attached to the device) and wireless key is 12345678.

4. Click Save.

If you access the Internet via a wired connection, you can now access the Internet when finishing the required settings. If you access the Internet via a wireless connection, follow instructions in [3.2.2 Join Your Wireless Network](#) to reconnect to the device.

C. 3G Internet Setup & Wireless Setup

1. Country: Select your country.

2. Select your 3G ISP and system will automatically populate the relevant fields. If your ISP is not included in the integrated list, select **Other** and manually enter the required information (Consult your ISP, if you are not clear.).

Secondary Setup -- 3G Dial Enable 3G:

Country:	Argentina	▼	
ISP:	Movistar AR	▼	
APN:	internet.gprs.unifon.com.ar		
Dial number:	*99#		
Username:	internet		
Password:	internet		
Net Select:	Auto		▼

3. Wireless SSID/Wireless Key: Configure your **Wireless SSID** and **Wireless key**.

Wireless Setup Enable Wireless:

Wireless SSID	Tenda_211011	
Wireless Key	●●●●●●●●	<input type="button" value="Show Key"/>

Wireless Key is made up of 8-63 ASCII or 64 hex characters.



Tip:

If you click **Save** without customizing the wireless SSID and wireless key, then the wireless SSID is Tenda_XXXXXX (where "XXXXXX" is the last six characters of the device's MAC address in the label attached to the device) and wireless key is 12345678.

4. Click Save.

If you access the Internet via a wired connection, you can now access the Internet when finishing the required settings. If you access the Internet via a wireless connection, follow instructions in [3.2.2 Join Your Wireless Network](#) to reconnect to the device.

Chapter 4 Advanced Settings

This chapter describes the advanced features of your router.

The information is for users with a solid understanding of networking concepts who want to configure the router for unique situations.

This chapter includes the following sections:

- [Device Info](#)
- [Advanced Setup](#)
- [Wireless](#)
- [Diagnostics](#)
- [Management](#)

Click **Advanced** on the home page to enter the screen below.

Device Info	
Board ID:	96318REF
Build Timestamp:	140318_0909
Software Version:	V5.2.1.3
Hardware Version:	V1.0.0
Bootloader (CFE) Version:	1.0.38-114.185
DSL PHY and Driver Version:	A2pG039d1.d24h
Wireless Driver Version:	6.30.102.7.cpe4.12L08.4
Uptime:	0D 0H 1M 57S

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Thu Jan 1 00:01:57 1970

4.1 Device Info

This section includes the following information:

- [Summary](#)
- [WAN](#)
- [Statistics](#)
- [Route](#)
- [ARP](#)
- [DHCP](#)

Summary

Here you can view system information and current status of your WAN connection as seen in the screenshot.

Device Info	
Board ID:	96318REF
Build Timestamp:	140318_0909
Software Version:	V5.2.1.3
Hardware Version:	V1.0.0
Bootloader (CFE) Version:	1.0.38-114.185
DSL PHY and Driver Version:	A2pG039d1.d24h
Wireless Driver Version:	6.30.102.7.cpe4.12L08.4
Uptime:	0D 0H 1M 57S

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Thu Jan 1 00:01:57 1970

WAN

Here you can view the WAN Information including Interface, Description, Type, IGMP, NAT, Firewall, Status, IPv4 Address and VLAN ID as seen in the screenshot.

WAN Info											
Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
eth0.1	ipoe_eth0	IPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	192.168.130.104	

USB-3G WAN Info						
Interface	Status	IPv4 Address	net mask	dns1	dns2	gateway
ppp3g0	Disconnect	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Statistics

Here you can view the packets received and transmitted on LAN/WAN ports.

Statistics--LAN: Displays the packets received and transmitted on the LAN ports as seen in the screenshot below.

Statistics -- LAN								
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth1	0	0	0	0	0	0	0	0
eth2	152947	1057	0	0	982875	1614	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	5044	60	0	0

Statistics--WAN: Displays the packets received and transmitted on the WAN ports as seen in the screenshot below.

Statistics -- WAN									
Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0.1	ipoe_eth0	160732	1744	0	0	1648	8	0	0

Statistics--ADSL: Displays the packets received and transmitted over the ADSL link as seen in the screenshot below.

Statistics -- ADSL		
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		

Route

Here you can view the route table as seen in the screenshot:

Device Info -- Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.130.130	192.168.130.130	255.255.255.255	UGH	0	ipoe_eth0	eth0.1
192.168.130.0	0.0.0.0	255.255.255.0	U	0	ipoe_eth0	eth0.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	192.168.130.130	0.0.0.0	UG	0	ipoe_eth0	eth0.1

ARP

Here you can view the IP and MAC addresses of the PCs that attach to the device either via a wired or wireless connection as seen in the screenshot:

IP address	Flags	HW Address	Device
192.168.1.100	Complete	c8:9c:dc:3b:ac:89	br0

DHCP

Here you can view the DHCP leases, including IP and MAC addresses of the PCs, hostnames and remaining lease time as seen in the screenshot:

Hostname	MAC Address	IP Address	Expires In
INVE-20140221TG	c8:9c:dc:3b:ac:89	192.168.1.100	23 hours, 59 minutes, 56 seconds

4.2 Advanced Setup

This section explains the following information:

- [Layer2 Interface](#)
- [WAN Service](#)
- [USB Application](#)
- [LAN](#)
- [NAT](#)
- [Security](#)
- [Parental Control](#)
- [Quality of Service](#)
- [Routing](#)
- [DNS](#)

- [DSL](#)
- [UPnP](#)
- [Interface Grouping](#)
- [IP Tunnel](#)
- [Certificate](#)
- [Multicast](#)
- [IPTV](#)

4.2.1 Layer2 Interface

Click **Advanced Setup** -> **Layer2 Interface** to enter the Layer2 Interface screen.

This router provides two Layer2 Interfaces:

- **ATM Interface** for ADSL broadband Internet service
- **ETH Interface** for connecting to the Internet via an Ethernet cable.

By default, system applies the ATM Interface (ADSL uplink).

If you directly connect to the ADSL line via a phone cable, first refer to [To set up the ATM interface](#) and then skip to [To set up WAN Service for ATM Interface](#).

Or if you connect to the Internet via a fiber/cable modem using an Ethernet cable, first refer to [To set up the ETH interface](#) and then skip to [To set up WAN Service for ETH Interface](#).

DSL ATM Interface Configuration													
Choose Add, or Remove to configure DSL ATM interfaces.													
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Min Cell Rate(cells/s)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>													

To set up the ATM interface

Select **ATM Interface** and click **Add** to configure it.

DSL ATM Interface Configuration													
Choose Add, or Remove to configure DSL ATM interfaces.													
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Min Cell Rate(cells/s)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>													

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: [0-255]
VCI: [32-65535]

Select DSL Latency
 Path0 (Fast)
 Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
 EoA
 PPPoA
 IPoA

Encapsulation Mode:

Service Category:

Minimum Cell Rate: [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue
 Weighted Round Robin
 Weighted Fair Queuing

Default Queue Weight: [1-63]

Enter the VPI and VCI values, Select a DSL Link Type (Internet connection type): EoA (EoA is for PPPoE, IPoE, and Bridge.), PPPoA or IPoA, leave other options unchanged from factory defaults and click **Apply/Save** and then refer to [To set up WAN Service for ATM Interface](#) to configure the WAN service for the Internet access.



Tip:

If you are unsure about the VPI/VCI parameters, see [Appendix 3 VPI/VCI List](#). Or if your ISP and the VPI/VCI information is not covered there, ask your ISP to provide it.

To set up the ETH interface

1. Click **Add** to display the **ETH WAN Configuration** screen.
2. Select **eth0/eth0** as the ETH port.
3. Click the **Apply/Save** button and then refer to [To set up WAN Service for ETH Interface](#) to

configure the WAN service for Internet access.

ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove
<div style="display: flex; justify-content: center; gap: 20px;"> Add Remove </div>		

ETH WAN Configuration

This screen allows you to configure a ETH port .

Select a ETH port:

eth0/eth0 ▼

Back
Apply/Save

The Ethernet port configured here is to function as a WAN port. Only eth0/eth0 can be configured as the WAN port.

4.2.2 WAN Service

This router provides two WAN services:

- WAN Service for ATM Interface (ADSL uplink)
- WAN Service for ETH Interface (Ethernet uplink)

To setup WAN Service for ATM Interface

If you configured the **ATM Interface** (ADSL uplink), follow steps below to configure the WAN service:

Click **Advanced Setup** -> **WAN Service** and then click the **Add** button. Select the interface you have configured

Depending on the type of connection, you will come to different screens and be prompted to enter your ISP settings accordingly. Select one connection type from the five Internet connection types as shown in the following table (If you are unsure, consult your ISP.):

Internet Connection Type		ISP Information
PPPoE PPPoA		Enter the ISP login user name and password. If you cannot locate this information, ask your ISP to provide it.
IPoE (If your ISP uses DHCP to assign your IP address or if your ISP assigns you a static (fixed) IP address, IP subnet mask and the gateway IP address, you need to select the IP over Ethernet (IPoE).	Dynamic IP	No entries are needed.
	Static (Fixed) IP	Enter the assigned IP address, subnet mask, and the IP address of your ISP's primary DNS server. This information should have been provided to you by your ISP. If a secondary DNS server address is available, enter it also.
IPoA	Static (Fixed) IP	Enter the assigned IP address, subnet mask, and the IP address of your ISP's primary DNS server. This information should have been provided to you by your ISP. If a secondary DNS server address is available, enter it also.
Bridging		If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead of sharing it with others), you can select the Bridging and then click Next .



Tip:

For PPPoE, IPoE, and Bridging Internet connection types, you must first select EoA on the ATM Interface Screen, for more information, see [To set up the ATM interface](#).

PPP over Ethernet (PPPoE)

If you have selected the EoA from the **ATM Interface** screen in **Layer2 Interface**, you will see the screen below when you click the **WAN Service** tab, select the configured interface and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

1. Select **PPPoE**.
2. Edit the **Enter Service Description**. This field is optional. We recommend that you keep the default.
3. Select a network protocol: IPv4, IPv6 or IPv4 & IPv6 (dual stack).
4. Click **Next**.



If you select IPv6 or IPv4 & IPv6 (dual stack), skip to [IPv6](#).

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

MAC Clone:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

- ✧ **PPP User Name:** This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.
- ✧ **PPP Password:** This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.
- ✧ **PPPoE Service Name:** This information is provided by your ISP. Only enter it if instructed by your ISP.
- ✧ **Authentication Method:** This is used by ISP to authenticate the client that attempts to connect. If you are not sure, consult your ISP or select **Auto**.
- ✧ **Clone MAC:** Clicking this button copies the MAC address of your PC to the router. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally register the MAC address of the network interface card in your computer when your account is first opened. They then accept traffic only from the MAC address of that computer. If so, configure your router to “clone” the MAC address from the authorized computer.
- ✧ **Dial on demand:** Connect to ISP only when there is traffic transmission. This saves your broadband Internet service bill.
- ✧ **PPP IP extension:** If enabled, all the IP addresses in outgoing packets including management packets on the WAN port will be changed to the device's WAN IP address. Only change the default settings if necessary.

- ❖ **Enable PPP Debug Mode:** Only enable this feature if supported by your ISP.
- ❖ **Bridge PPPoE Frames Between WAN and Local Ports:** If enabled, PPPoE dialup frame from LAN side will directly egress the WAN port without modification.
- ❖ **Multicast Proxy:** If enabled, the router will use multicast proxy.

IPv6

If you select IPv4 as the network protocol, skip this section.

PPP IP extension

Use Static IPv4 Address

Use Static IPv6 Address

Enable IPv6 Unnumbered Model

Launch Dhcp6c for Address Assignment (IANA)

Launch Dhcp6c for Prefix Delegation (IAPD)

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

Enable MLD Multicast Proxy

1. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**.
2. If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also. Or configure a static IP address.
3. Click **Next -> Next -> Apply/Save**.

WAN Gateway

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	<input type="button" value="→"/> <input type="button" value="←"/>	

Here you can configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.



Note:

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

WAN DNS

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
ppp0.1	<input type="button" value="→"/> <input type="button" value="←"/>	

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Here you can configure the WAN DNS address:

-Click the **Select DNS Server Interface from available WAN interfaces** option

-OR select the **Use the following Static DNS IP address** option and enter static DNS server IP

addresses for the system

And then click **Next**.



Note:

- DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
 - In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
 - If you cannot locate the static DNS server IP information, ask your ISP to provide it.
-

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

When the PPPoE connection is successful, you can access the Internet.

IP over Ethernet (IPoE)

If your ISP uses DHCP to assign your IP address or if your ISP assigns you a static (fixed) IP address, IP subnet mask and the gateway IP address, you need to select the IP over Ethernet (IPoE).

If you have selected the **EoA** from the **ATM Interface** screen in **Layer2 Interface**, you will see the screen below when you click the **WAN Service** tab, select the configured interface and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

IPv4 Only
 IPv4&IPv6(Dual Stack)
 IPv6 Only

1. Select IPoE.
2. Edit the **Enter Service Description** (optional). We recommend that you keep the default.
3. Select a network protocol: IPv4, IPv6 or IPv4 & IPv6 (dual stack).
4. Click **Next**.



Note:

If you select IPv6 or IPv4 & IPv6 (dual stack), skip to [IPv6](#).

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

- ✧ **Obtain an IP address automatically:** This allows the router to automatically acquire IP information from your ISP or your existing networking equipment.
- ✧ **Use the following Static IP address:** This allows you to specify the Static IP information provided by your ISP or that corresponds with your existing networking equipment.
- ✧ **WAN IP Address:** The Internet IP address provided by your ISP for accessing the Internet.
- ✧ **WAN Subnet Mask:** The subnet mask address provided by your ISP for accessing the Internet.
- ✧ **WAN gateway IP Address:** The gateway IP address provided by your ISP for accessing the Internet.

IPv6

If you select IPv4 as the network protocol, skip this section.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.

Notice:

If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.

If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

To obtain an IP address automatically:

1. Select **Obtain an IP address automatically**.
2. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**.
3. If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)**.
4. Click **Next -> Next -> Apply/Save**.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.

Notice:

If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.

If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

To configure a static IPv6 address

1. Select **Use the following Static IPv6 address**.
2. Configure **WAN IPv6 Address/Prefix Length** and **WAN Next-Hop IPv6 Address**.

Use the following Static IP address:
 WAN IP Address:
 WAN Subnet Mask:
 WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.

Notice:
 If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
 If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

Obtain an IPv6 address automatically
 Dhcpv6 Address Assignment (IANA)
 Dhcpv6 Prefix Delegation (IAPD)
 Use the following Static IPv6 address:
 WAN IPv6 Address/Prefix Length:

Specify the Next-Hop IPv6 address for this WAN interface.

Notice: This address can be either a link local or a global unicast IPv6 address.

WAN Next-Hop IPv6 Address:

3. Click **Next** -> **Next** to enter the screen below.

Use the following Static DNS IP address:
 Primary DNS server:
 Secondary DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses
 Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:
 WAN Interface selected:

Use the following Static IPv6 DNS address:
 Primary IPv6 DNS server:
 Secondary IPv6 DNS server:

4. Select **Use the following Static IPv6 DNS address** and manually enter the DNS server address. If you have two DNS server addresses, enter the second also.
5. Click **Next -> Apply/Save**.



Note:

If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT
 Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast
 No Multicast VLAN Filter

Here you can configure the NAT settings. If you are unsure about the options, please keep the default settings and then click **Next**.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0.1	atm0.2

Here you can configure the WAN gateway address. Default gateway interface list can have multiple

WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

If you are unsure about the options, please keep the default settings and then click **Next**.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

ppp0.1 atm0.2

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Here you can configure the WAN DNS address:

-Click the **Select DNS Server Interface from available WAN interfaces** option

-OR select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system

And then click **Next**.



Note:

- DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
 - In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
 - If you cannot locate the static DNS server IP information, ask your ISP to provide it.
-

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm0.2	ipoe_0_0_35	IPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

When the IPoE connection is successful, you can access the Internet.

Bridging

If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead of sharing it with others), you can use the Bridging DSL link type and create a dialup program on your PC.

If you have selected the **EoA** from the **ATM Interface** screen in **Layer2 Interface**, you will see the screen below when you click the **WAN Service** tab, select the configured interface and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

The **Enter Service Description** field is optional. We recommend that you keep it unchanged from default and click **Next**.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm0.1	br_0_0_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

When the bridging connection is successful, you can access the Internet.



Note:

To configure multiple WAN connections, simply configure multiple ATM interfaces and then follow the instructions above.

PPPoA

If you have selected the **PPPoA** from the **ATM Interface** screen in **Layer2 Interface**, you will see the screen below when you click the **WAN Service** tab, select the configured interface and click **Next**.

WAN Service Configuration

Enter Service Description:

Network Protocol Selection:

-
-
-
-

1. Edit the **Enter Service Description**. This field is optional. We recommend that you keep the default.
2. Select a network protocol: IPv4, IPv6 or IPv4 & IPv6 (dual stack).
3. Click **Next**.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Use Static IPv4 Address

Enable PPP Debug Mode

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

✧ **PPP User Name:** This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.

✧ **PPP Password:** This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.

✧ **Authentication Method:** This is used by ISP to authenticate the client that attempts to connect. If you are not sure, consult your ISP or select **Auto**.

✧ **Dial on demand:** Connect to ISP only when there is traffic transmission. This saves your broadband Internet service bill.

✧ **Enable PPP Debug Mode:** Only enable this feature if supported by your ISP.

✧ **Bridge PPPoE Frames Between WAN and Local Ports:** If enabled, PPPoE dialup frame from LAN side will directly egress the WAN port without modification.

✧ **Multicast Proxy:** If enabled, the router will use multicast proxy.

If you are not sure about the options on this screen, simply enter your ISP user name and password and leave the other options unchanged from defaults. Click **Next** to enter the following screen.

WAN gateway

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

Available Routed WAN Interfaces

pppoe0

>>
<<

Back Next

Here you can configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.



Note:

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

WAN DNS

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

Available WAN Interfaces

pppoe0

>>
<<

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Here you can configure the WAN DNS address:

-Click the **Select DNS Server Interface from available WAN interfaces** option

-OR select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system

And then click **Next**.



Note:

- DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
- In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
- If you cannot locate the static DNS server IP information, ask your ISP to provide it.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

Wide Area Network (WAN) Service Setup

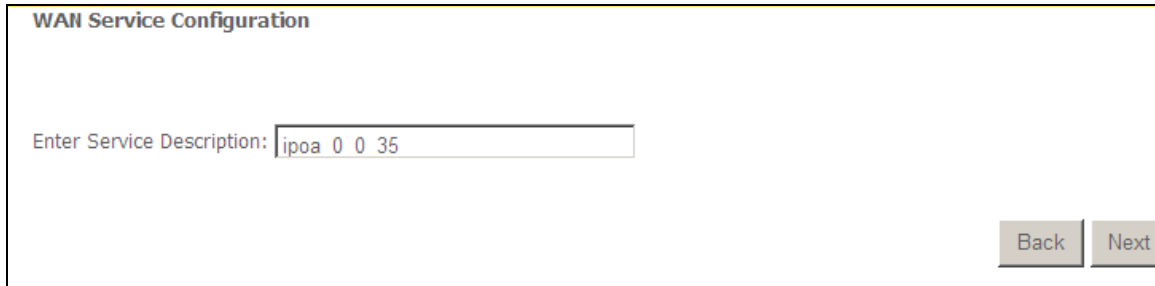
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0a0	ppp0a_0_6_35	PPPoA	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

When the PPPoA connection is successful, you can access the Internet.

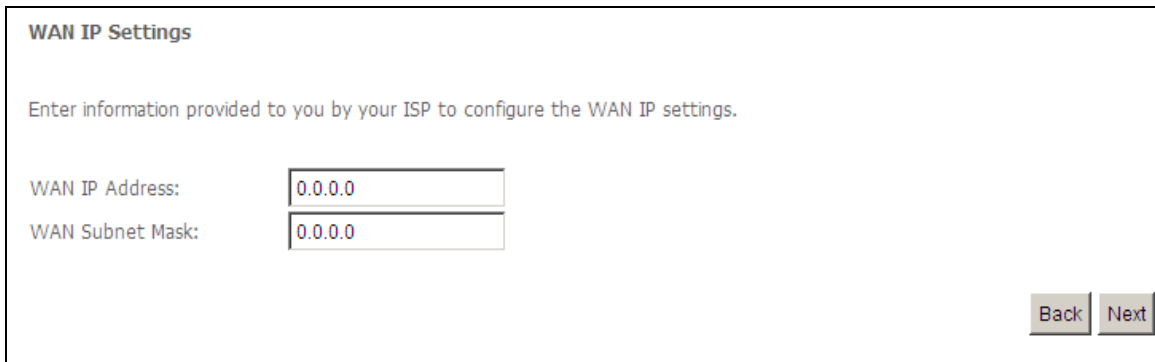
IPoA

If you have selected the **IPoA** from the **ATM Interface** screen in **Layer2 Interface**, you will see the screen above when you click the **WAN Service** tab, select the configured interface and click **Next**.



The screenshot shows the 'WAN Service Configuration' screen. It features a text input field labeled 'Enter Service Description:' with the value 'ipoa 0 0 35'. At the bottom right, there are two buttons: 'Back' and 'Next'.

1. Edit the **Enter Service Description**. This field is optional. We recommend that you keep the default.
2. Click **Next**.



The screenshot shows the 'WAN IP Settings' screen. It includes the instruction 'Enter information provided to you by your ISP to configure the WAN IP settings.' Below this, there are two input fields: 'WAN IP Address:' with the value '0.0.0.0' and 'WAN Subnet Mask:' with the value '0.0.0.0'. At the bottom right, there are two buttons: 'Back' and 'Next'.

- ✧ **WAN IP Address:** The Internet IP address provided by your ISP for accessing the Internet.
- ✧ **WAN Subnet Mask:** The subnet mask address provided by your ISP for accessing the Internet.

Enter the WAN IP address and subnet mask assigned by your ISP. This information should have been provided to you by your ISP. If you cannot locate this information, ask your ISP to provide it. And then click **Next** to enter the following screen.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN)

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

No Multicast VLAN Filter

If you are unsure about the options on the screen above, keep the defaults and click **Next**.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

Available Routed WAN Interfaces

ipoa0

Here you can configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.



Note:

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

->

-<

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Here you can configure the WAN DNS address:

-Click the **Select DNS Server Interface from available WAN interfaces** option

-OR select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system

And then click **Next** to enter the following screen.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

 **Note:**

- DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
- In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
- If you cannot locate the static DNS server IP information, ask your ISP to provide it.

Confirm your settings and then click Apply/Save to apply and save your settings. Your settings will then be displayed on the screen below:

Wide Area Network (WAN) Service Setup											
Choose Add, Remove or Edit to configure a WAN service over a selected interface.											
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ipoa0	ipoa_0_0_35	IPoA	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

To setup WAN Service for ETH Interface

After you configured the **ETH Interface** (eth0/eth0), follow steps below to configure the WAN service.

Two Internet connections: PPP over Ethernet (PPPoE) and IP over Ethernet (IPoE) are available in the Ethernet uplink mode.

PPP over Ethernet (PPPoE)

Click **Advanced Setup** -> **WAN Service** -> **Add**, select the configured interface and then click **Next** to enter the following screen.

WAN Service Configuration	
Select WAN service type:	
<input checked="" type="radio"/>	PPP over Ethernet (PPPoE)
<input type="radio"/>	IP over Ethernet
<input type="radio"/>	Bridging
Enter Service Description: <input type="text" value="pppoe eth3"/>	
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.	
Enter 802.1P Priority [0-7]:	<input type="text" value="-1"/>
Enter 802.1Q VLAN ID [0-4094]:	<input type="text" value="-1"/>
Network Protocol Selection:	
<input type="text" value="IPV4 Only"/> <ul style="list-style-type: none"> IPV4 Only IPV4&IPV6(Dual Stack) IPV6 Only 	
<input type="button" value="Back"/> <input type="button" value="Next"/>	

1. Select PPPoE.

2. Edit the **Enter Service Description**. This field is optional. We recommend that you keep the default.
3. Select a network protocol: IPv4, IPv6 or IPv4 & IPv6 (dual stack).
4. Click **Next**.



Note:

If you select IPv6 or IPv4 & IPv6 (dual stack), skip to [IPv6](#).

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

MAC Clone:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

- ✧ **PPP User Name:** This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.
- ✧ **PPP Password:** This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.
- ✧ **PPPoE Service Name:** This information is provided by your ISP. Only enter it if instructed by your ISP.
- ✧ **Authentication Method:** This is used by ISP to authenticate the client that attempts to connect. If you are not sure, consult your ISP or select **Auto**.
- ✧ **Clone MAC:** Clicking this button copies the MAC address of your PC to the router. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally register the MAC address of the network interface card in your

computer when your account is first opened. They then accept traffic only from the MAC address of that computer. If so, configure your router to “clone” the MAC address from the authorized computer.

✧ **Dial on demand:** Connect to ISP only when there is traffic transmission. This saves your broadband Internet service bill.

✧ **PPP IP extension:** If enabled, all the IP addresses in outgoing packets including management packets on the WAN port will be changed to the device's WAN IP address. Only change the default settings if necessary.

✧ **Enable PPP Debug Mode:** Only enable this feature if supported by your ISP.

✧ **Bridge PPPoE Frames Between WAN and Local Ports:** If enabled, PPPoE dialup frame from LAN side will directly egress the WAN port without modification.

✧ **Multicast Proxy:** If enabled, the router will use multicast proxy.

If you are not sure about the options on this screen, simply enter your ISP user name and password and leave the other options unchanged from defaults. Click **Next**.

IPv6

If you select IPv4 as the network protocol, skip this section.

PPP Password:	<input type="text"/>
PPPoE Service Name:	<input type="text"/>
Authentication Method:	AUTO <input type="button" value="v"/>
MAC Clone:	<input type="checkbox"/> <input type="text"/> <input type="button" value="Clone MAC"/>
<input type="checkbox"/>	Enable Fullcone NAT
<input type="checkbox"/>	Dial on demand (with idle timeout timer)
<input type="checkbox"/>	PPP IP extension
<input type="checkbox"/>	Use Static IPv4 Address
<input type="checkbox"/>	Use Static IPv6 Address
<input type="checkbox"/>	Enable IPv6 Unnumbered Model
<input type="checkbox"/>	Launch Dhcp6c for Address Assignment (IANA)
<input checked="" type="checkbox"/>	Launch Dhcp6c for Prefix Delegation (IAPD)
<input type="checkbox"/>	Enable PPP Debug Mode
<input type="checkbox"/>	Bridge PPPoE Frames Between WAN and Local Ports
Multicast Proxy	
<input type="checkbox"/>	Enable IGMP Multicast Proxy
<input type="checkbox"/>	No Multicast VLAN Filter
<input type="checkbox"/>	Enable MLD Multicast Proxy

1. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**.
2. If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)**

also. Or configure a static IP address.

3. Click **Next -> Next -> Apply/Save**.

WAN Gateway

Here you can configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.

WAN DNS

Here you can configure the WAN DNS address. After you configure it click **Next**. The default setting is recommended if you cannot locate this information.

Here you can configure the WAN DNS address:

-Click the **Select DNS Server Interface from available WAN interfaces** option

-OR select the **Use the following Static DNS IP address** option and enter static DNS server IP

addresses for the system

And then click **Next**.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Here you can view configurations. Click **Apply/Save** to save your settings if everything is correctly set.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_eth0	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

When the PPPoE connection is successful, you can access the Internet.

IP over Ethernet (IPoE)

If your ISP uses DHCP to assign your IP address or if your ISP assigns you a static (fixed) IP address, IP subnet mask and the gateway IP address, you need to select the IP over Ethernet (IPoE).

Click **Advanced Setup** -> **WAN Service** -> **Add**, select the configured interface and then click **Next** to enter the following screen.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:

IPV4 Only ▼

IPV4 Only

IPv4&IPv6(Dual Stack)

IPV6 Only

1. Select IPoE.
2. Edit the **Enter Service Description**. This field is optional. We recommend that you keep the default.
3. Select a network protocol: IPv4, IPv6 or IPv4 & IPv6 (dual stack).
4. Click **Next**.



Note:

If you select IPv6 or IPv4 & IPv6 (dual stack), skip to [IPv6](#).

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

❖ **Obtain an IP address automatically:** This allows the router to automatically acquire IP information from your ISP or your existing networking equipment.

❖ **Use the following Static IP address:** This allows you to specify the Static IP information provided by your ISP or that corresponds with your existing networking equipment.

❖ **WAN IP Address:** The Internet IP address provided by your ISP for accessing the Internet.

❖ **WAN Subnet Mask:** The subnet mask address provided by your ISP for accessing the Internet.

❖ **WAN gateway IP Address:** The gateway IP address provided by your ISP for accessing the Internet.

Enter the IP address/ subnet mask/gateway IP address provided by your ISP or select **Obtain an IP address automatically** and then click the **Next** button.

IPv6

If you select IPv4 as the network protocol, skip this section.

Option 61 DUID:	<input type="text"/>	(hexadecimal digit)
Option 125:	<input type="radio"/> Disable	<input type="radio"/> Enable
<input checked="" type="radio"/> Use the following Static IP address:		
WAN IP Address:	<input type="text"/>	
WAN Subnet Mask:	<input type="text"/>	
WAN gateway IP Address:	<input type="text"/>	
Enter information provided to you by your ISP to configure the WAN IPv6 settings.		
Notice:		
If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.		
If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.		
<input checked="" type="radio"/> Obtain an IPv6 address automatically		
<input type="checkbox"/> Dhcpv6 Address Assignment (IANA)		
<input checked="" type="checkbox"/> Dhcpv6 Prefix Delegation (IAPD)		
<input type="radio"/> Use the following Static IPv6 address:		
WAN IPv6 Address/Prefix Length:	<input type="text"/>	
Specify the Next-Hop IPv6 address for this WAN interface.		
Notice: This address can be either a link local or a global unicast IPv6 address.		
WAN Next-Hop IPv6 Address:	<input type="text"/>	
		<input type="button" value="Back"/> <input type="button" value="Next"/>

To obtain an IP address automatically:

1. Select **Obtain an IP address automatically**.
2. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**.
3. If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)**.

4. Click **Next** -> **Next** -> **Apply/Save**.

Option 61 DUID:	<input type="text"/>	(hexadecimal digit)
Option 125:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
<input checked="" type="radio"/> Use the following Static IP address:		
WAN IP Address:	<input type="text"/>	
WAN Subnet Mask:	<input type="text"/>	
WAN gateway IP Address:	<input type="text"/>	
Enter information provided to you by your ISP to configure the WAN IPv6 settings.		
Notice:		
If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.		
If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64		
<input checked="" type="radio"/> Obtain an IPv6 address automatically		
<input type="checkbox"/> Dhcpv6 Address Assignment (IANA)		
<input checked="" type="checkbox"/> Dhcpv6 Prefix Delegation (IAPD)		
<input type="radio"/> Use the following Static IPv6 address:		
WAN IPv6 Address/Prefix Length:	<input type="text"/>	
Specify the Next-Hop IPv6 address for this WAN interface.		
Notice: This address can be either a link local or a global unicast IPv6 address.		
WAN Next-Hop IPv6 Address:	<input type="text"/>	
		<input type="button" value="Back"/> <input type="button" value="Next"/>

To configure a static IPv6 address

1. Select **Use the following Static IPv6 address**.
2. Configure **WAN IPv6 Address/Prefix Length** and **WAN Next-Hop IPv6 Address**.

Option 61 DUID:	<input type="text"/>	(hexadecimal digit)
Option 125:	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
<input checked="" type="radio"/> Use the following Static IP address:		
WAN IP Address:	<input type="text"/>	
WAN Subnet Mask:	<input type="text"/>	
WAN gateway IP Address:	<input type="text"/>	
Enter information provided to you by your ISP to configure the WAN IPv6 settings.		
Notice:		
If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.		
If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64		
<input type="radio"/> Obtain an IPv6 address automatically		
<input type="checkbox"/> Dhcpv6 Address Assignment (IANA)		
<input checked="" type="checkbox"/> Dhcpv6 Prefix Delegation (IAPD)		
<input checked="" type="radio"/> Use the following Static IPv6 address:		
WAN IPv6 Address/Prefix Length:	<input type="text" value="2000::1"/>	
Specify the Next-Hop IPv6 address for this WAN interface.		
Notice: This address can be either a link local or a global unicast IPv6 address.		
WAN Next-Hop IPv6 Address:	<input type="text" value="2013::1"/>	
<input type="button" value="Back"/> <input type="button" value="Next"/>		

3. Click **Next** -> **Next** to enter the screen below.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

Interfaces

eth0.2
ppp0.1

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

4. Select **Use the following Static IPv6 DNS address** and manually enter the DNS server address. If you have two DNS server addresses, enter the second also.
5. Click **Next -> Apply/Save**.

NAT

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

No Multicast VLAN Filter

[Back](#) [Next](#)

Here you can configure the NAT. If you are not an advanced user we recommend you to keep the default settings and then click **Next**.

WAN Gateway

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
eth0.1	

[Back](#) [Next](#)

Here you can configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.

WAN DNS

Here you can configure the WAN DNS address. After you configure it click **Next**. The default setting is

recommended if you cannot locate this information.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: Available WAN Interfaces

eth0.2

->

-<

ppp0.1

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Here you can configure the WAN DNS address:

-Click the **Select DNS Server Interface from available WAN interfaces** option

-OR select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system

And then click **Next**.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
eth0.1	ipoe_eth0	IPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

When the IPoE connection is successful, you can access the Internet.

Bridging

If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead of sharing it with others), you can select the Bridging and create a dialup program on your PC.

Click **Advanced Setup** -> **WAN Service** -> **Add**, select the configured interface and then click **Next** to enter the following screen.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Edit the **Service Description**, which is optional. And then click **Next**.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

Wide Area Network (WAN) Service Setup											
Choose Add, Remove or Edit to configure a WAN service over a selected interface.											
Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
eth0.2	br_eth0	Bridge	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

When the connection is successful, you can access the Internet.

4.2.3 USB Application

USB – 3G WAN Service

This device supports 3G Internet access which can be shared by PCs on LAN. Click **Advanced Setup** -> **USB Application** to enter the configuration interface.

Notice: Please enter the correct parameters according to the requirements of your ISP. After finishing and saving the settings, please check the connection status on the running status page. It costs about 1 minute to Dial-up, but the time needed is different according to different model of USB modem card. If you still can't successfully Dial-up, please try to unplug and reboot the Router. If SIM is lock, Please input right pin code within 3 times, or SIM will be invalid.

3G Dial

Enable 3G:

*Country:

*ISP:

Username:

Password:

Dial number:

APN :

Net Select:

PIN Code:

Configuration Procedures:

1. Insert the 3G modem (with an activated SIM card) to the device's USB port.
 2. **Country:** Select your country.
 3. **ISP:** Select your 3G ISP.
 4. Click **Apply/Save**.
- ❖ **APN/Dial number/Username/Password:** This information is provided by your 3G ISP. Normally,

there is no need for manual configuration, as system will automatically match the right settings according to the country and ISP you select.

✧ **Net Select:** Select the right 3G network protocol for your 3G service. If you are not clear, simply select **Auto**.

PIN Code: You need to enter the SIM card's PIN code here if you have enabled it in your 3G modem. Note that your SIM card will be locked after 3 consecutive entries of wrong PIN codes.

Print Server

This page allows you to enable/disable printer support.

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name

Make and model

✧ **Enable on-board print server:** Check/uncheck to enable / disable the printer support.

✧ **Printer name:** Enter a descriptive name of your printer.

✧ **Make and model:** Enter the make and model of your printer.

✧ **Apply/Save:** Click to apply and save your settings.

Storage Service

The storage service allows you to use Storage devices with the modem router to be more easily accessed.

This section explains the following:

- [Storage Device Info](#)
- [User Account](#)

Storage Device Info

This screen displays the information of the storage device as seen on the screenshot below.

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed.Usage of USB Sharing: Open My Computer, input \\X.X.X.X (X.X.X.X=IP Address of the router) and then input username and password,you can access the folder.

Volumename	FileSystem	Total Space	Used Space
<input type="button" value="umount"/>			

User Account

This section allows you to Add, or Remove User Accounts.

Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.Reboot to take effect for removal.

UserName	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>	

To add a user account:

1. Click **Add** to enter the following screen:

Storage User Account Setup

In the boxes below, enter the user name and password on which the home directory is to be created.

Username:

Password:

Confirm Password:

2. Enter the user name, password and volume name on which the home directory is to be created.
3. Click **Apply/Save** to apply and save your settings.

To remove an existing user account:

1. Check **Remove** next to the user account.
2. Click the **Remove** button.

4.2.4 LAN Setup

Here you can configure the LAN IP Address and Subnet Mask. This IP address is to be used to access the device's settings through a web browser. Be sure to make a note of any changes you apply to this page.

IPv4

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface.

GroupName

IP Address:

Subnet Mask:

Enable IGMP Snooping

Standard Mode

Blocking Mode

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

DNS Servers Assigned by DHCP Server:

Primary DNS server:

Secondary DNS server:

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="text"/>	<input type="text"/>	<input type="text"/>

Configure the second IP Address and Subnet Mask for LAN interface

- ✧ **IP Address:** The device's LAN IP address. The default setting is 192.168.1.1.
- ✧ **Subnet Mask:** The LAN subnet mask of the device. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router. You can change the subnet mask to fit your network.

- ✧ **Enable IGMP Snooping:** Check to enable the IGMP Snooping feature and select either of the following two modes:
 - ✧ **Configure the second IP Address and Subnet Mask for LAN interface:** If you want to configure two IP addresses for the LAN interface, you can check this option and enter the second IP Address and Subnet Mask manually.
 - ✧ **Disable DHCP Server:** Click to disable the DHCP Server.
 - ✧ **Enable DHCP Server:** Click to enable the DHCP Server.
 - ✧ **Start IP Address:** Specify the start of the range for the pool of IP addresses in the same subnet as the router.
 - ✧ **End IP Address:** Specify the end of the range for the pool of IP addresses in the same subnet as the router.
 - ✧ **Leased Time:** The lease time is a time length that the IP address is assigned to each device before it is refreshed.
 - ✧ **Static IP Lease List:** Displays a list of devices with reserved static IP addresses.
 - ✧ **Add Entries:** Click to add a static IP lease entry. A maximum 32 entries can be configured.
 - ✧ **Remove Entries:** Click to remove a static IP lease entry.
 - ✧ **Apply/Save:** After you configure all the needed settings, click this button to apply and save them.
-

**Tip:**

DHCP (Dynamic Host Configuration Protocol) assigns an IP address to each device on the LAN/private network. When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool specified in this screen to the requesting device as long as the device is set to "Obtain an IP Address Automatically". By default, the router functions as a DHCP server.

IPv6 Autoconfig

IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION ":::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

Enable DHCPv6 Server

Stateless

Stateful

Start interface ID:

End interface ID:

Leased Time (hour):

Enable RADVD

Enable ULA Prefix Advertisement

Randomly Generate

Statically Configure

Prefix:

Preferred Life Time (hour):

Valid Life Time (hour):

Enable MLD Snooping

Standard Mode

Blocking Mode

Static LAN IPv6 Address Configuration

✧ **Interface Address (prefix length is required):** Enter the interface address.



Note:

- IPv6 address can only be Aggregatable Global Unicast Addresses and Unique Local Address. Link-Local Unicast Addresses and Multicast Addresses are not permitted.
- The IPv6 address must be entered with a prefix length.

IPv6 LAN Applications

- ✧ **Enable DHCPv6 Server:** Check to enable the DHCPv6 Server.
- **Stateless:** If selected, IPv6 clients will generate IPv6 addresses automatically based on the Prefix Delegation's IPv6 prefix and their own MAC addresses.
- **Stateful:** Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Select this option and configure the start/end interface ID and leased time. The router will automatically assign IPv6 addresses to IPv6 clients.
- **Leased Time (hour):** The lease time is a time length that the IP address is assigned to each device before it is refreshed.
- **Start interface ID/End interface ID:** Specify the start/end interface ID Interface ID does NOT

support ZERO COMPRESSION ":::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of ":::2".

✧ **Enable RADVD:** The RADVD (Router Advertisement Daemon) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) and is used by system administrators in stateless autoconfiguration methods of network hosts on Internet Protocol version 6 networks. Check the checkbox to enable the RADVD.

- **Enable ULA Prefix Advertisement:** If enabled, the router will advertise ULA prefix periodically.
- **Randomly Generate:** If selected, address prefix can be automatically generated.
- **Statically Configure:** If you select this option, you need to manually configure the address prefix and life time.
- **Prefix:** Specify the prefix.
- **Preferred Life Time (hour):** Specify the preferred life time in hour.
- **Valid Life Time (hour):** Specify the valid life time in hour.

✧ **Enable MLD Snooping:** MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link. If disabled on layer2 devices, IPv6 multicast data packets will be broadcast on the entire layer2; if enabled, these packets will be multicast to only specified recipient instead of being broadcast on the entire layer2.



Tip:

If you change the LAN IP address of the device, you will lose your connection to the device. You must type the new IP address into your browser address field to log in to the device and set all gateway addresses of the LAN PCs to this new address to access the Internet. Be sure to write the new address on a sticky label and attach it to the bottom of the unit. You will need the new address to log in to the device in the future.

4.2.5 NAT

This section explains the following:

- [Virtual Server](#)
- [Port Triggering](#)
- [DMZ Host](#)

Virtual Server

The Virtual Server is useful for web servers, ftp servers, e-mail servers, gaming and other specialized Internet applications. When you enable the Virtual Server, the communication requests from the Internet to your router's WAN port will be forwarded to the specified LAN IP address.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

To enter the virtual server screen, click NAT -> **Virtual Server** and then click the **Add** button to add rules.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
Remaining number of entries that can be configured: 32

Use Interface Use Interface pppoe_eth0/ppp0.1 ▼

Service Name:

Select a Service: Select One ▼

Custom Service:

Server IP Address:

Apply/Save

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		

- ❖ **Use Interface:** Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection available, the rules will be automatically applied to it.
- ❖ **Service Name:**
 - **Select a Service option:** Allows you to select an existing service from the drop-down list.
 - **Custom Service:** Allows you to customize a service.
- ❖ **Server IP Address:** Enter the IP address of your local computer that will provide this service.
- ❖ **External Starting Port and External Ending Port:** These are the starting number and ending number for the public ports at the Internet interface.
- ❖ **Protocol:** Select the protocol from the Protocol drop-down list. If you are unsure, select TCP/UDP.
- ❖ **Internal Starting Port and Internal Ending Port:** These are the starting number and ending number for the ports of a computer on the router's local area network (LAN).

**Note:**

If you have enabled the UPnP functionality on both the router and your PC that is attached to one of the LAN port on the router, you will be prompted on the Virtual Server page that the UPnP interface is being used.

Application Example:

You have set up two servers on your LAN side:

- An FTP server (using the default port number of 21) at the IP address of 192.168.1.100
- A web server (using the default port number of 80) at the IP address of 192.168.1.110

And want your friends on Internet to access the FTP server and web server on default ports. To access your FTP or web server from the Internet, a remote user has to know the Internet IP address or Internet name of your router, such as www.tendacn.com. In this example, we assume the Internet IP address of your router is 183.37.227.201. Then follow instructions below:

To configure the router to make your local FTP server public:

1. Click **NAT -> Virtual Server** to enter it and then click the **Add** button.
2. - Select FTP that you wish to host on your network from the **Select a Service** drop-down list. The port number (21) used by this service will then be automatically populated.
- Or if you wish to define the service yourself, enter a descriptive name in the **Custom Service**, say My FTP, and then manually enter the port number (21) used by this service in the **Internal Starting Port, Internal Ending Port, External Starting Port and External Ending Port fields**.
3. Select a protocol from the **Protocol** drop-down list. If you are unsure, select **TCP/UDP**.
4. In the **Server IP Address** field, enter the last digit of the IP address of your local computer that offers this service. Here in this example, we enter 192.168.1.100.
5. Click the **Apply/Save** button.
6. Your friends on Internet will then be able to access your FTP server simply by entering "ftp://183.37.227.201" in his browser.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

Remaining number of entries that can be configured:32

Use Interface Use Interface

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
21	21	TCP	21	21
		TCP		
		TCP		



To configure your router to make your local web server public:

1. Click **NAT -> Virtual Server** to enter it and then click the **Add** button.
2. - Select **Web Server (HTTP)** that you wish to host on your network from the **Select a Service** drop-down list. The port number (80) used by this service will then be automatically populated.
 - Or if you wish to define the service yourself, enter a descriptive name in the **Custom Service**, say My Web Server (HTTP), and then manually enter the port number (80) used by this service in the **Internal Starting Port, Internal Ending Port, External Starting Port and External Ending Port** fields.
3. Select a protocol from the **Protocol** drop-down list. If you are unsure, select **TCP/UDP**.
4. In the **Server IP Address** field, enter the last digit of the IP address of your local computer that offers this service. Here in this example, we enter 192.168.1.110.
5. Click the **Apply/Save** button.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

Remaining number of entries that can be configured:32

Use Interface Use Interface

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
80	80	TCP	80	80

6. Now you can view your configurations as seen in the screenshot below. Your friends on Internet

will then be able to access the web server simply by entering "http://183.37.227.201" in his browser.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Web Server (HTTP)	80	80	TCP	80	80	192.168.1.110	ppp0.1	<input type="checkbox"/>
FTP Server	21	21	TCP	21	21	192.168.1.100	ppp0.1	<input type="checkbox"/>

Browser window: https://accounts.google.com x
 http://183.37.227.201



Note:

The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".



Tip:

If the service or game you wish to host on your network is not included in the list, manually add it in the Custom Service field and then add the port number used by it to the **Internal Starting Port, Internal Ending Port, External Starting Port and External Ending Port** fields.

Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the Open Ports.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Add Remove

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range	Port Range	Protocol	Port Range			
		Start	End		Start	End		

To enter the Port Triggering screen, click **NAT -> Port Triggering** and then click the **Add** button to add rules.

You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured: 32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

✧ **Use Interface:** Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection available, the rules will be automatically applied to it.

✧ **Application Name:** Two options are available:

- Select an application

- Custom application

✧ **Trigger Port Start/Trigger Port End:** The port range for an application to initiate connections.

✧ **Trigger Protocol:** Select the protocol from the drop-down list. If you are unsure, select TCP/UDP.

✧ **Open Port Start/ Open Port End:** These are the starting number and ending number for the ports that will be automatically opened by the built-in firewall when connections initiated by an application are established.

DMZ Host

The default DMZ (De-Militarized Zone) host feature is helpful when you are using some online games and videoconferencing applications that are not compatible with NAT (Network Address Translation).

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Save/Apply' to activate the DMZ host.

Clear the IP address field and click 'Save/Apply' to deactivate the DMZ host.

DMZ Host IP Address:

❖ **DMZ Host IP Address:** The IP Address of the device for which the router's firewall will be disabled. Be sure to assign a static IP Address to that device. The DMZ host should be connected to a LAN port of the device. Be sure to assign a static IP address to that DMZ host.

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Save/Apply' to activate the DMZ host.

Clear the IP address field and click 'Save/Apply' to deactivate the DMZ host.

DMZ Host IP Address:



Warning!

DMZ servers pose a security risk. A computer designated as the DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet.

4.2.6 Security

This section explains the following information:

- [IP Filtering](#)
- [MAC Filtering](#)

IP Filtering

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

Choose **Add** to enter the following screen:

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

- ✧ **Filter Name:** Enter a descriptive filtering name.
- ✧ **IP Version:** Select either IPv4 or IPv6.
- ✧ **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.
- ✧ **Source IP address [/prefix length]:** Enter the LAN IP address to be filtered.
- ✧ **Source Port (port or port: port):** Specify a port number or a range of ports used by LAN PCs to access the Internet. If you are unsure, leave it blank.
- ✧ **Destination IP address [/prefix length]:** Specify the external network IP address to be accessed by specified LAN PCs.
- ✧ **Destination Port (port or port:port):** Specify a port number or a range of ports used by LAN PCs to access external network.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is **BLOCKED**. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose **Add** or **Remove** to configure incoming IP filters.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>								

Click **Add** to enter the following screen:

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All pppoe_eth0/ppp0.1 br0/br0

This screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click Apply/Save to save and activate the filter.

- ✧ **IP Version:** Select either IPv4 or IPv6.
- ✧ **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.
- ✧ **Source IP address [/prefix length]:** Enter the Internal IP address [/prefix length] to be filtered.
- ✧ **Source Port (port or port: port):** Specify a port number or a range of ports used by PCs from external network to access your internal network.
- ✧ **Destination IP address [/prefix length]:** Specify the internal network IP address [/prefix length] to be accessed by the specified PCs from external network.
- ✧ **Destination Port (port or port:port):** Specify a port number or a range of ports used by PCs from external network to access your internal network.

MAC Filtering

A bridge WAN service is needed to configure this service.

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

Choose Add or Remove to configure MAC filtering rules.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm0.1	FORWARD	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					



Warning!

Changing from one policy to another of an interface will cause all defined rules for that interface to be **REMOVED AUTOMATICALLY!** You will need to create new rules for the new policy.

Click **Add** to enter the following screen:

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Here you can create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click **Save/Apply** to save and activate the filter.

- ✧ **Protocol Type:** Select a protocol type from the drop-down list.
- ✧ **Destination MAC Address:** Enter the destination MAC address apply the MAC filtering rule to which you wish to apply the MAC filtering rule.

- ✧ **Source MAC Address:** Enter the source MAC address to which you wish to apply the MAC filtering rule.
- ✧ **Frame Direction:** Select a frame direction from the drop-down list.
- ✧ **WAN Interfaces:** Select a WAN interface from the drop-down list.

4.2.7 Parental Control

This section explains the following information:

- [Time Restriction](#)
- [URL Filter](#)

Time Restriction

Click **Parental Control** -> **Time Restriction** -> **Add** to enter the following screen.

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address
 Other MAC Address
(xxxxxxxxxxxx)

Days of the week

Mon	Tue	Wed	Thu	Fri	Sat	Sun
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Click to select

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Here you can add time of day restriction that an attached LAN device can access the Internet.

The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device.

- ✧ **User Name:** Enter a user name.
- ✧ **Browser's MAC Address:** Automatically adds the MAC address of the attached LAN device where the browser is running.
- ✧ **Other MAC Address:** Specify the MAC address of the computer that you want to apply Internet access restriction.
- ✧ **Days of the week:** Click to select the days of the week during which you wish to restrict Internet

access.

- ✧ **Start Blocking Time/ End Blocking Time:** Specify time of day restriction to an attached LAN device. Within this specified time length of the day, this LAN device will be blocked from the Internet.
- ✧ **Apply/Save:** Click to Apply/Save your settings.

URL Filter

Here you can add URL access restriction to specific LAN PCs

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

First select **Exclude** or **Include** and then click **Add** to enter the screen below for configuring the list entries. Maximum 100 entries can be configured.

Parental Control -- URL Filter Add

Enter the URL address then click "Apply/Save" to add the entry to the URL filter.

URL Address:

- ✧ **URL Address:** Enter the URLs that a specific LAN PC cannot access.

Enter the URL address and then click "Apply/Save" to add the entry to the URL filter.



If you have accessed the URL before you include it in a URL filter rule, you must reboot the router and erase it from your PC to activate this URL filter rule. To erase the domain name from your PC, click **Start -> Run**, enter **cmd** and then type **ipconfig /flushdns**.

4.2.8 Quality of Service

This section explains the following:

- [QoS Queue](#)
- [QoS Classification](#)

If **Enable QoS** checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click **Apply/Save** button to save it.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Enable QoS: Check/uncheck to enable/disable the QoS feature.



Note:

- If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.
 - The default DSCP mark is used to mark all egress packets that do not match any classification rules.
-

QoS Queue

In ATM mode, maximum 8 queues can be configured.

In PTM mode, maximum 8 queues can be configured.

For each Ethernet interface, maximum 4 queues can be configured.

For each Ethernet WAN interface, maximum 4 queues can be configured.

To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes and then click the **Remove** button.

The **Enable** button will scan through every queue in the table. Queues with enable-checkbox checked

will be enabled. Queues with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

QoS Queue Setup

In ATM mode, maximum 8 queues can be configured.
 In PTM mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 4 queues can be configured.
 For each Ethernet WAN interface, maximum 4 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.
 Note that WMM function is enabled in Wireless Page.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Min Bit Rate(bps)	Shaping Rate(bps)	Burst Size(bytes)	Enable	Remove
Default Queue	33	atm0	1	8/WRR/1	Path0					<input type="checkbox"/>	

To add a queue, click the **Add** button to enter the following screen.

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable: ▾

Interface: ▾

Here you can configure a QoS queue and add it to a selected layer2 interface.

QoS Classification

To add a rule, click the **Add** button.

To remove rules, check their remove-checkboxes and then click the **Remove** button.

The **Enable** button will scan through every rule in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the rule after page reload.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.
 To remove rules, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 Note that WMM function is enabled in Wireless Page.

The QoS function has been disabled. Classification rules would not take effects.

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS				
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																		

To add a rule, click the **Add** button to enter the following screen.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order: ▼

Rule Status: ▼

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface: ▼

Ether Type: ▼

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required): ▼

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP): ▼

Mark 802.1p priority: ▼

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Here you can create a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.

Click **Apply/Save** to save and activate the rule.

4.2.9 Routing



This section explains the following:

- [Default Gateway](#)

- [Static Route](#)

Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

- ✧ **Selected Default Gateway Interfaces:** Displays the selected default gateway interfaces. Select a WAN interface and click the  button to move it to the **Available Routed WAN Interfaces** box.
- ✧ **Available Routed WAN Interfaces:** Displays the available routed WAN interfaces. Select a WAN interface and click the  button to add it to the **Selected Default Gateway Interfaces** box.
- ✧ **Apply/Save:** Click to save and activate your settings.

Static Route

Static routes provide additional routing information to your router. Typically, you do not need to add static routes. However, when there are several routers in the network, you may want to set up static routing. Static routing determines the path of the data in your network. You can use this feature to allow users on different IP domains to access the Internet via this device. It is not recommended to use this setting unless you are familiar with static routing. In most cases, dynamic routing is recommended, because this feature allows the router to detect the physical changes of the network layout automatically. If you want to use static routing, make sure the router's DHCP function is disabled.

Routing -- Static Route (A maximum 32 entries can be configured)

NOTE: For system created route, the 'Remove' checkbox is disabled.

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

Click **Add** to enter the following screen:

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric: (Range:1-9999)

- ✧ **IP Version:** Select either IPv4 or IPv6.
- ✧ **Destination IP address/prefix length:** Enter the destination IP address and prefix length of the final destination.
- ✧ **Interface:** Select an interface from the drop-down list.
- ✧ **Gateway IP address:** Enter the gateway IP address, which must be a router on the same LAN segment as the router.
- ✧ **Metric:** Enter a number in the Metric field. This stands for the number of routers between your network and the destination.
- ✧ **Apply /Save:** Click to apply and save your settings.

 *Note:*

- Destination IP address cannot be on the same IP segment as WAN or LAN segment as the router.
 - Only configure additional static routes for unusual cases such as multiple routers or multiple IP subnets located on your network. Wrong static routes may lead to network failure.
 - For system created route, the 'Remove' checkbox is disabled.
-

4.2.10 DNS

DNS Server (Static DNS)

The DNS server translates domain names to numeric IP addresses. It is used to look up site addresses based on their names.

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system.

Here you can configure the WAN DNS address:

For IPv4:

-Click the **Select DNS Server Interface from available WAN interfaces** option

-OR select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system

And then click **Apply/Save**.

For IPv6:

-Select **Obtain IPv6 DNS info from a WAN interface** and Select a configured WAN interface for the IPv6 DNS server information.

-Select **Use the following Static IPv6 DNS address** and enter the static IPv6 DNS server Addresses.

And then click **Apply/Save**.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp0.1

>>

<<

Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

TODO: IPv6 ***** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:



Note:

- DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
- In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
- If you cannot locate the static DNS server IP information, ask your ISP to provide it.
- The default settings are recommended if you are unsure about the DNS server addresses. If a wrong DNS server address is configured, webpages may not be open.

Dynamic DNS (DDNS)

If your Internet service provider (ISP) gave you a static (fixed) public IP address, you can register a domain name and have that name associated with your IP address by public Domain Name Servers (DNS). However, if your ISP gave you a dynamic (changing) public IP address, you cannot predict what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. It lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address. If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

Click **Advanced Setup** -> **DNS** -> **Dynamic DNS** to enter the Dynamic DNS screen.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
----------	----------	---------	-----------	--------

Click the **Add** button to configure the DDNS settings.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO, or NO-IP.

DDNS provider: DynDNS.org ▼

Hostname:

Interface: pppoe_eth0/ppp0.1 ▼

DynDNS Settings

Username:

Password:

- ❖ **D-DNS Provider:** Select your DDNS service provider from the drop-down menu.
- ❖ **Hostname:** Enter the DDNS domain name registered with your DDNS service provider.
- ❖ **Interface:** Specify a WAN connection interface.
- ❖ **User Name:** Enter the DDNS user name registered with your DDNS service provider.
- ❖ **Password:** Enter the DDNS Password registered with your DDNS service provider.

Click **Apply/Save** to save your settings.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
DDNS	123	dyndns	ppp0.1	<input type="checkbox"/>

4.2.11 DSL

This screen provides multiple ADSL modulation modes to meet diversified environments. You can also select phone line pair and Capability.

DSL parameter configurations must be supported by ISP to take effect. Actual parameters (see Statistics-xDSL) resulted from the negotiation between your router and ISP. Wrong configurations may fail your Internet access.

The best DSL configurations are the factory defaults. Only change them if you are instructed by your ISP or our technical staff when your router fails to negotiate with ISP in DSL (ATM) mode. Usually,

this failure can be identified and confirmed if the ADSL LED on the device keeps displaying a slow or quick blinking light.

DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Check the checkbox next to a modulation to enable it and then click **Apply/Save**.

✧ **Advanced Settings:** Click to enter the screen below.

DSL Advanced Settings

Select the test mode below.

- Normal
- Reverb
- Medley
- No retrain
- L3

Here you can select the test mode and tone.

**Tip:**

If you are unsure about the ADSL parameters, please apply the factory default settings. Wrong configurations may fail your Internet access.

4.2.12 UPnP

UPnP (Universal Plug and Play) allows Windows based systems to configure the device for various Internet applications automatically. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications, such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

Enable UPnP

✧ **Enable UPnP:** Check/uncheck to enable/disable the UPnP feature.

**Note:**

UPnP is activated only when there is a live WAN service with NAT enabled.

4.2.13 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	eth1	
			eth2	
			eth3	

Click **Add** to enter the screen below:

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping

Grouped LAN Interfaces:

Available LAN Interfaces:

- ✧ **Group Name:** The name of a configured rule.
- ✧ **WAN Interface used in the grouping:** WAN connection to which the interface grouping rules apply.
- ✧ **Available LAN Interfaces:** LAN interfaces that can be used for interface grouping.
- ✧ **Grouped LAN Interfaces:** LAN interfaces that use specified WAN interface.

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the

arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses.

4. Click **Apply/Save** button to make the changes effective immediately.



Note:

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

4.2.14 IP Tunnel

This section explains the following information:

- [IPv6inIPv4](#)
- [IPv4inIPv6](#)

IPv6inIPv4

Click **IPv6inIPv4** and **Add** to enter the following screen:

The screenshot shows a web configuration page titled "IP Tunneling -- 6in4 Tunnel Configuration". It contains the following fields and controls:

- A text box for "Tunnel Name".
- A dropdown menu for "Mechanism:" with "6RD" selected.
- A dropdown menu for "Associated WAN Interface:".
- A dropdown menu for "Associated LAN Interface:" with "LAN/br0" selected.
- Two radio buttons for "Manual" (selected) and "Automatic".
- Text boxes for "IPv4 Mask Length:", "6rd Prefix with Prefix Length:", and "Border Relay IPv4 Address:".
- An "Apply/Save" button in the bottom right corner.

- ❖ **Tunnel Name:** Specify the name of the tunnel.
- ❖ **Mechanism:** Currently, only DS-Lite configuration is supported.
- ❖ **Associated WAN Interface:** Specify the WAN interface of the tunnel.
- ❖ **Associated LAN Interface:** Specify the LAN interface of the tunnel.

- ✧ **Manual:** If you select Manual, configure the following settings also:
 - **IPv4 Mask Length:** Specify the IPv4 Mask Length.
 - **6rd Prefix with Prefix Length:** Specify the 6rd Prefix with Prefix Length.
 - **Border Relay IPv4 Address:** Specify the Border Relay IPv4 Address.
- ✧ **Automatic:** If Automatic is selected, no configurations are required.
- ✧ **Apply/Save:** Click to apply and save your settings.

IPv4inIPv6

Click **IPv4inIPv6** and **Add** to enter the following screen:

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

Manual Automatic

AFTR:

- ✧ **Tunnel Name:** Specify the name of the tunnel.
- ✧ **Mechanism:** Currently, only 6rd configuration is supported.
- ✧ **Associated WAN Interface:** Specify the WAN interface of the tunnel.
- ✧ **Associated LAN Interface:** Specify the LAN interface of the tunnel.
- ✧ **Manual:** If you select Manual, enter the AFTR information also:
- ✧ **Automatic:** If Automatic is selected, no configurations are required.
- ✧ **Apply/Save:** Click to apply and save your settings.

4.2.15 Certificate

This section explains the following information:

- [Local Certificates](#)

- [Trusted CA \(Certificate Authority\) Certificates](#)

Local Certificates

Here you can Add, View or Remove certificates. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
------	--------	---------	------	--------

To generate generate a certificate signing request:

1. Click the **Create Certificate Request** button to enter the page below.

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

2. Specify the Common Name, Organization Name and State/Province Name
3. Enter the 2-letter Country Code for the certificate.
4. Click **Apply** to apply your settings.

To Import certificate:

1. Click the **Import Certificate** button on the local certificates page to enter the page below.

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

2. Enter the certificate name.
3. Paste the certificate content and private key.
4. Click **Apply** to apply your settings.

Trusted CA (Certificate Authority) Certificates

Here you can Add, View or Remove CA certificates. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

Name	Subject	Type	Action
<input type="button" value="Import Certificate"/>			

To Import certificate:

1. Click the **Import Certificate** button to enter the page below.

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Apply

2. Enter the certificate name.
3. Paste the certificate content.
4. Click **Apply** to apply your settings.

4.2.16 Multicast

Here you can configure the multicast feature.

To configure IGMP for IPv4

1. Check the **LAN to LAN (Intra LAN) Multicast Enable** box.
2. Check the **Membership Join Immediate (IPTV)** box. This is only required for IPTV.
3. Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly recommended.

Multicast Precedence:		Disable ▾ lower value, higher priority
IGMP Configuration		
Enter IGMP protocol configuration fields if you want modify default values shown below.		
Default Version:		3
Query Interval:		125
Query Response Interval:		10
Last Member Query Interval:		10
Robustness Value:		2
Maximum Multicast Groups:		25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):		10
Maximum Multicast Group Members:		25
Fast Leave Enable:		<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:		<input checked="" type="checkbox"/>
Mebership Join Immediate (IPTV):		<input type="checkbox"/>
MLD Configuration		
Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.		
Default Version:		2
Query Interval:		125
Query Response Interval:		10

To configure IGMP for IPv6

1. Check the **LAN to LAN (Intra LAN) Multicast Enable** box.
2. Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly recommended.

Robustness Value:		2
Maximum Multicast Groups:		25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):		10
Maximum Multicast Group Members:		25
Fast Leave Enable:		<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:		<input checked="" type="checkbox"/>
Mebership Join Immediate (IPTV):		<input type="checkbox"/>
MLD Configuration		
Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.		
Default Version:		2
Query Interval:		125
Query Response Interval:		10
Last Member Query Interval:		10
Robustness Value:		2
Maximum Multicast Groups:		10
Maximum Multicast Data Sources (for mldv3):		10
Maximum Multicast Group Members:		10
Fast Leave Enable:		<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:		<input checked="" type="checkbox"/>
<input type="button" value="Apply/Save"/>		

4.2.17 IPTV

If you check the **Enable IPTV** checkbox, you must choose a layer2 interface, and then configure the PVC/VLAN info (ATM), or ETH port/VLAN info (ETH). Click **Apply/Save** button to save it.

Enable IPTV: Check/uncheck to enable/disable the IPTV service.

IPTV --- IPTV Management Configuration

If IPTV checkbox is selected, choose layer2 interface, then configure the PVC/VLAN info(ATM), or ETH port/VLAN info(ETH). Click 'Apply/Save' button to save it.

Enable IPTV

Select Layer2 Interface

ATM Interface

ETH Interface

This screen allows you to configure a ATM PVC.

VPI: [0-255]

VCI: [32-65535]

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [1-4094]:



Tip:

- For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
- For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

4.3 Wireless

This section explains the following information:

- [Basic](#)
- [Security](#)
- [MAC Filter](#)
- [Wireless Bridge](#)
- [Station Info](#)

4.3.1 Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

Click **Apply/Save** to configure the basic wireless options.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless

Hide Access Point

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 76:54:32:21:10:12

Channel:

- ✧ **Enable Wireless:** check/uncheck to enable/disable the wireless feature.
- ✧ **SSID:** This is the public name of your wireless network.
- ✧ **Hide SSID (Hide Access Point):** This option allows you to have your network names (SSID) publicly broadcast or if you choose to enable it, the SSID will be hidden.
- ✧ **BSSID:** Display the BSSID.
- ✧ **Channel:** Select a channel or select **Auto** to let system automatically select one for your wireless network to operate on if you are unsure. The best selection is a channel that is the least used by neighboring networks.

4.3.2 Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually or through WiFi Protected Setup (WPS).

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When the STA PIN is empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS:

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WEP Encryption:

WPS Setup

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. Simply enter a PIN code on the device web interface or press hardware WPS button (on the back panel of the device) and a secure wireless connection is established.

✧ **WPS Button:** Press the hardware WPS button on the device for 1 second and the WPS LED will keep blinking for about 2 minutes. Within the 2 minutes, press the WPS button on your wireless computer or other device. When the WPS displays a solid light, the device has joined your wireless network.

✧ **PIN:** To use this option, you must know the PIN code from the wireless client and enter it in the corresponding field on your device while using the same PIN code on client side for such connection.

✧ **Enable WPS:** Check/uncheck to enable/disable the WPS function. It is enabled by default.



Note:

- To use the WPS security, the wireless client must be also WPS-capable.
 - When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled.
-

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click "Apply/Save" when done.

- ✧ **Network Authentication:** Select Open, Shared, WPA-PSK, WPA2-PSK or Mixed WPA/WPA2-PSK from the drop-down list to encrypt your wireless network.
- ✧ Depending on the type of network authentication you select, you will be prompted to enter corresponding settings.
- ✧ **WEP Encryption:** Select Enabled or Disabled.
- ✧ **Encryption Strength:** Select 128-bit or 64-bit.
- ✧ **Current Network Key:** Select a network key to be active.
- ✧ **Network Key 1/2/3/4:** Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys; enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.
- ✧ **WPA/WAPI passphrase:** Enter a WPA/WAPI network key.
- ✧ **WPA Group Rekey Interval:** Specify a key update interval.
- ✧ **WPA/WAPI Encryption:** Select AES or TKIP+AES.

4.3.3 MAC Filter

The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your wireless network.

Wireless -- MAC Filter

Note: If 'Allow' is choosed and mac filter is empty, WPS will be disabled, and you will not be able to access the router wirelessly.

Select SSID:

MAC Restrict Mode: Disabled Allow Deny

MAC Address	Remove
-------------	--------

- ✧ **Allow:** Only allow PCs at specified MAC addresses (in the list) to connect to your wireless network.
- ✧ **Deny:** Block only PCs at specified MAC addresses from connecting to your wireless network.
- ✧ **Disable:** Disable this feature.
- ✧ **Add:** Click to add a MAC address.
- ✧ To delete an existing MAC address, first check the **Remove** box next to the MAC address in list and then click the **Remove** button.

Example 1: To allow only the PC at the MAC address of 00:1A:3D:9C:BB:23 to connect to your wireless network, do as follows:

1. Select **Allow**.
2. Click the **Add** button.
3. Enter **00:1A:3D:9C:BB:23** in the MAC address box as shown in the figure below:

Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

4. Click **Apply/Save**.

Wireless -- MAC Filter

Select SSID: Tenda_010001

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address	Remove
00:1A:3D:9C:BB:23	<input type="checkbox"/>



Note:

If **allow** is chose and mac filter is empty, WPS will be disabled.

4.3.4 Wireless Bridge

This page allows you to configure wireless bridge (also known as Wireless Distribution System) features of the wireless LAN interface.

Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Action which disables wireless bridge. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode: Access Point

Bridge Action: Enabled

Remote Bridges MAC Address:

✧ **AP Mode:** You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.

✧ **Bridge Restrict:** There are three options available: Enabled, Enabled (Scan) and Disabled. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be

granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. The Enabled (Scan) enables wireless bridge restriction and automatically scans the remote bridges.

- ✧ **Remote Bridges MAC Address:** Specify the MAC address of the remote bridge. If you select the Enabled (Scan) option in Bridge Restrict, system automatically scans the remote bridges and you only need to select those bridges and their MAC addresses will be added to automatically.
- ✧ **Refresh:** Click to update the remote bridges. Wait for few seconds to update.
- ✧ **Apply/Save:** Click to apply and save the settings.



Note:

The WDS feature (also known as Wireless Bridge) can only be implemented between 2 WDS-capable wireless devices. Plus, SSID, channel, security settings and security key must be exactly the same on both such devices.

4.3.5 Station Info

This page shows authenticated wireless stations and their status.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

4.4 Diagnostics

The modem router is capable of testing the connection to your DSL service provider, the connection to your Internet service provider and the connection to your local network. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

pppoe_eth0 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your eth1 Connection:	FAIL	Help
Test your eth2 Connection:	PASS	Help
Test your eth3 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	Help
Test authentication with ISP:	DISABLED	Help
Test the assigned IP address:	DISABLED	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

System Tools -- Ping tool

Ping IP Address:

4.5 Management

This section explains the following information:

- [Settings](#)
- [System Logs](#)
- [TR-069 Client](#)
- [Internet Time](#)
- [Access Control](#)
- [Update Firmware](#)
- [Reboot](#)

4.5.1 Settings

This section explains the following information:

- [Backup](#)
- [Restore Backup](#)
- [Restore Default](#)

Backup

Here you can save a copy of your device's configurations to your computer. Once you have configured the device, you can save these settings to a configuration file on your local hard drive. The configuration file can later be imported to your device in case the device is reset to factory default settings.

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Restore Backup

Here you can restore the configuration from a file saved on your PC.

Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name: No file chosen

Restore Default

Under some circumstances (for example, join a different network or unfortunately forgetting the login password), you may need to remove the existing configuration and restore the factory default settings.

Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

4.5.2 System Logs

The System Log dialog allows you to view the System Log and configure the System Log options.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

To view the System Log, simply click **View System Log**.

System Log

Date/Time	Facility	Severity	Message
<input type="button" value="Refresh"/> <input type="button" value="Close"/>			

To configure the System Log options, click **Configure System Log**.

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

- ✧ **Log:** If Enable is selected, the system will begin to log all the selected events.
- ✧ **Log Level:** All events above or equal to the selected level will be logged.
- ✧ **Display Level:** All logged events above or equal to the selected level will be displayed.
- ✧ **Apply/Save:** click to apply and save the system log settings.

4.5.3 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Click the **TR-069 Client** tab to enter the TR-069 Client configuration screen as seen below:

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

- ✧ **Inform:** Select **Enable/Disable** to enable/disable the **TR-069 Client** function. By default, it is disabled.
- ✧ **Inform Interval:** Specify the inform interval.
- ✧ **ACS URL:** Enter the ACS (Auto-Configuration Server) URL address.
- ✧ **ACS User Name:** Enter the ACS (Auto-Configuration Server) user name.
- ✧ **ACS Password:** Enter the ACS (Auto-Configuration Server) password.
- ✧ **WAN Interface used by TR-069 client:** Select the WAN interface used by the TR-069 client from the drop-down list.
- ✧ **Display SOAP messages on serial console:** If **Enable** is selected, SOAP messages will be displayed on serial console; if **Disable** is selected, SOAP messages will not be displayed on serial console.
- ✧ **Connection Request Authentication:** Check/uncheck to enable/disable the connection request authentication.

- ✧ **Connection Request User Name:** Enter the connection request user name.
- ✧ **Connection Request Password:** Enter the connection request password.
- ✧ **Connection Request URL:** Specify the connection request URL.

4.5.4 Internet Time

This page is used to set the router's system time. If **Automatically synchronize with Internet time servers** is checked, the system will automatically connect to NTP server to synchronize the time.

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:	<input type="text" value="time.nist.gov"/>	<input type="text"/>
Second NTP time server:	<input type="text" value="ntp1.tummy.com"/>	<input type="text"/>
Third NTP time server:	<input type="text" value="None"/>	<input type="text"/>
Fourth NTP time server:	<input type="text" value="None"/>	<input type="text"/>
Fifth NTP time server:	<input type="text" value="None"/>	<input type="text"/>
Time zone offset:	<input type="text" value="(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi"/>	

- ✧ **First/Second/Third/Fourth/Fifth NTP time server:** Select a NTP time server from the drop-down list. If the NTP time server you are looking for is not included in the list, select **Other** and then enter it manually in the box.
- ✧ **Time zone offset:** Select your time zone from the drop-down list.

4.5.5 Access Control

This section explains the following information:

- [Password](#)
- [AccessControl - Service](#)

Password

Access to your broadband router is controlled through the user account: admin.

The user name "admin" has unrestricted access to change and view configuration of your Router.

Access Control -- Passwords

Access to your broadband router is controlled through user account: admin.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords.

Note: User Name and Password can only include letters, numbers or underscore.

User Name:

Old Password:

New Password:

Confirm Password:

- ✧ **User Name:** Enter the user name of up to 16 characters.
- ✧ **Old Password:** Enter the old password of up to 16 characters.
- ✧ **New Password:** Enter a new password of up to 16 characters.
- ✧ **Confirm Password:** Re-enter to confirm the new password.
- ✧ **Apply/Save:** Click to change or create passwords.



Note:

The device's user name and password are respectively preset to admin. Please change the password for better security. The password can be up to 16 characters without any space.

AccessControl - Service

Here you can manage the device either from LAN or WAN side using HTTP, ICMP and TELNET. Click **Management -> Access Control -> AccessCtr** to enter the configuration interface.

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
ICMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable

- ✧ **HTTP:** If enabled, the device can be configured via a Web browser from the specified side (LAN or WAN). This configuration method is simple and thus suitable for most users.
- ✧ **ICMP:** If enabled, you can run a ping command from the specified side (LAN or WAN) to test the reachability of a host on an Internet Protocol (IP) network.
- ✧ **TELNET:** If enabled, you can access the device using Telnet from the specified side (LAN or WAN) to view detailed settings. This can be used by network administrators, technicians or people with solid understanding of network concepts for troubleshooting network problems.



Tip:

- If you are not an advanced user, we suggest you keep the default settings.
- To manage the device from LAN side, use the device's current LAN IP address and log in as "admin"; to manage the device from WAN side, use the device's current WAN IP address and log in as "admin".

4.5.6 Update Firmware

Firmware upgrade is released periodically to improve the functionality of your device and add any new features. If you run into a problem with a specific feature of the device you could log in to our website (www.tendacn.com) to download the latest firmware to update your device.

Tools -- Update Firmware

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: No file chosen Software Version: **V5.2.1.3**

To update software, do as follows:

1. Obtain an updated software image file from our website: www.tendacn.com.
2. Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
3. Click the "Update Software" button once to upload the new image file.



Note:

The update process takes about 2 minutes to complete, and your Broadband Router will reboot.


4.5.7 Reboot

Click the Reboot button to reboot the router.

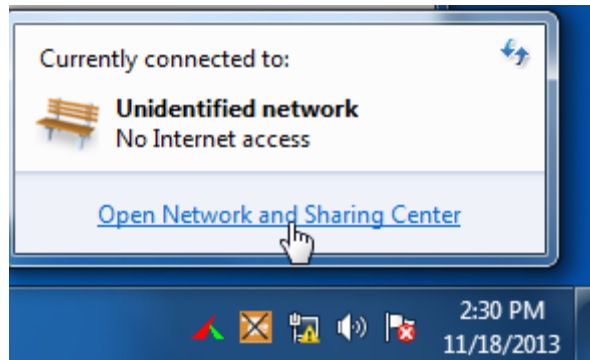
Click the button below to reboot the router.


Appendix 1 Configure Your PC

Windows 7

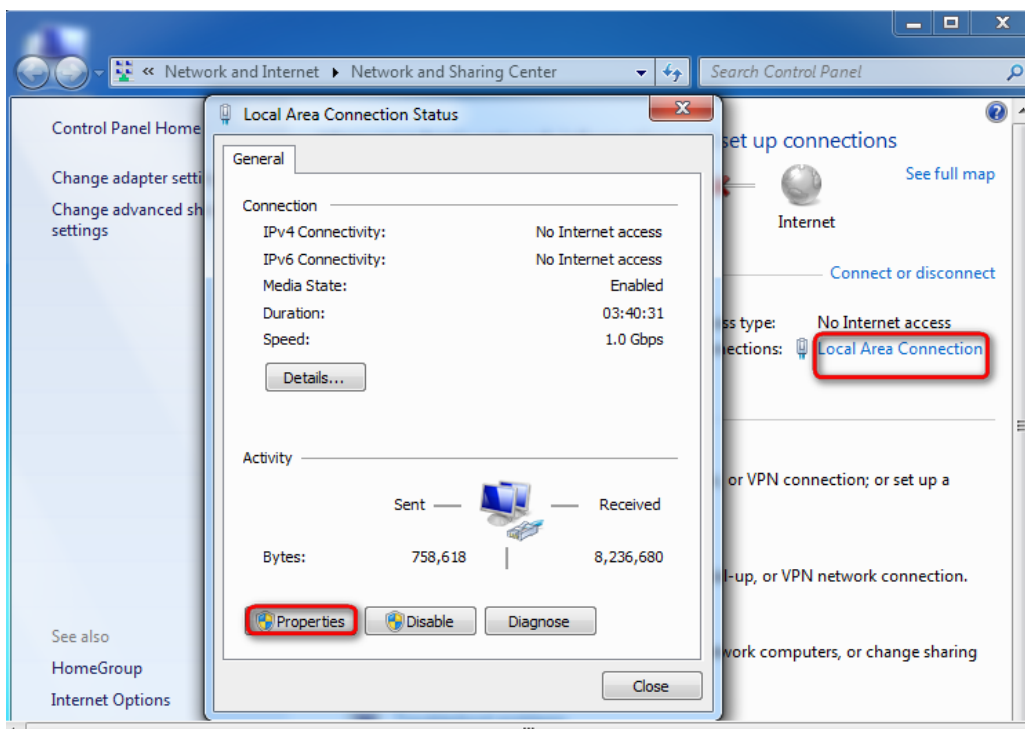
Step 1: Click the icon  on the bottom right corner of your desktop.

Step 2: Click **Open Network and Sharing Center**.

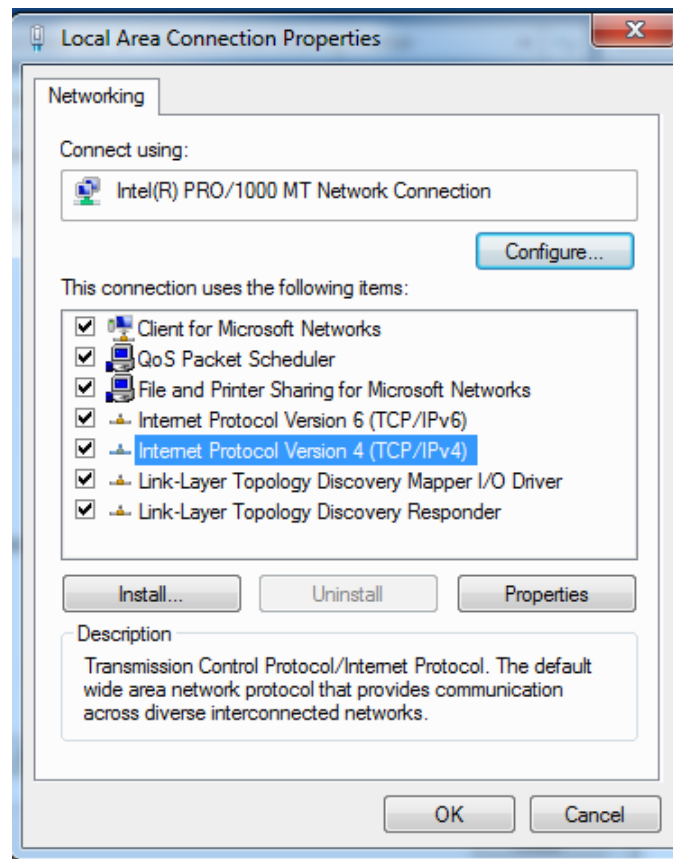


If you cannot find the icon  on the right bottom corner of your desktop, follow steps below: Click **Start -> Control Panel -> Network and Internet -> Network and Sharing Center**.

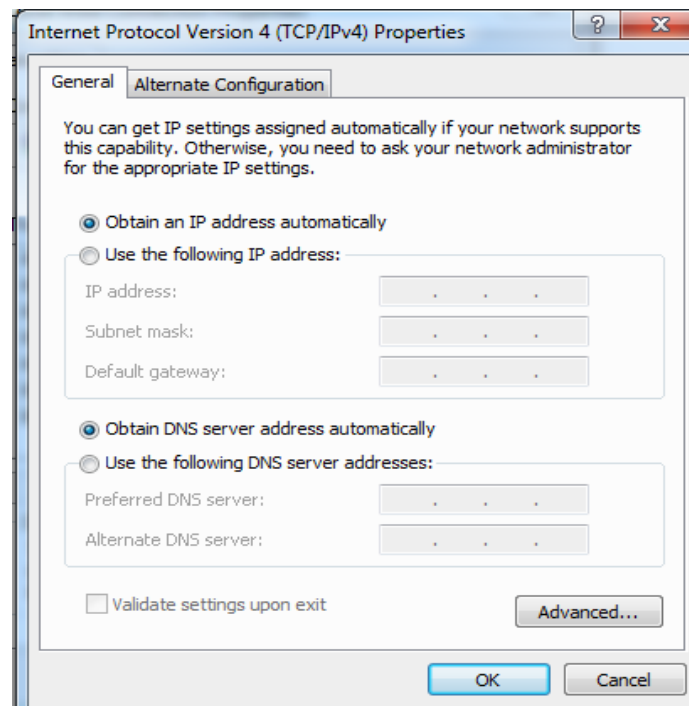
Step 3: Click **Local Area Connection -> Properties**.



Step 4: Find and double click **Internet Protocol Version 4(TCP/IPv4)**.



Step 5: Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



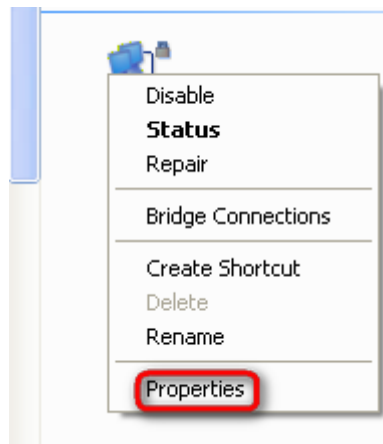
Step 6: Click **OK** on the **Local Area Connection Properties** window (see **Step 4** for the screenshot).

Windows XP

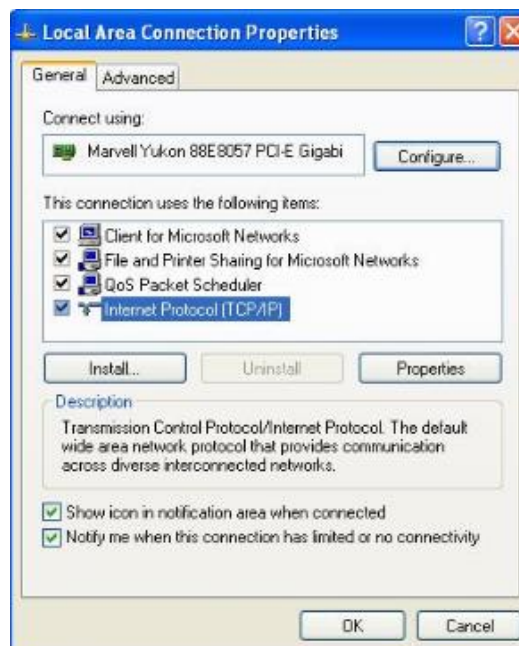
Step 1: Right click **My Network Places** on your desktop and select **Properties**.



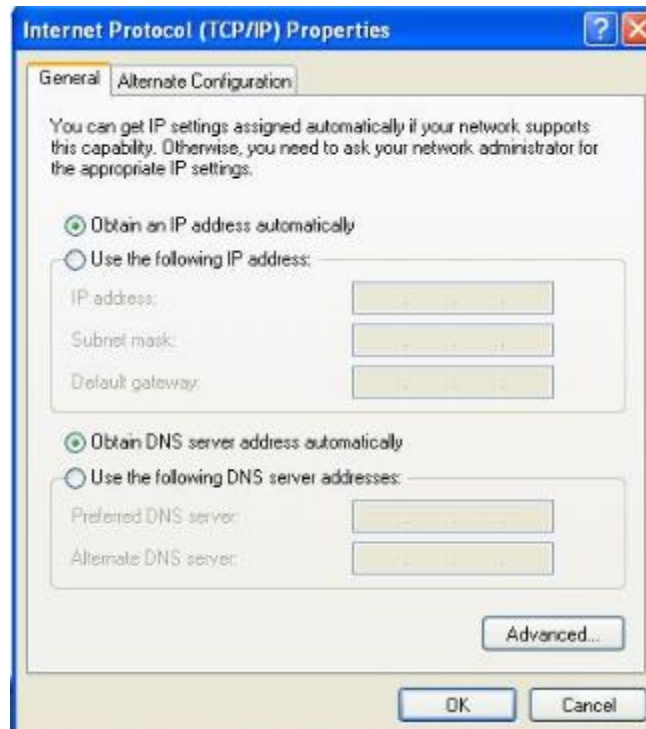
Step 2: Right click **Local Area Connection** and select **Properties**.



Step 3: Scroll down to find and double click **Internet Protocol (TCP/IP)**.



Step 4: Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



Step 5: Click **OK** on the **Local Area Connection Properties** window (see **Step 3** for the screenshot).

Appendix 2 FAQs

1. What information should I have to access Internet via the ADSL uplink?

If you have DSL broadband service, you might need the following information to set up your modem router.



- Active Internet service provided by an ADSL account
- The ISP configuration information for your ADSL account
 - ISP login name and password
 - Fixed or static IP address

Depending on how your ISP set up your Internet account, you could need to know the Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters for a manual setup.

2. I cannot access the device's management interface. What should I do?

1. Verify the physical connection (namely, the Ethernet cable) between your PC and the device. For details, see **3.1 Hardware Install** hereof.
2. Double check the TCP/IP settings on your PC. For details, see [Appendix 1 Configure Your PC](#) hereof.
3. Press the **WPS/RST** button on the device and then re-access the management interface.
4. Change the Ethernet cable that connects your PC and the device.
5. Try accessing device management interface from other PCs, smart phones or iPads.
6. Connect your PC alone to one of the LAN ports on the device.

3. My notebook is unable to search wireless networks, what should I do?

1. Verify that wireless service is enabled on your notebook by checking the wireless hardware or software button on your notebook. The hardware button is usually located on the side of your notebook. Note that some notebooks may not have such hardware button. Software button can be implemented by pressing Fn+. **Fn** is situated on the bottom left corner of your keyboard,  may be any key between **F1-F12** depending on what type of keyboard you are using.
2. Log in to the device, select **Advanced-> Wireless-> Basic** and change the wireless network name

(SSID). Then search again.

3. Follow below steps to verify that wireless service is enabled on your notebook (for Windows XP OS only).

- a) Right click on the **My Computer** icon and select **Manage**.
- b) Select **Services and Applications**, double click **Services** and view the status of **Wireless Zero Configuration**.
- c) If **Status** does not display **Started**, right click the **Wireless Zero Configuration** and select **Start**.
- d) If **Startup Type** displays **Disabled**, right click the **Wireless Zero Configuration** and select **Properties**.
- e) Select **Automatic** from the **Startup Type** drop-down list box and then click **Start** in **Service Status**.

4. Why cannot I connect to the searched wireless network?

1. Verify that you enter a correct security key.
2. Log in to the device, select **Advanced-> Wireless** and change the wireless network name (SSID). Then connect again.
3. Log in to the device, select **Advanced-> Wireless-> Security** and change the security settings. Then connect again.

5. Where should I place the wireless device for optimum performance?

1. Place it in the center to extend wireless coverage as far as possible.
2. Never place the device near to metal objects or in direct sunshine.
3. Keep it far away from devices that use the 2.4 GHz radio wave frequency to transmit and receive data, such as 802.11g/n wireless network devices, electronic devices such as cell phones, radio transmitters, blue tooth, cordless phones, fax machines, refrigerators and microwaves to avoid electronic interference.

6. I cannot find my wireless network in the scan list. What should I do?

1. Verify that you have switched on wireless on your notebook.
2. Verify that your wireless adapter's driver is successfully installed and the adapter is enabled.
3. Make sure that wireless service is enabled on your notebook.

4. Verify that you have enabled the wireless feature and SSID broadcast on your device.
5. Move closer to your wireless device to avoid potential signal attenuation caused by multiple obstacles and then search again.
6. Try searching for your wireless network from other wireless network adapters. If this fails too, reset your device to factory default settings.

7. I connect to the Internet via an Ethernet cable and my PC fails to obtain an IP address of 192.168.1.X (X represents any integer between 2 and 254). What should I do?

Step 1: Set your PC to Use the following IP address and manually configure below settings (Refer to [Appendix 1 Configure Your PC](#)):

IP address: 192.168.1.x (where x can be any number between 2~254)

Subnet Mask: 255.255.255.0

Default gateway and Preferred DNS server: 192.168.1.1

And then click **OK** twice to save your settings and to exit

Step 2: Enter your device's Web interface to configure Internet and wireless security settings.

Appendix 3 VPI/VCI List

The following table lists common ISPs and their VPI and VCI numbers. If you cannot locate your ISP and their VPI and VCI information here, ask your ISP to provide it.

Country	ISP	VPI	VCI	Encapsulation
Australia	Telstra	8	35	PPPoA LLC
Australia	GoldenIT	8	35	_PPPOA_VCMUX
Australia	Telstra Bigpond	8	35	PPPOE_LL
Australia	OptusNET	8	35	PPPOE_VCMUX
Australia	AAPT	8	35	PPPOE_VCMUX
Australia	ADSL Direct	8	35	PPPOE_LL
Australia	Ausie Broadband	8	35	PPPOE_LL
Australia	Australia On Line	8	35	PPPOA_VCMUX
Australia	Connexus	8	35	PPPOE_LL
Australia	Dodo	8	35	PPPOE_LL
Australia	Gotalk	8	35	PPPOE_VCMUX
Australia	Internode	8	35	PPPOE_VCMUX
Australia	iPrimus	8	35	PPPOA_VCMUX
Australia	Netspace	8	35	PPPOE_VCMUX
Australia	Southern Cross Telco	8	35	PPPOE_LL
Australia	TPG Internet	8	35	PPPOE_LL
Argentina	Telecom	0	33	PPPoE LLC
Argentina	Telefonica	8	35	PPPoE LLC
Argentina		1	33	PPPoA VC-MUX
Belgium	ADSL Office	8	35	1483 Routed IP LLC
Belgium	Turboline	8	35	PPPoA LLC
Bolivia		0	34	1483 Routed IP LLC
Brazil	Brasil Telcom	0	35	PPPoE LLC

Brazil	Telefonica	8	35	PPPoE LLC
Brazil	Telmar	0	33	PPPoE LLC
Brazil	South Region	1	32	PPPoE LLC
Colombia	EMCALI	0	33	PPPoA VC-MUX
Columbia	ETB	0	33	PPPoE LLC
Costa Rica	ICE	1	50	1483 Routed IP LLC
Denmark	Cybercity, Tiscali	0	35	PPPoA VC-MUX
France (1)	Orange	8	35	PPPoE LLC
France (2)		8	67	PPPoE LLC
France (3)	SFR	8	35	PPPoA VC-MUX
Germany		1	32	PPPoE LLC
Hungary	Sci-Network	0	35	PPPoE LLC
Iceland	Islandssimi	0	35	PPPoA VC-MUX
Iceland	Siminn	8	48	PPPoA VC-MUX
Israel		8	35	PPPoA VC-MUX
Italy		8	35	PPPoA VC-MUX
Iran (1)		0	35	PPPoE LLC
Iran (2)		8	81	PPPoE LLC
Israel(1)		8	48	PPPoA VC-MUX
Jamaica (1)		8	35	PPPoA VC-MUX
Jamaica (2)		0	35	PPPoA VC-MUX
Jamaica (3)		8	35	1483 Bridged IP LLC SNAP
Jamaica (4)		0	35	1483 Bridged IP LLC SNAP
Kazakhstan		0	33	PPPoA VC-MUX
Malaysia		0	35	PPPoE LLC
Mexico	Telmex (1)	8	81	PPPoE LLC
Mexico	Telmex (2)	8	35	PPPoE LLC
Mexico	Telmex (3)	0	81	PPPoE LLC
Mexico	Telmex (4)	0	35	PPPoE LLC

Netherlands	BBNED	0	35	PPPoA VC-MUX
Netherlands	MX Stream	8	48	PPPoA VC-MUX
New Zealand	Xtra	0	35	PPPoA VC-MUX
New Zealand	Slingshot	0	100	PPPoA VC-MUX
Pakistan (cyber net)		8	35	PPPoE LLC
Pakistan (linkDotnet)		0	35	PPPoA LLC
Pakistan(PTCL)		8	81	PPPoE LLc
Portugal		0	35	PPPoE LLC
Puerto Rico	Coqui.net	0	35	PPPoA LLC
Saudi Arabia (1)		0	33	PPPoE LLC
Saudi Arabia (2)		0	35	PPPoE LLC
Saudi Arabia (3)		0	33	1483 Bridged IP LLC
Saudi Arabia (4)		0	33	1483 Routed IP LLC
Saudi Arabia (5)		0	35	1483 Bridged IP LLC
Saudi Arabia (6)		0	35	1483 Routed IP LLC
Spain	Albura, Tiscali	1	32	PPPoA VC-MUX
Spain	Colt Telecom, Ola Internet	0	35	PPPoA VC-MUX
Spain	EresMas, Retevision	8	35	PPPoA VC-MUX
Spain	Telefonica (1)	8	32	PPPoE LLC
Spain	Telefonica (2), Terra	8	32	1483 Routed IP LLC
Spain	Wanadoo (1)	8	35	PPPoA VC-MUX
Spain	Wanadoo (2)	8	32	PPPoE LLC
Spain	Wanadoo (3)	8	32	1483 Routed IP LLC
Sweden	Telenordia	8	35	PPPoE
Sweden	Telia	8	35	1483 Routed IP LLC
Switzerland		8	35	PPPoE LLC
Trinidad & Tobago	TSTT	0	35	PPPoA VC-MUX

Turkey (1)		8	35	PPPoE LLC
Turkey (2)		8	35	PPPoA VC-MUX
Thailand	TRUE	0	100	PPPoE LLC
Thailand	TOT	1	32	PPPoE LLC
Thailand	3BB	0	33	PPPoE LLC
Thailand	Cat Telecom	0	35	PPPoE LLC
Thailand	BuddyBB	0	35	PPPoE LLC
United States	4DV.Net	0	32	PPPoA VC-MUX
United States	All Tel (1)	0	35	PPPoE LLC
United States	All Tel (2)	0	35	1483 Bridged IP LLC
United States	Ameritech	8	35	PPPoA LLC
United States	AT&T (1)	0	35	PPPoE LLC
United States	AT&T (2)	8	35	1483 Bridged IP LLC
United States	AT&T (3)	0	35	1483 Bridged IP LLC
United States	August.net (1)	0	35	1483 Bridged IP LLC
United States	August.net (2)	8	35	1483 Bridged IP LLC
United States	BellSouth	8	35	PPPoE LLC
United States	Casstle.Net	0	96	1483 Bridged IP LLC
United States	CenturyTel (1)	8	35	PPPoE LLC
United States	CenturyTel (2)	8	35	1483 Bridged IP LLC
United States	Coqui.net	0	35	PPPoA LLC
United States	Covad	0	35	PPPoE LLC
United States	Earthlink (1)	0	35	PPPoE LLC
United States	Earthlink (2)	8	35	PPPoE LLC
United States	Earthlink (3)	8	35	PPPoE VC-MUX
United States	Earthlink (4)	0	32	PPPoA LLC
United States	Eastex	0	100	PPPoA LLC
United States	Embarq	8	35	1483 Bridged IP LLC
United States	Frontier	0	35	PPPoE LLC

United States	Grande ommunications	1	34	PPPoE LLC
United States	GWI	0	35	1483 Bridged IP LLC
United States	Hotwire	0	35	1483 Bridged IP LLC
United States	Internet Junction	0	35	1484 Bridged IP LLC
United States	PVT	0	35	1485 Bridged IP LLC
United States	QWest (1)	0	32	PPPoALLC
United States	QWest (2)	0	32	PPPoA VC-MUX
United States	QWest (3)	0	32	1483 Bridged IP LLC
United States	QWest (4)	0	32	PPPoE LLC
United States	SBC (1)	0	35	PPPoE LLC
United States	SBC (2)	0	35	1483 Bridged IP LLC
United States	SBC (3)	8	35	1483 Bridged IP LLC
United States	Sonic	0	35	1484 Bridged IP LLC
United States	SouthWestern Bell	0	35	1483 Bridged IP LLC
United States	Sprint (1)	0	35	PPPoALLC
United States	Sprint (2)	8	35	PPPoE LLC
United States	Sprint Territory	0	35	PPPoE LLC
United States	SureWest Communications(1)	0	34	1483 Bridged LLC Snap
United States	SureWest Communications(2)	0	32	PPPoE LLC
United States	SureWest Communications(3)	0	32	PPPoA LLC
United States	Toast.Net	0	35	PPPoE LLC
United States	Uniserv	0	33	1483 Bridged IP LLC
United States	US West	0	32	PPPoA VC-MUX
United States	Verizon (1)	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United States	Windstream	0	35	PPPoE LLC

Canada	Primus Canada	0	35	PPPoE LLC
Canada	Rogers Canada (1)	0	35	PPPoE LLC
Canada	Rogers Canada (2)	8	35	1483 Bridged IP LLC
Canada	Rogers Canada (3)	0	35	1484 Bridged IP LLC
Canada	BellSouth(1) Canada	8	35	PPPoE LLC
Canada	BellSouth(2) Canada	0	35	PPPoE LLC
Canada	Sprint (1) Canada	0	35	PPPoA LLC
Canada	Sprint (2) Canada	8	35	PPPoE LLC
Canada	Verizon (1) Canada	0	35	PPPoE LLC
Canada	Verizon (2) Canada	0	35	1483 Bridged IP LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United Kingdom (1)		0	38	PPPoA VC-MUX
United Kingdom (2)		0	38	PPPoE LLC
United Kingdom	AOL	0	38	PPPoE VC-MUX
United Kingdom	Karoo	1	50	PPPoA LLC
Venezuela	CANTV	0	33	1483 Routed IP LLC
Vietnam		0	35	PPPoE LLC
Vietnam	VDC	8	35	PPPoE LLC
Vietnam	Viettel	8	35	PPPoE LLC
Vietnam	FPT	0	33	PPPoE LLC
Russia	Rostel	0	35	PPPoE LLC
Russia	Port telecom	0	35	PPPoE LLC
Russia	VNTC	8	35	PPPoE LLC
Uzbekistan	Sharq Stream	8	35	PPPoE LLC
Uzbekistan	Sarkor	0	33	PPPoE LLC
Uzbekistan	TShTT	0	35	PPPoE LLC
Kazakhstan	Kazakhtelecom	0	40	LLC/SNAP Bridging

	Megaline			
Spain	Arrakis	0	35	1483 Bridged IP VC-MUX
Spain	Auna	8	35	1483 Bridged IP VC-MUX
Spain	Comunitel	0	33	1483 Bridged IP VC-MUX
Spain	Eresmas	8	35	1483 Bridged IP VC-MUX
Spain	Jazztel	8	35	IPOE VC-MUX
Spain	Jazztel ADSL2+ / Desagregado	8	35	1483 Bridged IP LLC-BRIDGING
Spain	OpenforYou	8	32	1483 Bridged IP VC-MUX
Spain	Tele2	8	35	1483 Bridged IP VC-MUX
Spain	Telefónica (España)	8	32	1483 Bridged IP LLC/SNAP
Telefónica (Argentina)		8	35	1483 Bridged IP LLC-based
Telefónica (Perú)		8	48	1483 Bridged IP VC-MUX
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Uni2	1	33	1483 Bridged IP VC-MUX
Spain	Orange	8	35	1483 Bridged IP VC-MUX
Spain	Orange 20 Megas	8	35	LLC-BRIDGING
Spain	Orange	8	32	1483 Bridged IP LLC/SNAP
Spain	Ya.com	8	32	1483 Bridged IP VC - MUX
Spain	Ya.com	8	32	1483 Bridged IP LLC/SNAP
France	Free	8	36	LLC
Netherlands	MXSTREAM	8	48	1483 Bridged IP LLC
Netherlands	BBNED	0	35	1483 Bridged IP LLC
Belgium	Turboline	8	35	1483 Bridged IP LLC
Belgium	ADSL Office	8	35	1483 Bridged IP LLC

UK		0	38	1483 Bridged IP LLC
Italy		8	35	1483 Bridged IP LLC
Switzerland		8	35	1483 Bridged IP LLC
SpainWanadoo		8	32	1483 Bridged IP LLC
Czech Republic		8	48	1483 Bridged IP LLC
Dubai		0	50	1483 Bridged IP LLC
UAE (Al sahmil)		0	50	1483 Bridged IP LLC
Egypt:	TE-data	0	35	1483 Bridged IP LLC
Egypt:	Linkdsl	0	35	1483 Bridged IP LLC
Egypt:	Vodafone	8	35	1483 Bridged IP LLC
kuwait		0	33	1483 Bridged IP LLC
unitednetwork				
Pakistan (PALESTINE)		8	35	1483 Bridged IP LLC
Dominican Republic		0	33	1483 Bridged IP LLC
Orange Nyumbani (Kenya)		0	35	PPPoE LLC
Pakistan for PTCL		0	103	1483 Bridged IP LLC
Sri Lanka Telecom-(SLT)		8	35	PPPOE LLC
Philippines(1)		0	35	1483 Bridged IP LLC
Philippines(2)		0	100	1483 Bridged IP LLC
RomTelecom Romania:		0	35	1483 Bridged IP LLC
Finland	Saunalahti	0	100	1483 Bridged IP LLC
Finland	Elisa	0	100	1483 Bridged IP LLC
Finland	DNA	0	100	1483 Bridged IP LLC
Finland	Sonera	0	35	1483 Bridged IP LLC

Iran	Shatel Aria-Rasaneh-Tadbir	0	35	PPPOE LLC
Iran	Asia-Tech	0	35	PPPOE LLC
Iran	Pars-Online (Tehran)	0	35	PPPOE LLC
Iran	Pars-Online (Provinces)	0	59	PPPOE LLC
Iran	Saba-Net Neda-Gostar-Saba	0	35	PPPOE LLC
Iran	Pishgaman-Tose	0	35	PPPOE LLC
Iran	Fan-Ava	8	35	PPPOE LLC
Iran	Datak	0	35	PPPOE LLC
Iran	Laser (General)	0	35	PPPOE LLC
Iran	Laser (Privates)	0	32	PPPOE LLC
Iran	Asr-Enteghal-Dadeha	8	35	PPPOE LLC
Iran	Kara-Amin-Ertebat	0	33	PPPOE LLC
Iran	ITC	0	35	PPPOE LLC
Iran	Dadegostar Asre Novin	0	33	PPPOE LLC
India	Airtel	1	32	1483 Bridged IP LLC
India	BSNL	0	35	1483 Bridged IP LLC
India	MTNL	0	35	1483 Bridged IP LLC
India	RELIANCE COMMUNICATION	0	35	PPPOE LLC
India	TATA INDICOM	0	32	PPPOE LLC
India	CONNECT	1	32	PPPOE LLC
morocco	IAM	8	35	PPPOE
Malaysia	Streamyx	0	35	PPPOE LLC
Indonesia Speedy Telkomnet		8	81	PPPoE LLC

Appendix 4 Regulatory Compliance Information



CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures. This device complies with EU 1999/5/EC.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.



FCC Statement

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.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

— Reorient or relocate the receiving antenna.

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.