Inteno

User Manual
X5671

VDSL2/ADSL2+ router with 4-Port Ethernet Switch and 802.11b/g wireless AP

Issue 1.1
5th May. 2008

Inteno Broadband Technology AB
Tel: +46 8 579 190 00
Drivhjulsvägen 22, SE-126 30, Hägersten, Sweden

Inteno Broadband Technology AB provides this documentation without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Table of Contents

1 Introduction

Congratulations on becoming the owner of the **X5671**, VDSL2 with 4 Ethernet ports switch and 802.11g wireless gateway. You will now be able to access the Internet using your high-speed connection.

The **X5671** is a gateway integrating VDSL2, 4 Ethernet ports switch and 802.11g wireless interfaces into one device which provides the most flexibility and efficiency way to you. You could connect devices like PCs, Set-Top-Box, ATA, servers, phone and so on easily by Ethernet and wireless interfaces to enjoy data, voice, and video services immediately through high speed connection.

This User Guide will show you how to connect your **X5671** gateway and how to customize its configuration to get the most out of your new product.

Features

The list below contains the main features of the device (**X5671**) and may be useful to users with knowledge of networking protocols. The chapters throughout this guide will provide you with enough information to get the most out of your device.

The features include:

- Ethernet interface automatic speed-sensing and crossover correction supports up to 100 Mbps downstream and 100 Mbps upstream rates
- Integrated four-port 10/100BaseTX Ethernet switch with speed-sensing and crossover detection automatically
- 802.11b/g WLAN supports up to 54 Mbps transmission rate
- Provides wireless secure transmitting encryption by either 802.1x; WEP; WEP2; WPA; WPA2; TKIP; AES
- Support Networking protocols such as PPP, Routing, RIP and so on
- Support DHCP client and server for IP management
- Support Port Forwarding (virtual server) and MAC address filtering
- Network address translation (NAT) functions to provide security for your LAN and multiple PCs surfing Internet simultaneously.
- Configuration and management by Web-browser through the Ethernet interface and remotely through WAN interface
- Firmware Supports TR-069
- Upgradeable through HTTP (web browser)

Device Requirements

In order to use the **X5671**, you must have the following:

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

Note

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

2 Getting to know the device

Parts Check

In addition to this document, your package should arrive containing the following:

- ***The device (X5671)***
- ***Ethernet cable***
- ***Standard phone line cable***
- ***Power adapter***

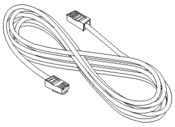
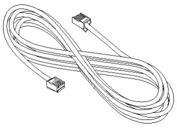
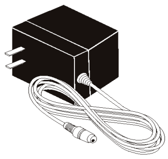
	One of **X5671** devices
	RJ-45 Cable
	RJ-11 Cable
	Power adapter

Figure 1: X5671 Package Contents

X5671 Front Panel

The front panel of this **X5671** will be described here which cover all front panel definitions of other models.

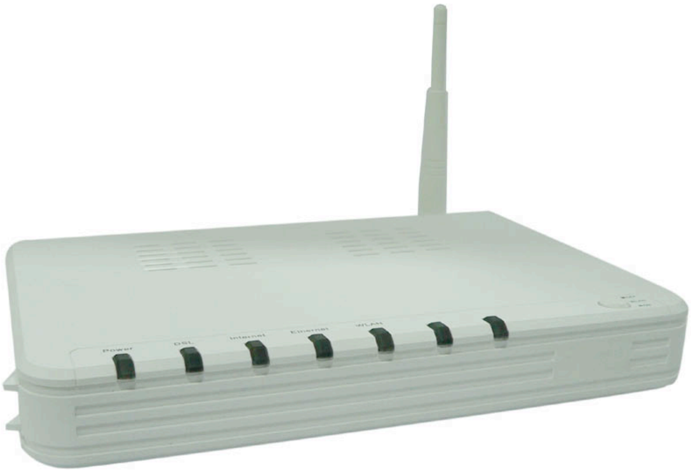


Figure 2: X5671 Front Panel and LEDs

Connector and LED definitions from left to right:

Label	Color	Function
Power	Green or Red	GREEN off : No power GREEN on : Power on RED on : Self-test fails
DSL	Green / Yellow	On : Physical layer sync up successfully. Off : No connection or no signal Blink : Physical sync up progress
Internet	Green or Red	GREEN off : No connection to Internet GREEN on : The device gets an IP address successfully in router mode GREEN blinking : Data being transmitted. RED on : PPP Authenication of the device failed. Or it can not get an IP address in ROUTER mode.
Ethernet	Green	On : LAN link established and active Off : No LAN link Blink : Data being transmitted
WLAN	Green	On : WLAN service is enabled Off : WLAN service is disabled Blink : Data being transmitted

X5671 Rear Panel

The rear panel of this **X5671** will be described here which cover all rear panel definitions of other models.

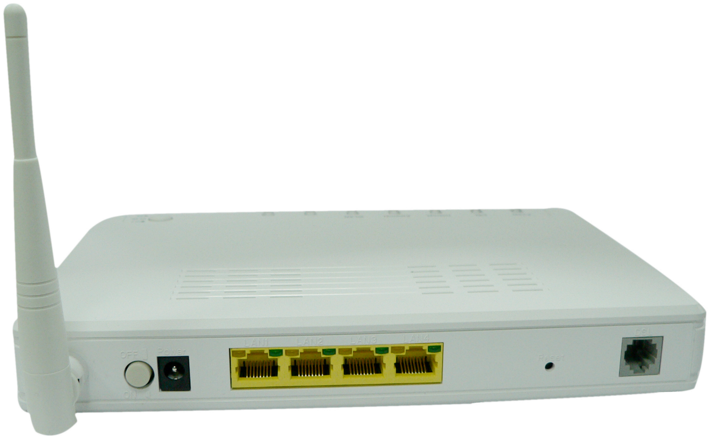


Figure 3: X5671 Rear Panel Connections

Connector definition:

Label	**Function**
Antenna	Connects to the 802.11b/11g enabled wireless devices in LAN
Power Switch	ON/OFF switch
Power Jack	Connects to the supplied power adapter
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
Reset	A reset button to reset the device or reset to default settings
DSL Jack	Connects to the VDSL2 network

3 Connecting your device

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

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

Configuring Ethernet PCs section

Configuring Wireless PCs section

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

Connecting the Hardware

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

WARNING

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

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

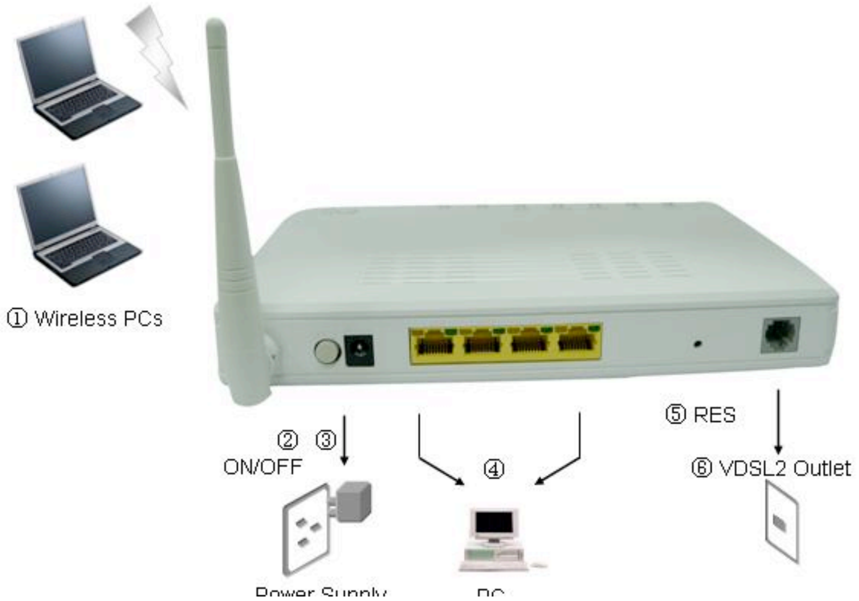


Figure 4: Overview of Hardware Connections for X5671

Step 1. Connect the WAN port to VDSL2 network

Connect the WAN port to the VDSL2 network which has the high speed internet connection.

Step 2. Connect the Ethernet cable

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

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

Step 3. Attach the power connector

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

Step 4. Configure your Ethernet PCs

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

Or, step 5. Install a Wireless card and connect Wireless PCs if the device is with wireless interface

You can attach a Wireless LAN that enables Wireless PCs to access the Internet via the device.

You must configure your Wireless computer(s) in order to access your device. For complete instructions, see Configuring Wireless PCs section.

Next step

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

4 Getting Start with the Web pages

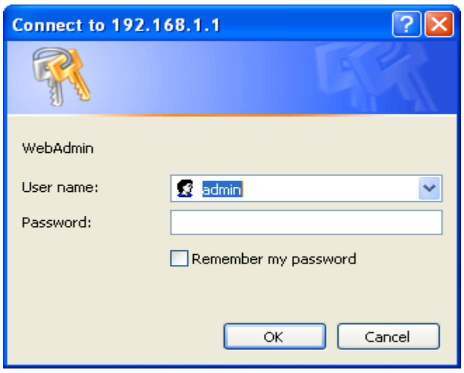
The device includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through a web browser on a PC connected to the device.

Accessing the Web pages

To access the web pages, you need the following:

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

A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox from any of the LAN computers, launch your web browser, type the URL, http://192.168.1.1 in the web address (or location) box, and press [Enter]. The default IP address of the device is 192.168.1.1. Then enter the default username and password: admin/admin to access the configuration web page, if you have not changed the username and password. Please be informed that strings of username and password are case-sentitive.



Connect to 192.168.1.1

WebAdmin

User name: admin

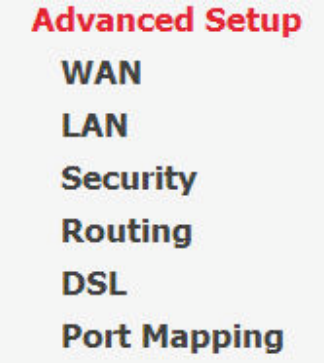
Password:

Figure 5: Login Page

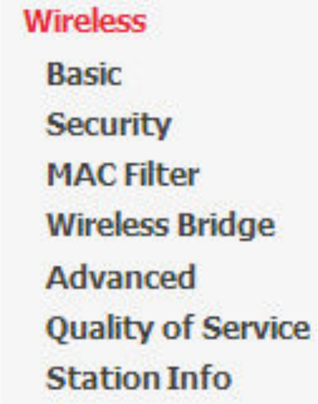
The Menu comprises:

Device Information: provides the basic information of the system. It includes sub menus, Summary, WAN, Statistics Route, and ARP.

Advanced Setup: provides information about the current configuration of various system features with options to change the configuration. It includes the sub menus WAN, LAN, Security, Routing, DSL and Port Mapping.

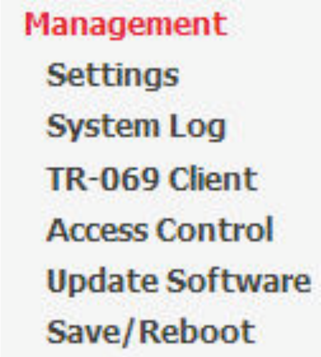


Wireless Setup: provides wireless SSID, security, key and various options to change the configuration. It includes the sub menu, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Quality of Service and Station Info.



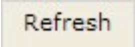
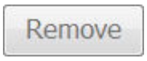
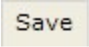
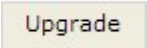
Diagnostic: provides the diagnostic utility to check the LAN and Wireless physical connection and ADSL connection as well.

Management: provides the administration utilities. It includes the sub menus, Settings, System Log, TR-069 Client, Access Control, Update Software, and Save/Reboot.



Commonly used buttons

The following buttons are used throughout the web pages:

Button	Function
	You could click this button to refresh the information on this current page again so that you could get the real time information.
	You click this button to create an entry into the list.
	You click this button to delete (remove) an entry from the list.
	check button – these appear on many configuration pages. You will be asked to check if you want this feature be selected.
	This button appears on every configuration page. Click on this button once you are through with the changes and decide to save the made changes.
	You may need to browse to find a file which needs to be uploaded for new configuration.
	This button allows you to upgrade to the new configuration file attached using the Browse button.

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

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

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

Testing your Setup

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

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

LED	Behavior
Power (PWR)	Solid red to indicate that the device is turned on. If this light is not on, check the power cable attachment.
Wireless (WLAN)	Solid green to indicate that the Wireless LAN function is operational.
Ethernet	Solid green to indicate that the device can communicate with your LAN.
DSL	Solid green to indicate that the device has successfully established a connection with your ISP.

Table 1: LED Indicators

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

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

Default device settings

The device is preconfigured with default settings for use with a typical home or small office network.

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

⚠ WARNING

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

Option	Default Setting	Explanation/Instructions
User/Password	admin/admin	User name and password to access the device
LAN Port *IP Address*	Assigned static IP address: 192.168.1.1 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See *Local Network* section.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.2 through 192.168.1.254 (Please be noted that the default DHCP IP address pool may be different in each firmware version.)	The device maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in *DHCP Server* section.

Table 2: Values of Default Settings (please check default setting.)

5 Device Information

The Device Information web page menu includes the following submenus:

Summary

WAN

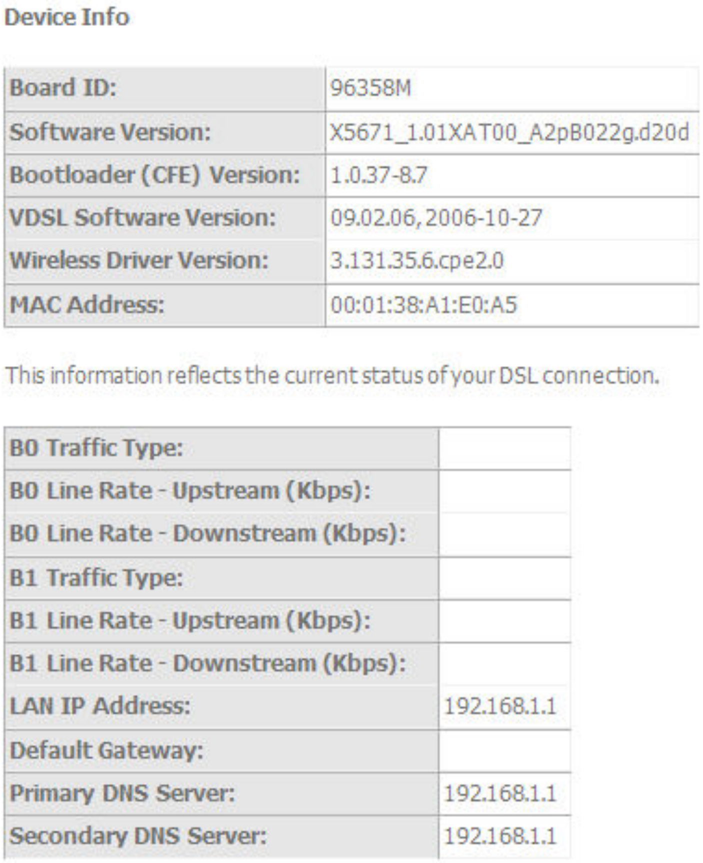
Statistics

Route

ARP

Summary

The Summary Page of the device shows the following information, Board ID, Software version, Bootloader version, VDSL software version, Wireless driver version, and MAC address. Besides, LAN IP, Default gateway, Primary DNS server and Secondary DNS server are shown too.



Device Info

Board ID:	96358M
Software Version:	X5671_1.01XAT00_A2pB022g.d20d
Bootloader (CFE) Version:	1.0.37-8.7
VDSL Software Version:	09.02.06, 2006-10-27
Wireless Driver Version:	3.131.35.6.cpe2.0
MAC Address:	00:01:38:A1:E0:A5

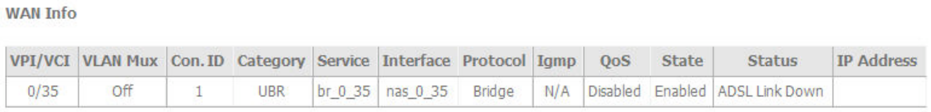
This information reflects the current status of your DSL connection.

B0 Traffic Type:	
B0 Line Rate - Upstream (Kbps):	
B0 Line Rate - Downstream (Kbps):	
B1 Traffic Type:	
B1 Line Rate - Upstream (Kbps):	
B1 Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

Figure 6: Device Information

WAN

The WAN information of the device shows detailed information about the WAN connection such as DSL port information (VPI/VCI, UBR/CBR/VBR and so on), Protocol, IGMP enabled or disabled, QoS enabled or disabled, IP address of WAN port and so on.



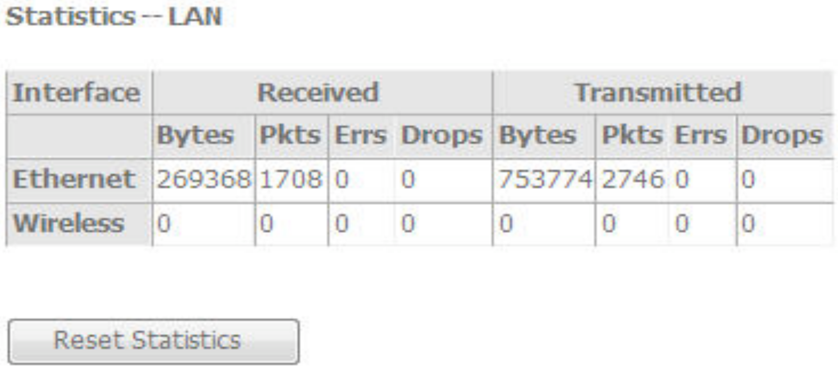
WAN Info

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address
0/35	Off	1	UBR	br_0_35	nas_0_35	Bridge	N/A	Disabled	Enabled	ADSL Link Down	

Figure 7: WAN Port Information

Statistic

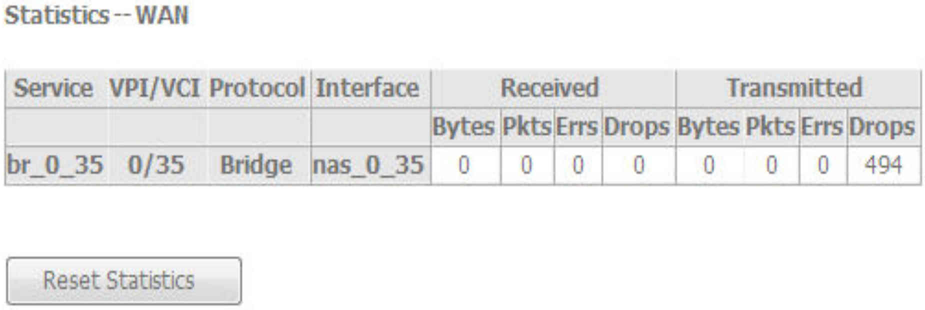
The Statistic Page of the device shows the following information, Interfaces, data transmitting (Received and Transmitted directions) in that interface such as total bytes, packets, error count and drop count of LAN port, WAN port, ATM, ADSL, and VDSL.



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	269368	1708	0	0	753774	2746	0	0
Wireless	0	0	0	0	0	0	0	0

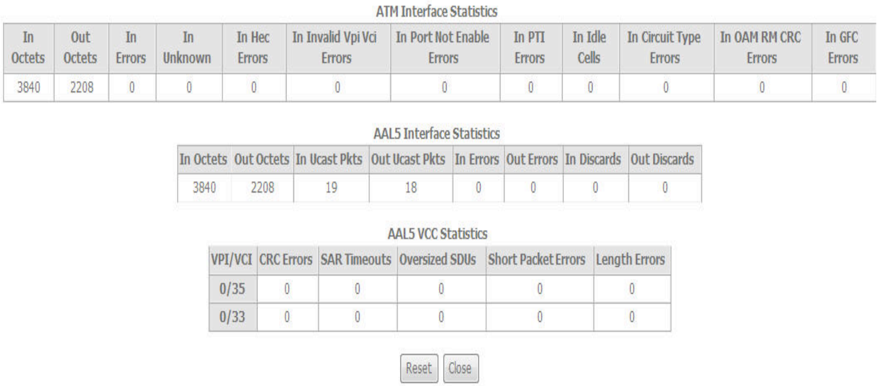
Figure 8: Device WAN Port Statistic Information



Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
br_0_35	0/35	Bridge	nas_0_35	0	0	0	0	0	0	0	494

Figure 9: Device LAN Port Statistic Information



ATM Interface Statistics

In Octets	Out Octets	In Errors	In Unknown	In Hec Errors	In Invalid Vpi Vci Errors	In Port Not Enable Errors	In PTI Errors	In Idle Cells	In Circuit Type Errors	In OAM RM CRC Errors	In GFC Errors
3840	2208	0	0	0	0	0	0	0	0	0	0

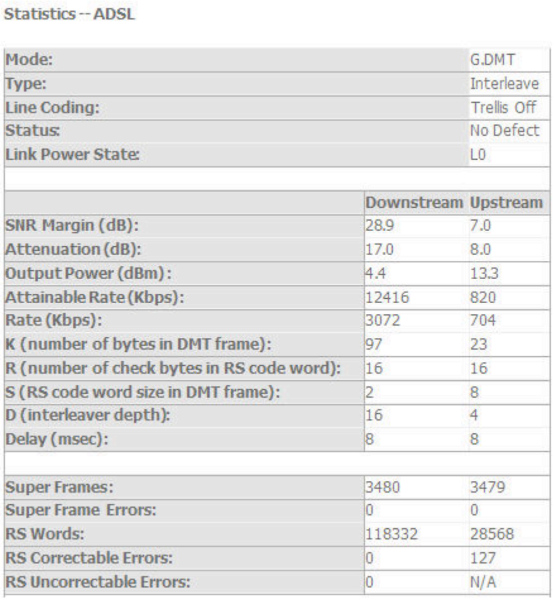
AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
3840	2208	19	18	0	0	0	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0/35	0	0	0	0	0
0/33	0	0	0	0	0

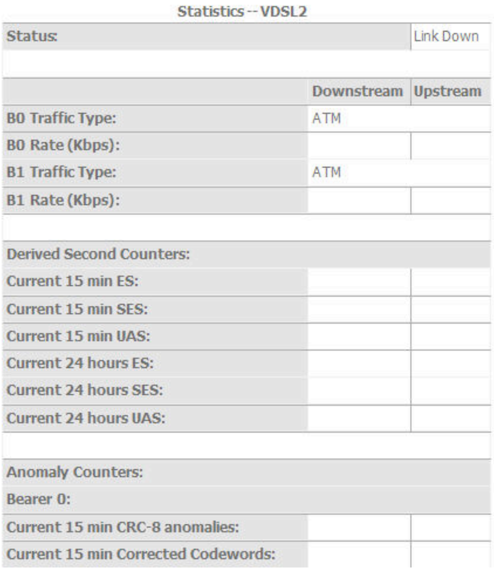
Figure 10: Device ATM Statistic Information



Statistics -- ADSL

Mode:	G.DMT	
Type:	Interleave	
Line Coding:	Trellis Off	
Status:	No Defect	
Link Power State:	L0	
	Downstream	Upstream
SNR Margin (dB):	28.9	7.0
Attenuation (dB):	17.0	8.0
Output Power (dBm):	4.4	13.3
Attainable Rate (Kbps):	12416	820
Rate (Kbps):	3072	704
K (number of bytes in DMT frame):	97	23
R (number of check bytes in RS code word):	16	16
S (RS code word size in DMT frame):	2	8
D (interleaver depth):	16	4
Delay (msec):	8	8
Super Frames:	3480	3479
Super Frame Errors:	0	0
RS Words:	118332	28568
RS Correctable Errors:	0	127
RS Uncorrectable Errors:	0	N/A

Figure 11: Device ADSL Statistic Information



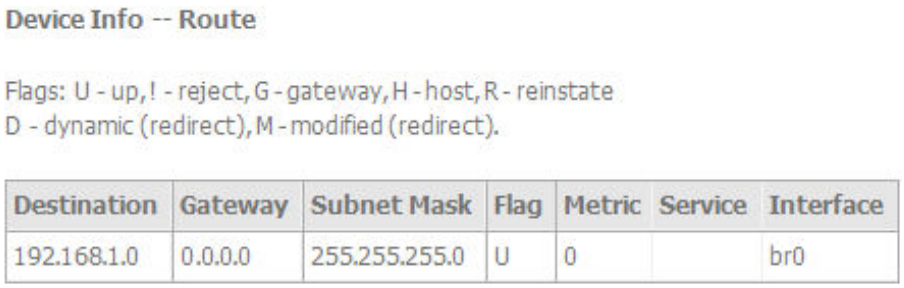
Statistics -- VDSL2

Status:	Link Down	
	Downstream	Upstream
B0 Traffic Type:	ATM	
B0 Rate (Kbps):		
B1 Traffic Type:	ATM	
B1 Rate (Kbps):		
Derived Second Counters:		
Current 15 min ES:		
Current 15 min SES:		
Current 15 min UAS:		
Current 24 hours ES:		
Current 24 hours SES:		
Current 24 hours UAS:		
Anomaly Counters:		
Bearer 0:		
Current 15 min CRC-8 anomalies:		
Current 15 min Corrected Codewords:		

Figure 12: Device VDSL Statistic Information

Route

The Route Page of the device shows the route table. It contains Destination IP address, Gateway, Subnet Mask, Flag, Metric, Service and Interface.



Device Info -- Route

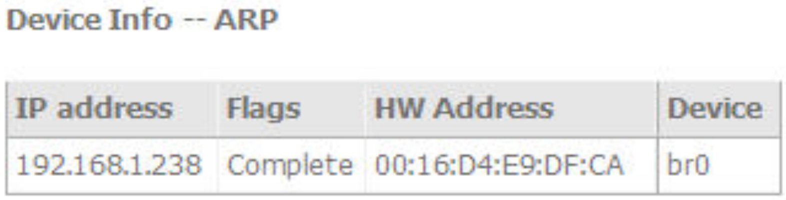
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Figure 13: Device Route Table Information

ARP

The ARP Page of the device shows the ARP table mapping the IP address and related MAC address. The ARP table contains IP address, Flag, MAC address, Device Interface.



Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.238	Complete	00:16:D4:E9:DF:CA	br0

Figure 14: Device ARP Table Information

6 Advanced Setup

The Advance Setup menu includes the sub menus WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, and Port Mapping.

WAN

LAN

Security

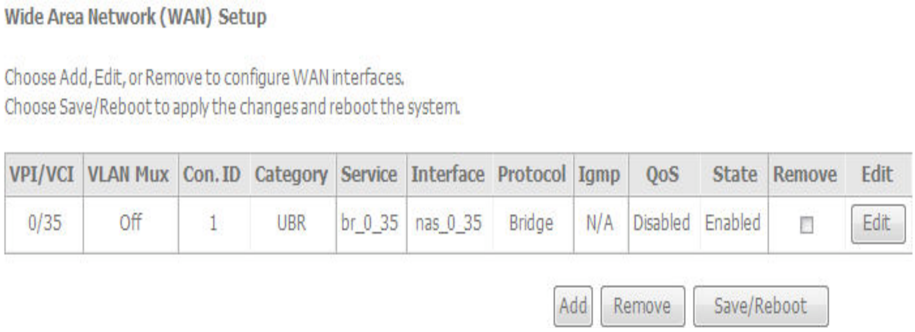
Routing

DSL

Port Mapping

WAN

You can configure your internet connection from this page. This page displays the details of existing internet connection. The device allows 1 bridge connection and 1 route connection existing at that same time without VLAN setting. But if you need more than 1 bridge connection or 1 route connection, the VLAN tag is required. Please refer below for more details. There are three connection types can be configured including PPP over Ethernet (PPPoE), IP over Ethernet, and Bridging.



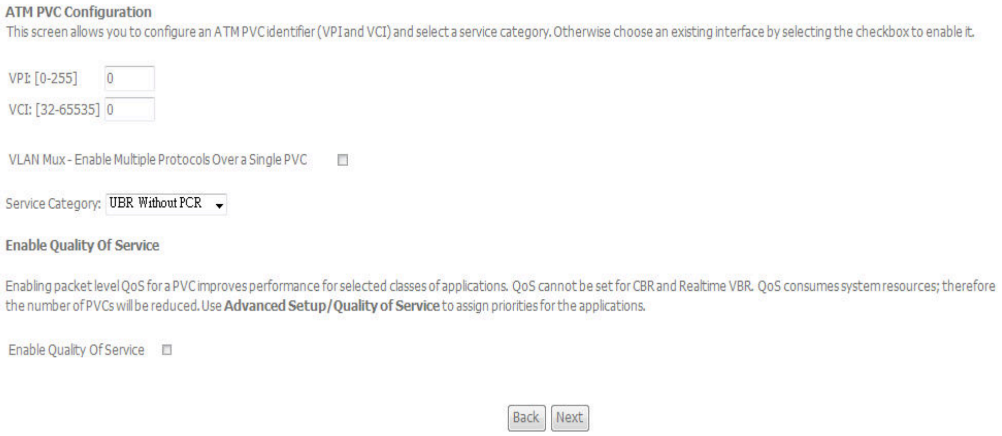
Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/35	Off	1	UBR	br_0_35	nas_0_35	Bridge	N/A	Disabled	Enabled	□	Edit

Figure 15: WAN Setup Page

To configure the WAN port, click Edit or Add to get the configuration pages. If there are many services (protocols) in the single PVC interface, please enter the unique VLAN tag number to identify the service (protocol).



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255] 0

VCI: [32-65535] 0

VLAN Mux - Enable Multiple Protocols Over a Single PVC □

Service Category: UBR Without PCR

Enable Quality Of Service

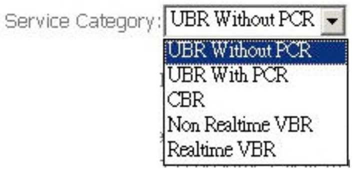
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service □

Figure 16: WAN Port Configuration

To configure ATM PVC on the WAN interface:

- Enter *VPI/VCI* values
- Check to enable the *VLAN Mux* that allows multiple protocols in the same PVC and then enter the *802.11Q VLAN ID* valued from 0 to 4095
- Select the Service Category from the list (UBR without PCR, UBR with PCR, CBR, Non Realtime VBR, Realtime VBR). Please leave it as default, UBR with PCR, if ISP does not give you any information of this setting.
- Check to enable the Qualify of Service if Service Category is UBR without PCR, URB with PCR or Non Realtime VBR and you like this service. Select the Service Category from the list (UBR without PCR, UBR with PCR, CBR, Non Realtime VBR, Realtime VBR). Please leave it as default, if ISP does not give you any information of this setting.



Service Category: UBR Without PCR

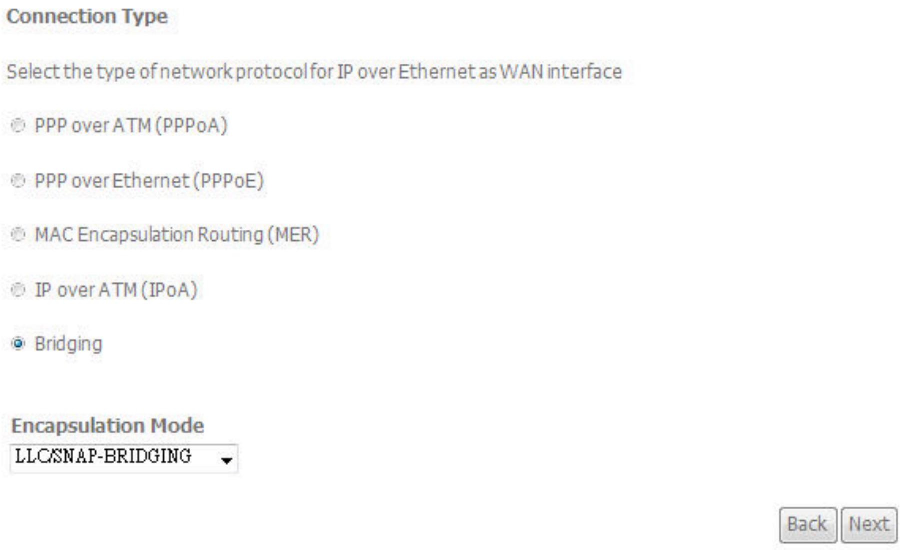
Figure 17: Service Category Configuration

PCR stands for Peak Cell Rate (ATM cells per second). It is the maximum allowable rate which cells can be transferred in the connection.

SCR stands for Sustainable Cell Rate (ATM cells per second). It is an average allowable rate which cells can be transferred in the connection.

MRS stands for Maximum Burst Size (ATM cells). It is the maximum allowable burst size of cells which cells can be transferred in the connection.

- Click *Next* to configure the Connection Type



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

○ PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

● Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

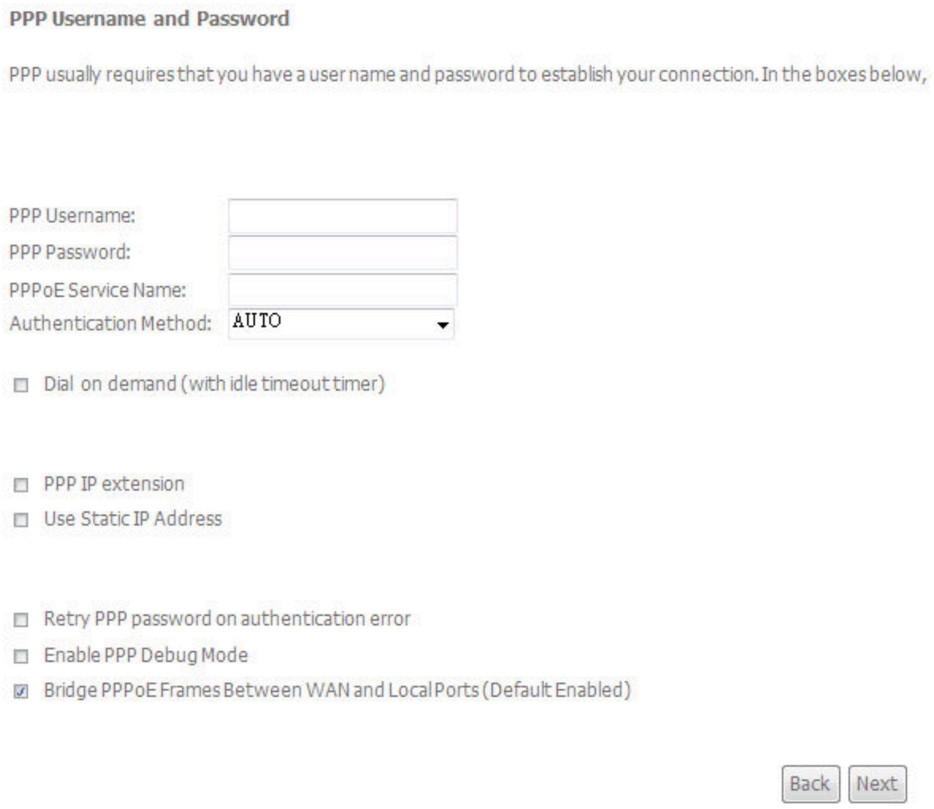
Figure 18: WAN Connection Type Configuration

Global settings:

- Check the *WAN protocol* from PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), MAC Encapsulation Routing (MER), IP over ATM (IPoA) and Briding.

- Select the *Encapsulation Mode* from the list (LLC/SNAP-BRIDGING, LLC/SNAP-Routing or VC/MUX)
- Click *Next*

PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)



PPP Username and Password

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

PPP Username:	
PPP Password:	
PPPoE Service Name:	
Authentication Method:	AUTO

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Use Static IP Address

□ Retry PPP password on authentication error

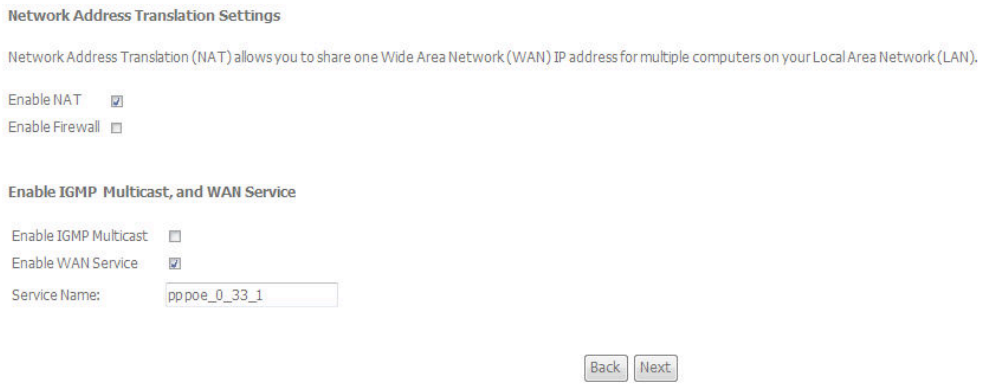
□ Enable PPP Debug Mode

☑ Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

Figure 19: WAN Connection, PPPoA or PPPoE Configuration

To configure the PPPoA or PPPoE settings:

- Enter the User's PPP *Username* and *Password*
- Enter the *Service Provider Name* if any
- Select the *Authentication Method* used during negotiation, default is AUTO.
- Check "*Dial On Demand*" if you do not need PPPoA or PPPoE connection always ON and enter the timeout value to disconnect the PPPoA or PPPoE connection when connection is idle and timeout. If you enter "0", zero for the timeout value, it means always ON.
- Check the "*IP extension"* if your ISP requests to enable it, otherwise do not select it. This is a special service to forward IP address assigned by remote to the local device in the LAN.
- Check the "*Use Static IP address"* and enter the IP address if your ISP assigns a fixed IP address to you. Otherwise, do not select it.
- Check to enable "*Retry PPP Password on Authentication Error*".
- Check to enable "*PPP Debug Mode*"
- This "*Bridge PPP frames between WAN and Local Ports*" is checked in default.
- Click *Next*



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 Firewall □

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

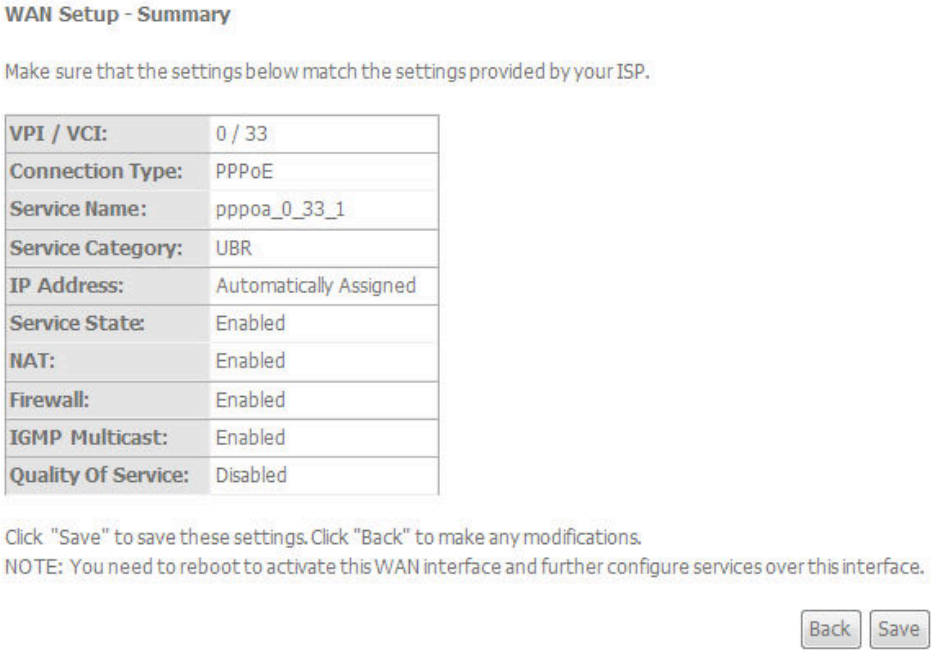
Service Name: pppoe_0_33_1

Figure 20: WAN Connection, PPPoA or PPPoE Configuration

NAT (Network Address Translation) setting:

- Check to enable *NAT* that allows multiple PCs surfing Internet simultaneously by using the same WAN IP address.
- Check to enable *Firewall*
- Check to enable *IGMP Multicast* to avoid the multicast packet flooding to other LAN ports where do not need this IGMP packet to get better efficiency in Ethernet port.
- Check to enable *WAN service*
- Enter the *Service Name* if you want to change it.
- Click *Next*

The *WAN Setup Summary* page shows all of parameters.



WAN Setup - Summary

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

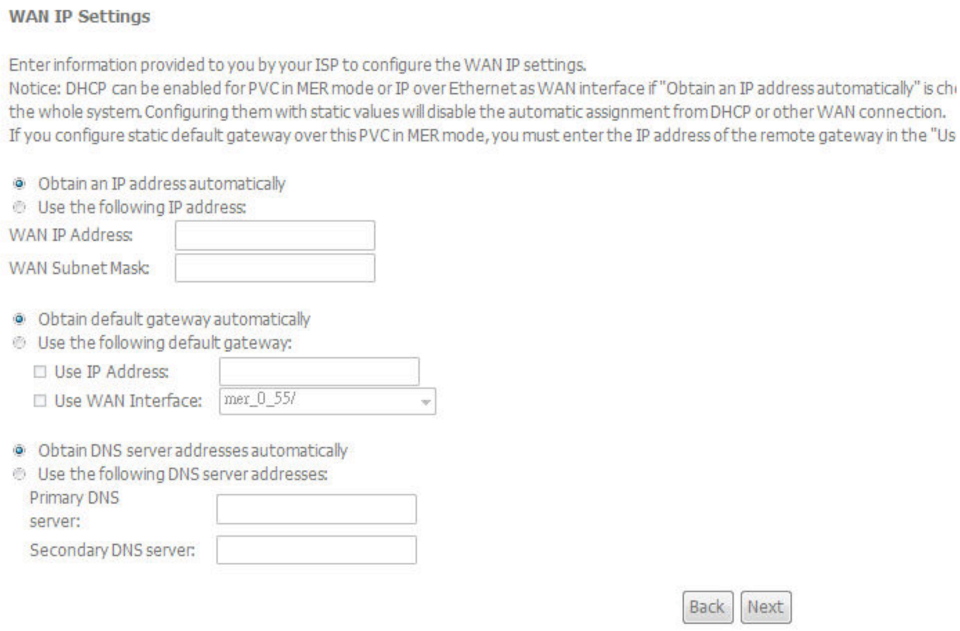
VPI / VCI:	0 / 33
Connection Type:	PPPoE
Service Name:	pppoa_0_33_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

Figure 21: WAN Connection, PPPoA or PPPoE Configuration

Click *Save* if correct and click *Back* to restart the configuration again.

MAC Encapsulation Routing (MER)



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is ch
the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Us

● Obtain an IP address automatically
○ Use the following IP address:
WAN IP Address:
WAN Subnet Mask:

● Obtain default gateway automatically
○ Use the following default gateway:
□ Use IP Address:
□ Use WAN Interface: mer_0_55/

● Obtain DNS server addresses automatically
○ Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:

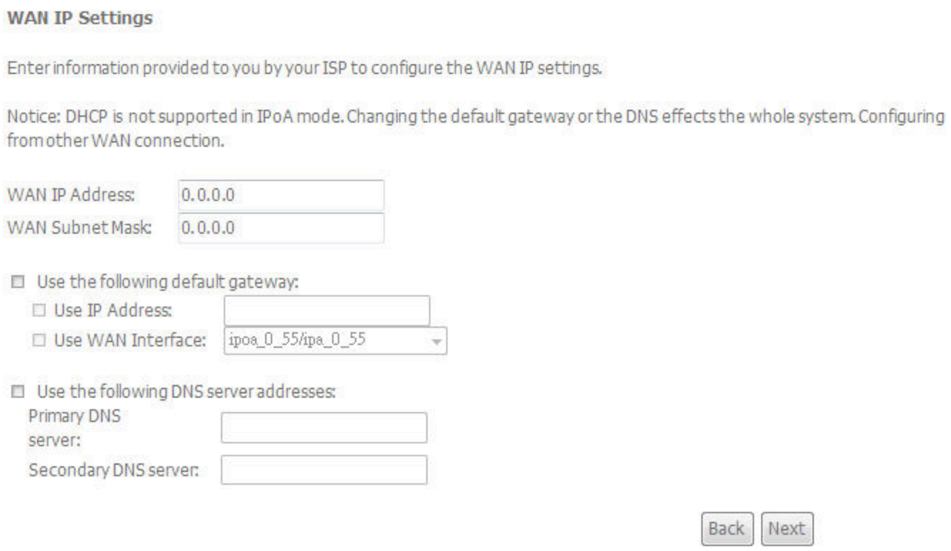
Figure 22: WAN Connection,MER Configuration

To configure the IP over Ethernet settings:

- Select "*Obtain an IP address automatically*" or "*Use the following (fixed) IP address*" and then also enter the *WAN IP address* and *WAN Subnet Mask*.
- Select "*Obtain default gateway automatically*" or "*Use the following default gateway*" and then also enter the *gateway IP address* and *Use WAN Interface* where packets will be sent to.
- Select "*Obtain DNS server address automatically*" or "*Use the following DNS server addresses*" and then also enter the IP addresses of *Primary DNS server* and *Secondary DNS server.*
- Click *Next*

The *NAT configuration* and *WAN Setup Summary* page will show up. Please refer related pages above for reference. Click *Save* if correct and click *Back* to restart the configuration again.

IP over ATM (IPoA)



WAN IP Settings

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

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring from other WAN connection.

WAN IP Address: 0.0.0.0

WAN Subnet Mask: 0.0.0.0

☐ Use the following default gateway:

☐ Use IP Address:

☐ Use WAN Interface: ipoa_0_55/ipa_0_55

☐ Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

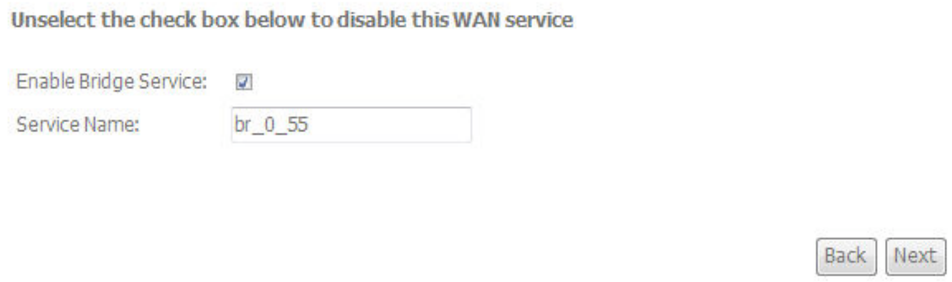
Figure 23: WAN Connection,MER Configuration

To configure the IP over Ethernet settings:

- Enter the *WAN IP address* and *WAN Subnet Mask*.
- Select "*Use the following default gateway*" and then also enter the *gateway IP address* and *Use WAN Interface* where packets will be sent to.
- Select "*Use the following DNS server addresses*" and then also enter the IP addresses of *Primary DNS server* and *Secondary DNS server.*
- Click *Next*

The *NAT configuration* and *WAN Setup Summary* page will show up. Please refer related pages above for reference. Click *Save* if correct and click *Back* to restart the configuration again.

Bridging



Unselect the check box below to disable this WAN service

Enable Bridge Service: ☑

Service Name: br_0_55

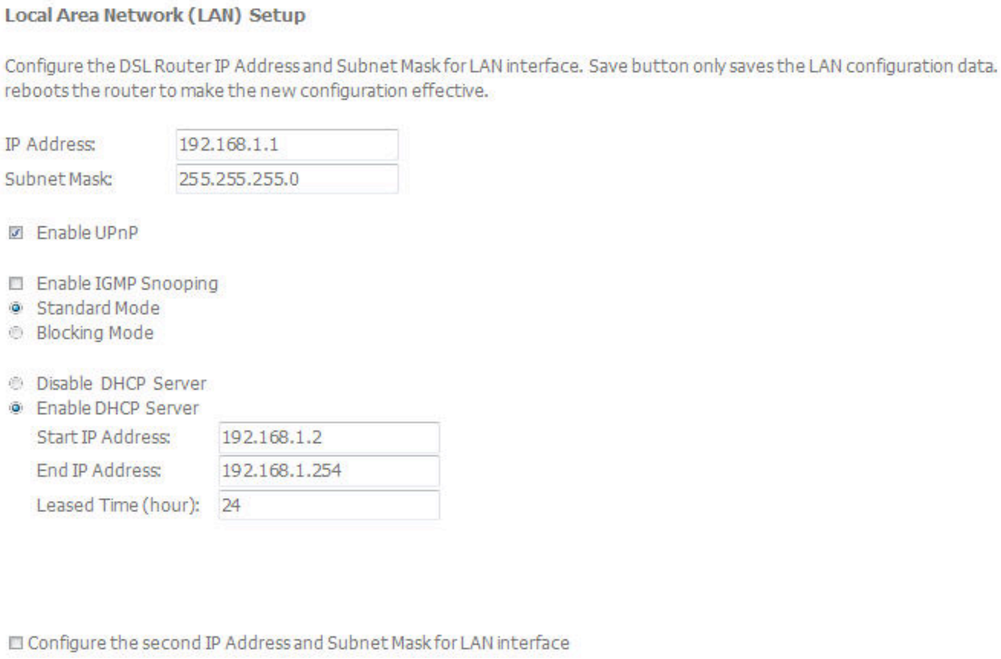
Figure 24: WAN Connection, Bridging Configuration

To configure the Bridging settings:

- Check "*Enable Bridge Service*" to enable bridge service
- Enter the *Service Name* for this bridging interface.
- Click *Next*

The *WAN Setup Summary* page shows all of parameters. Click *Save* if correct and click *Back* to restart the configuration again.

LAN



Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. reboots the router to make the new configuration effective.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☑ Enable UPnP

□ Enable IGMP Snooping

● Standard Mode

○ Blocking Mode

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

□ Configure the second IP Address and Subnet Mask for LAN interface

Figure 25: LAN Configuration

To configure LAN:

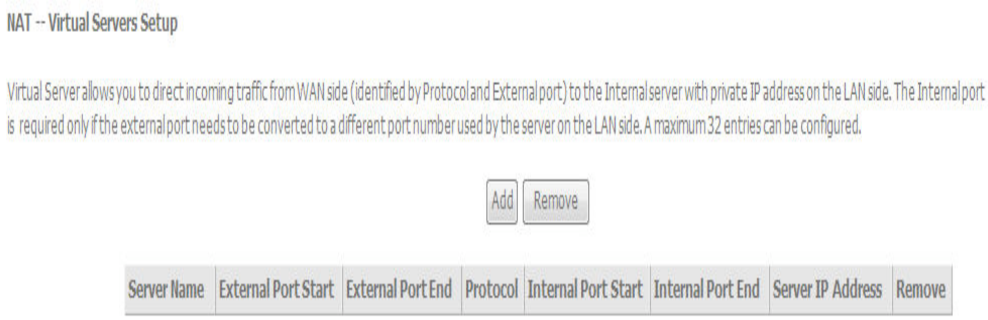
- Enter the *IP address* which the CPE in the LAN will use to connect to the device. For example, enter 192.168.1.1
- Enter the *Subnet Mask*. For example, enter 255.255.255.0
- Check to *Enable UPnP* feature
- Check to *Enable IGMP Snooping*. This feature will snoop all of IGMP packets and record related information. Therefore, multicast packets will be generated to the related LAN ports only to avoid the packet flooding on all of LAN ports. Select one of two modes, *Standard mode* or *Blocking mode*.
- Select to *Enable or Diable DHCP server*. If it is enabled, please enter the DHCP IP pool of *Start IP address* and *End IP address*. Enter the value of *leased time* of hour about the valid period of assigned IP address. The DHCP server ON (enabled) feature will enable this device to assign IP address automatically to PC in LAN if PC requests an IP address by DHCP client protocol.
- Check to enable "*Configure the second IP Address and Subnet Mask for LAN interface*" and enter the *IP address* and *Subnet Mask*. This is a feature to create second IP address/subnet in the LAN interface, so that the device can support two different IP address/subnet networks simultaneously.
- Click *Save* to save the configuration

NAT (Network Access Translation)

The NAT feature provides the basic firewall feature to avoid hacker attacks from remote site. There are three more setting pages including virtual server, port trigger, DMZ and ALG to provide specified service for remote users.

Virtual Server

Virtual Server enables you to run a server on your local network that can be accessed from the remote parties. You need to set up a rule to tell the device on which computer the server is held. When port virtual server is enabled, your router (the device) routes all the inbound traffic on a particular port to the chosen computer on your network.



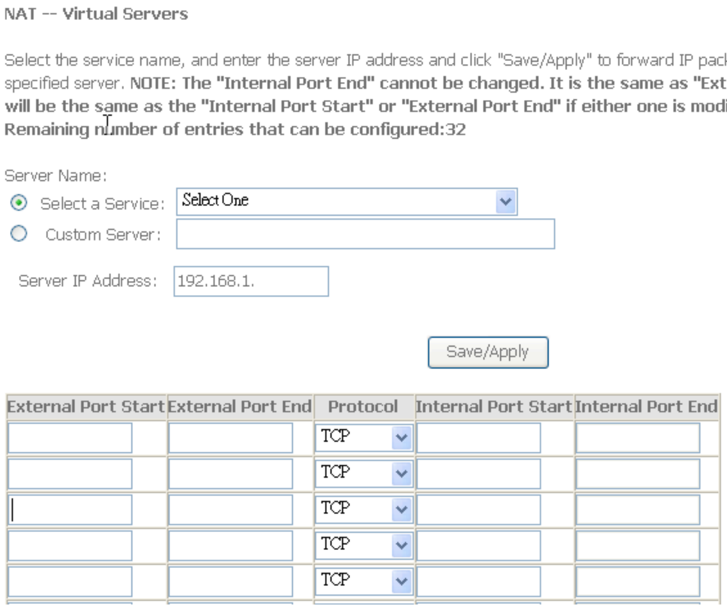
NAT -- Virtual Servers Setup

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.

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

Figure 26: Virtual Server Setup Configuration

Click *Add* to add a rule of virtual server.



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.
Remaining number of entries that can be configured:32

Server Name:
● Select a Service: Select One
○ Custom Server:

Server IP Address: 192.168.1.

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

Figure 27: Add a Rule of Virtual Server

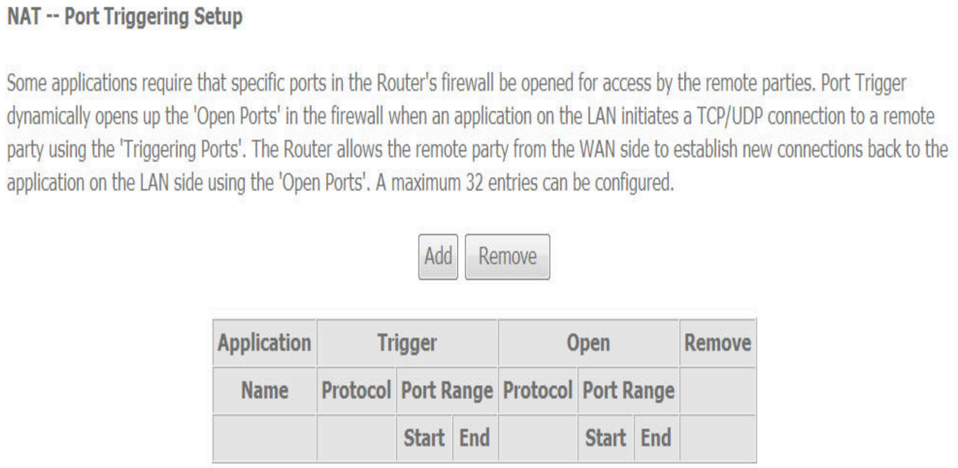
Global Setting

- Select a *service* from the predefined list or enter the name of *Custom Server*
- Enter the *Server IP Address* located in the LAN to provide the service to remote party

- Enter the *Start External Port #* and *End External Port #* that open to remote to access the service
- Select the *Protocol* from the list
- Enter the *Start Internal Port #* and *End Internal Port #* that may use different port # to secure the service. If you use the same port # as *external port #*, please leave *Internal Port #* as blank.
- Click *Save/Apply*

Port Triggering

The feature is similar to the virtual server, but provides a more secure way to provide your device. It opens up the port hole temporary and allows CPE in LAN to establish a connection with remote parties. Those ports are open only if a specified request from a PC in LAN is received, and then the device allows the remote parties to access to establish a connection with that PC in LAN.



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.

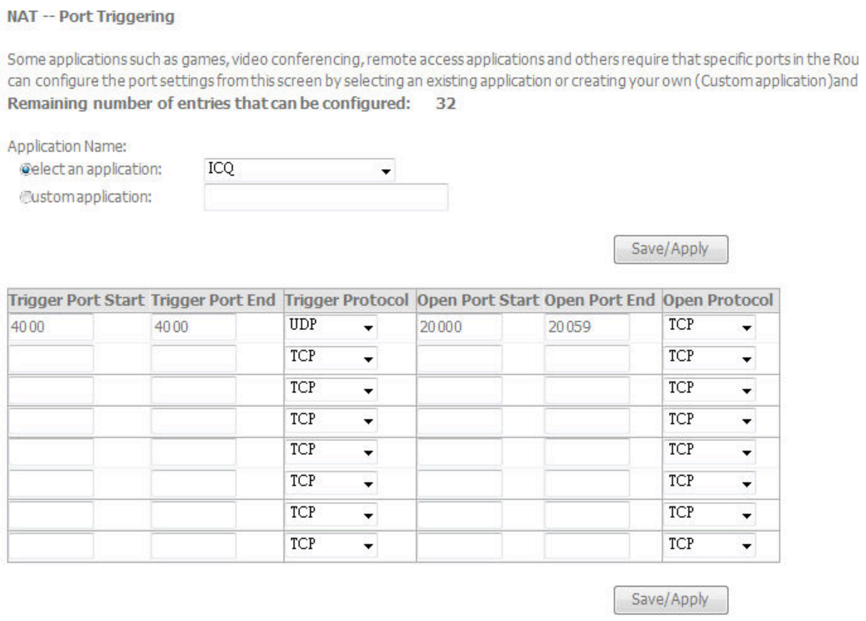
Application	Trigger			Open			Remove
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	

Figure 28: Port Triggering Setup

Click *Add* to add a rule of port triggering.

Global Setting

- Select a *service* from the predefined list or enter the name of *Custom Server*
- Enter the *Start Trigger Port #* and *End Trigger Port #* that open to remote to access the service
- Select the *Trigger Protocol*
- Enter the *Start Open Port #* and *End Open Port #* that may use different port # to secure the service. If you use the same port # as *Trigger port #*, please leave *Open Port #* as blank.
- Select the *Open Protocol*
- Click *Save/Apply*



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Rou
can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and
Remaining number of entries that can be configured: 32

Application Name:
●elect an application: ICQ
○ustom application:

Save/Apply

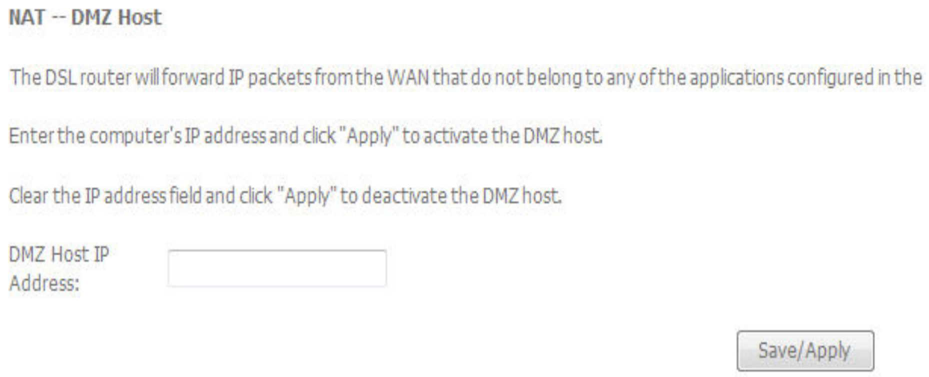
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
4000	4000	UDP	20000	20059	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

Figure 29: Add a Rule of Port Triggering

DMZ

A DMZ (DeMilitarized Zone) host is a computer on your network that can be accessed from the Internet. The de-militarised zone (DMZ) is for forwarding IP packets from the remote parties that are not fixed to any of the applications configured in the virtual server. These packets are forwarded to a designated DMZ host device. A DMZ is often used to host Web servers, FTP servers etc that need to be accessible from the Internet



NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the

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

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

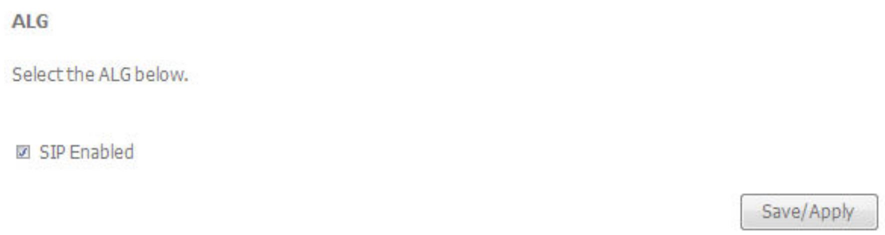
Figure 30: Add A Rule Of Port Triggering

Global Setting

- Enter the *DMZ Host IP address*
- Click *Save/Apply*

ALG

A ALG (Application Layer Gateway) is a method to allow specific application to pass through NAT firewall.



ALG

Select the ALG below.

☑ SIP Enabled

Figure 31: ALG configuration

Global Setting

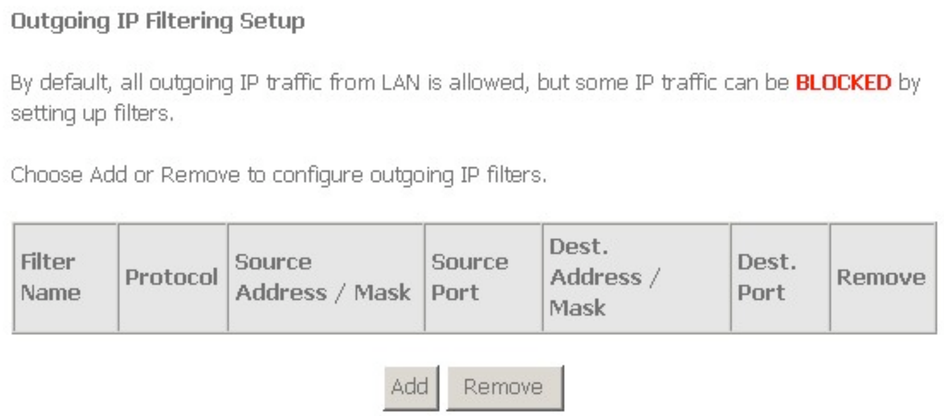
- Check to select *SIP ALG* enabled
- Click *Save/Apply*

Security

The Security feature provides two more setting pages including IP filtering in Route mode, MAC filtering and Parental Control.

IP Address Filter

The device can block the packet in outgoing and incoming directions. By default, all outgoing IP packets from LAN is allowed to surf Internet, but some IP packets can be blocked by setting up 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.

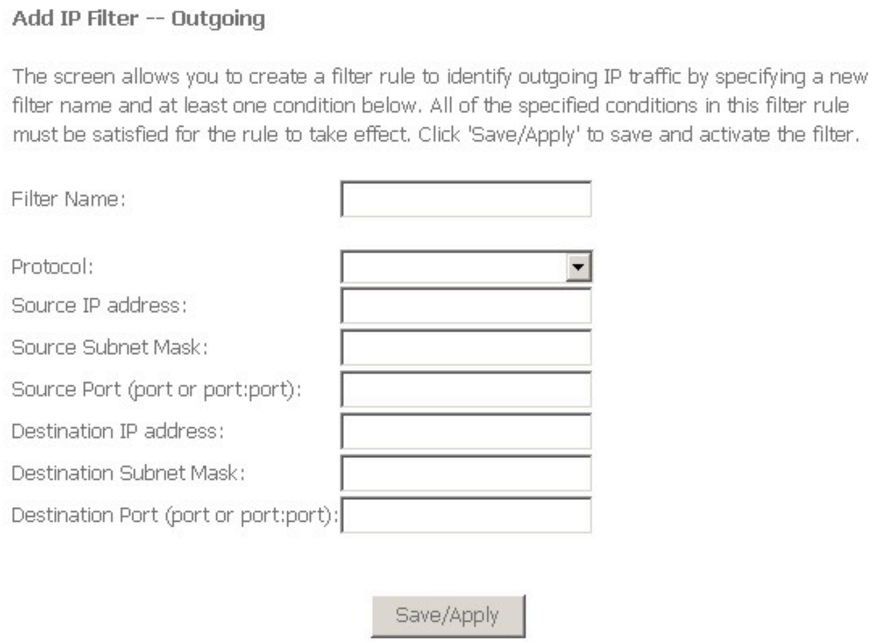
Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

Figure 32: Outgoing IP Filter Setup

Click *Add* to add a rule of Outgoing IP Filtering.

Check *Remove* and click *Remove* to remove the specified entry.



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 'Save/Apply' to save and activate the filter.

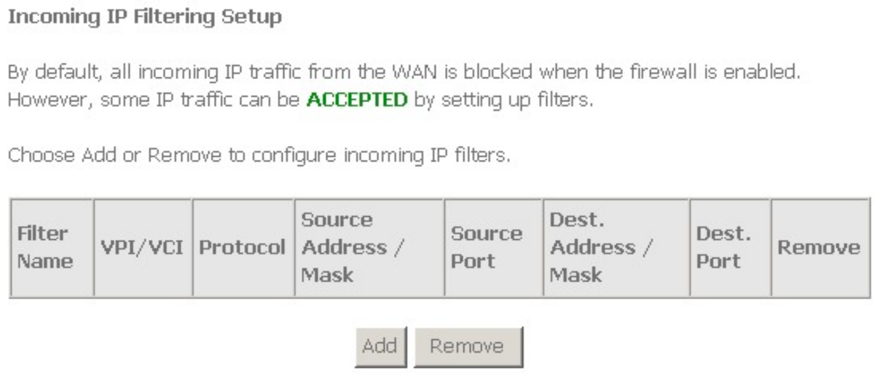
Filter Name:	
Protocol:	
Source IP address:	
Source Subnet Mask:	
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	

Figure 33: Add - Outgoing IP Filter Setup

Global Setting

- Enter the *Filter Name*
- Select the *Protocol* from the selection list.
- Enter the *Source IP Address* and *Subnet Mask (range of IP addresses)* of packet
- Enter the *one port or multi ports* (port range)
- Enter the *Destination IP Address* and *Subnet Mask (range of IP addresses)* of packet
- Enter the *one port or multi ports* (port range)
- Click *Save/Apply*

By default, all incoming IP packets from WAN are blocked to access PCs in LAN, but some IP packets can be accepted by setting up filters.



Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

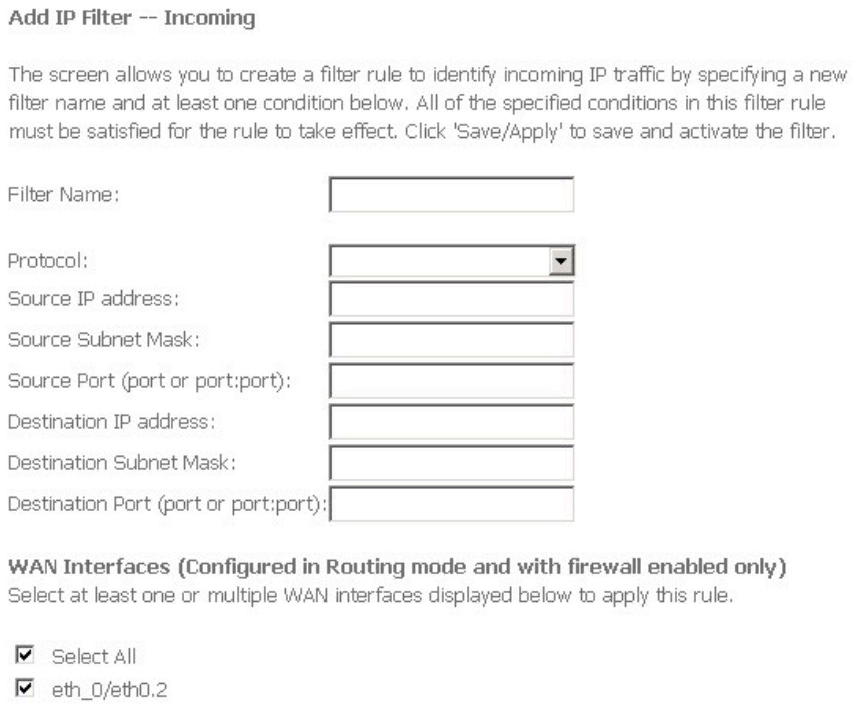
Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

Figure 34: Incoming IP Filter Setup

Click *Add* to add a rule of Incoming IP Filtering.

Check *Remove* and click *Remove* to remove the specified entry.



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 'Save/Apply' to save and activate the filter.

Filter Name:	
Protocol:	▾
Source IP address:	
Source Subnet Mask:	
Source Port (port or port:port):	
Destination IP address:	
Destination Subnet Mask:	
Destination Port (port or port:port):	

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All

☑ eth_0/eth0.2

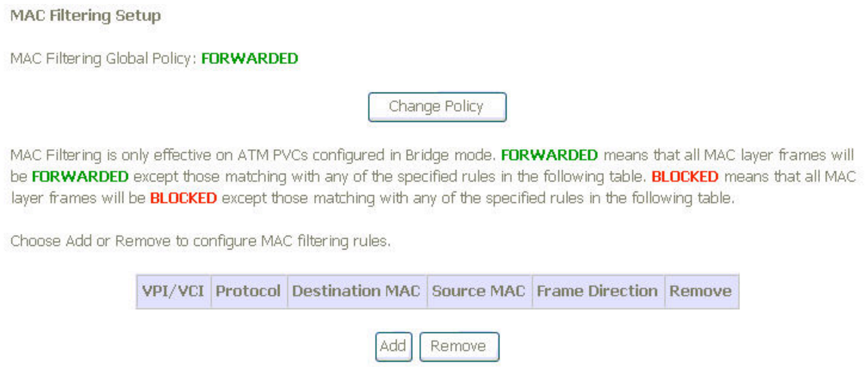
Figure 35: Add - Incoming IP Filter Setup

Global Setting

- Enter the *Filter Name*
- Select the *Protocol* from the selection list.
- Enter the *Source IP Address* and *Subnet Mask (range of IP addresses)* of packet
- Enter the *one port or multi ports* (port range)
- Enter the *Destination IP Address* and *Subnet Mask (range of IP addresses)* of packet
- Enter the *one port or multi ports* (port range)
- Select the *WAN interfaces* which will be applied with this incoming IP filter rule.
- Click *Save/Apply*

MAC Filtering

This feature allows you to configure the filter feature based on MAC address. The default MAC filtering rule is FORWARDED which means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the MAC filtering table. The default MAC filtering rule can be changed to BLOCKED. It means that all MAC layer frames will be blocked except those matching with any of the specified rule in the MAC filtering table.



MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

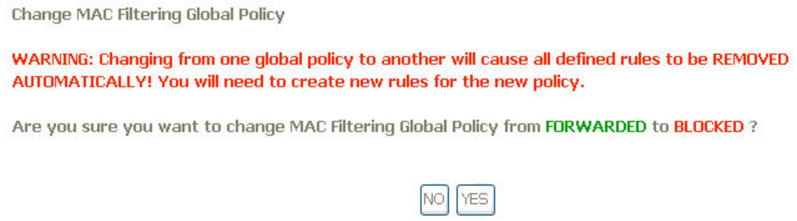
MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching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

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Figure 36: MAC Filtering Configuration

Click *Change Policy* to change the MAC filtering rule between FORWARDED and BLCOKED.



Change MAC Filtering Global Policy

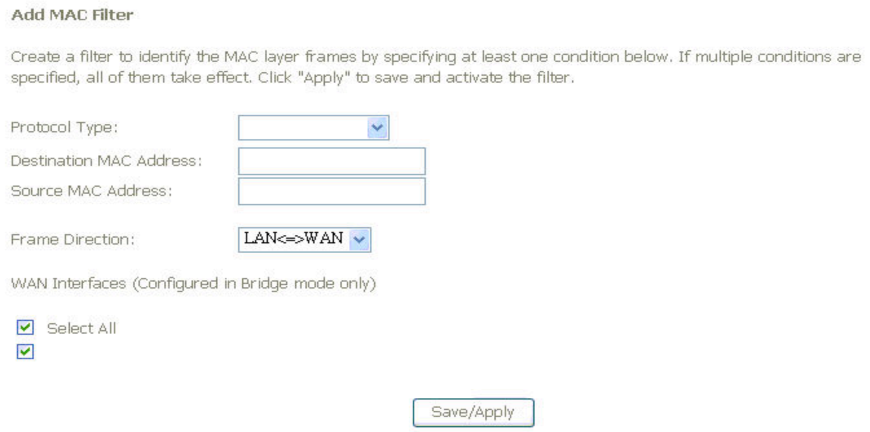
WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Are you sure you want to change MAC Filtering Global Policy from FORWARDED to BLOCKED ?

Figure 37: Change Policy Rule

Click *Add* to add a rule of MAC filtering.

Check *Remove* and click *Remove* to remove the specified entry



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: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

☑ Select All

☑

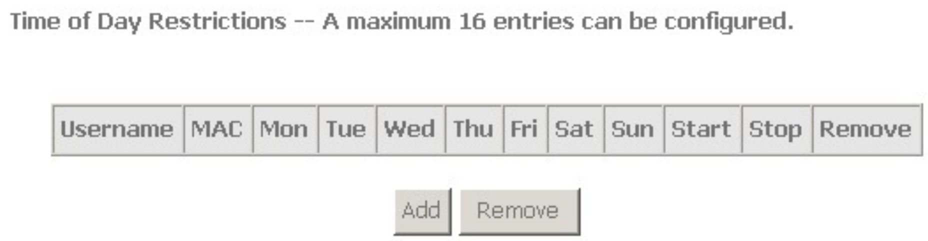
Figure 38: Add MAC Filter Rule

Global Setting

- Select the *Protocol Type* of packet from the list
- Enter the *Destination MAC Address* of packet
- Enter the *Source MAC Address* of packet
- Select the Frame Direction, both LAN to WAN and WAN to LAN, LAN to WAN (outgoing) or WAN to LAN (incoming) from the list
- Select the *WAN interfaces* which will be applied with this MAC filtering rule.
- Click Save/Apply to save the configuration

Parental Control

This feature allows you to configure some of PCs in LAN to surf Internet in specific time period.



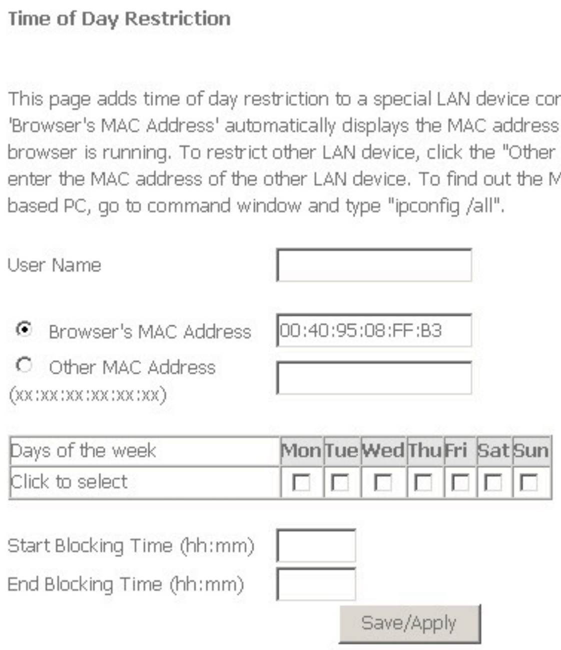
Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

Figure 39: Parental Control Configuration

Click *Add* to add a rule of schedule for parental control.

Check *Remove* and click *Remove* to remove the specified entry.



Time of Day 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 00:40:95:08:FF:B3

○ Other MAC Address (xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 40: Time of Day Restriction Configuration

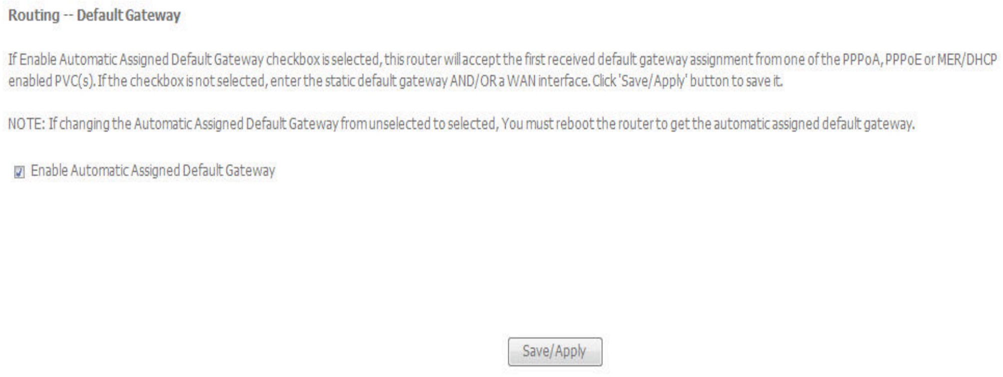
Global Setting

- Enter the *Username*
- Select the *Browser's MAC Address* or *Other MAC Address* to enter the specific PC MAC address.
- Check *those days* you want to block above PC to surf Internet.
- Enter the *Start Blocking Time* and *End Blocking Time*
- Click *Save/Apply*.

Routing

The section shows the IP addresses or address routes for the computers connected to the gateway to reach different destinations, such as the local network, the gateway, or the Internet. The Routing feature provides three more setting pages including Default Gateway, Static Route and RIP.

Default Gateway



Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☑ Enable Automatic Assigned Default Gateway

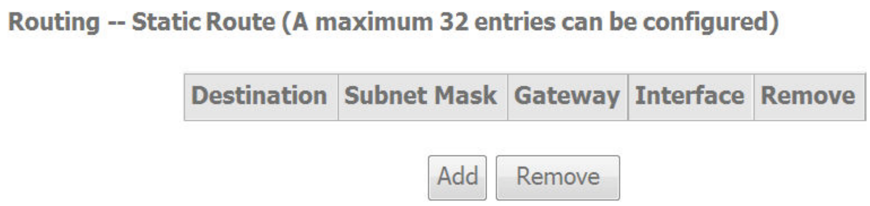
Figure 41: Default Gateway Configuration

Global Setting

- Check *Enable Automatic Assigned Default Gateway* checkbox, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or Static IP/DHCP interface. If the checkbox is not checked, enter the static default gateway AND/OR a WAN interface.
- Click *Save* to save the configuration

NOTE: If changing the Automatic Assigned Default Gateway from "unselected" to "selected", you must reboot the router to get the automatic assigned default gateway

Static Route

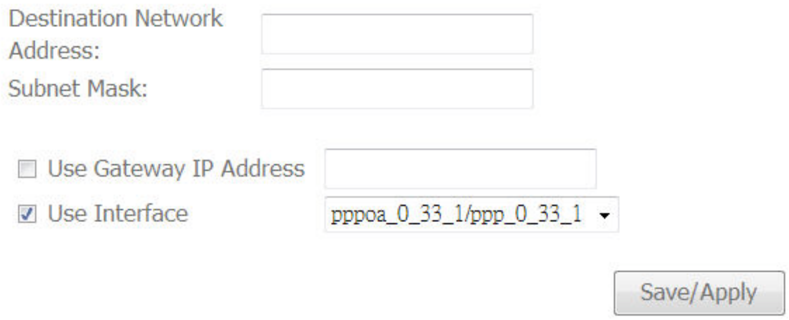


Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove

Figure 42: Static Route Configuration

Click Add to add the static route path.



Destination Network Address:	
Subnet Mask:	
☐ Use Gateway IP Address	
☑ Use Interface	pppoa_0_33_1/ppp_0_33_1

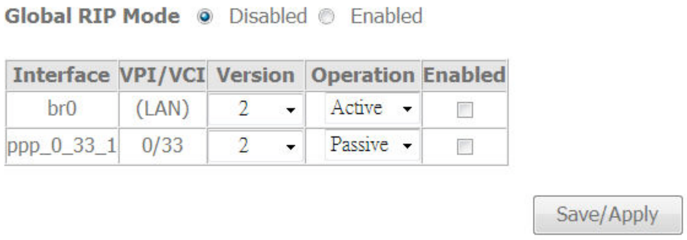
Figure 43: Add Static Route Configuration

Global Setting

- Enter the *Destination Network Address* and *Subnet Mask* (range)
- Check Use *Gateway IP Address* and enter the *IP address* where packet will be forwarded to.
- Check the *Use Interface* and select it from the list
- Click *Save* to save the configuration

RIP

To activate RIP for the device, select the 'Enable' radio button for Global RIP mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enable' checkbox for the interface.



Global RIP Mode ● Disabled ○ Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	☐
ppp_0_33_1	0/33	2	Passive	☐

Figure 44: Default Gateway Configuration

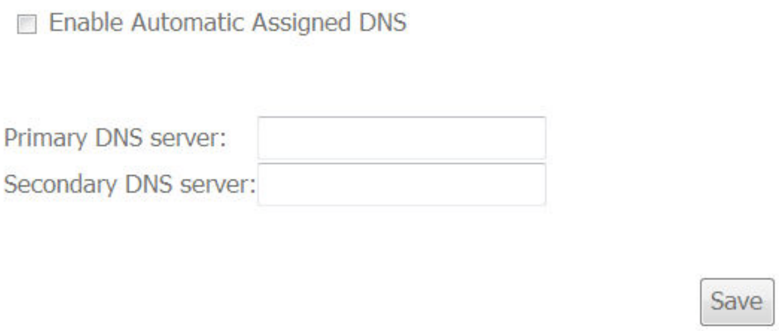
Global Setting

- Select the Enable to activate this RIP service
- Select the desired *RIP version* and *operation*, followed by placing a check in the 'Enabled' checkbox for the interface.
- Click *Save* to save the configuration

DNS

The DNS feature provides two more setting pages including DNS server setting and Dynamic DNS.

DNS Server



☐ Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

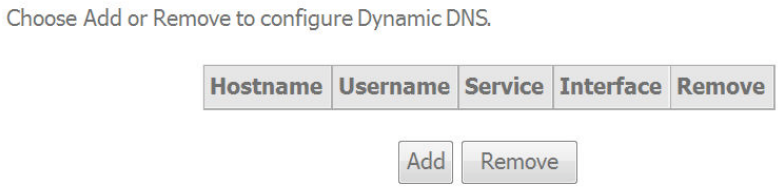
Figure 45: DNS Configuration

Global Setting

- Check *Enable Automatic Assigned DNS* checkbox, this router will accept the first received DNS assignment from one of the PPPoE or Static IP/DHCP interface. If the checkbox is not checked, enter the IP addresses of the static primary DNS server and secondary DNS server.
- Click *Save* to save the configuration

Dynamic DNS

The Dynamic DNS feature allows you to bind the dynamic assigned WAN IP address into a specified domain name. You could pass this domain name to friends to access your service in your site instead of informing them every times if WAN IP address is changed.



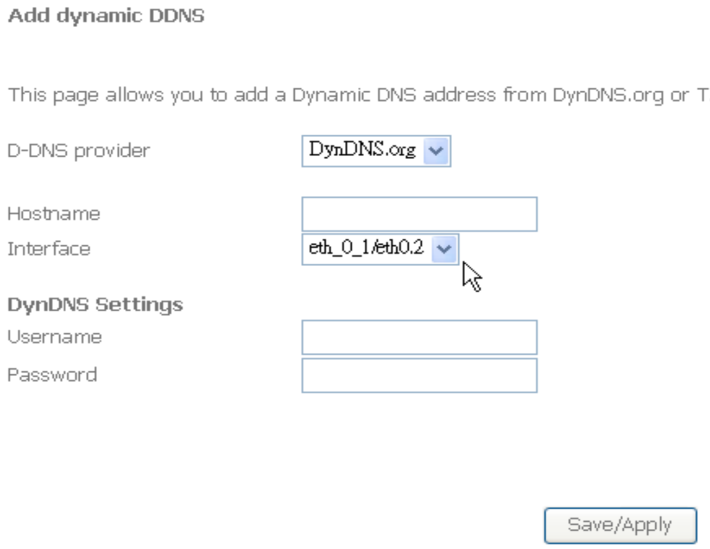
Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Figure 46: Dynamic DNS Configuration

Click *Add* to add Dynamic DNS setting.

Check *Remove* and click *Remove* to remove the specified entry.



Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Hostname:

Interface: eth_0_1/eth0.2

DynDNS Settings

Username:

Password:

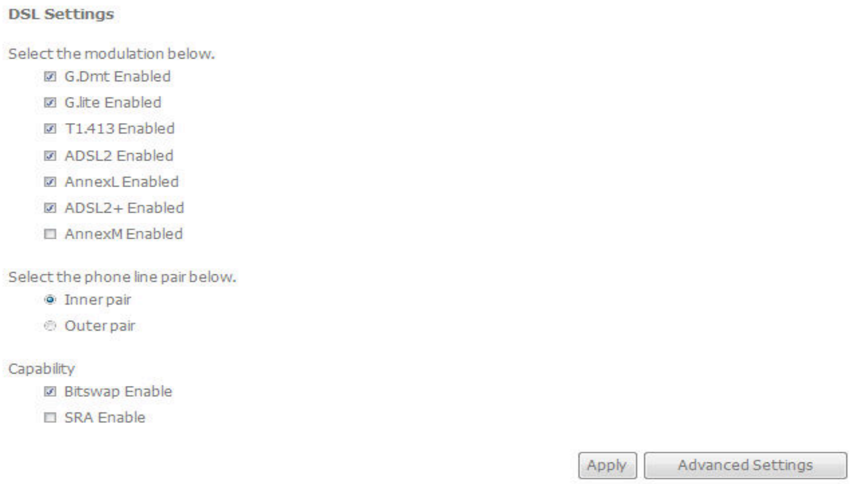
Figure 47: Add a Dynamic DNS

Global Setting

- Select the Dynamic DNS service provider from the list
- Enter the your Hostname
- Select the *Interface* from the list where the device can reach it for registration
- Enter the *Username* and *Password* for registering IP address of the device to Dynamic DNS server
- Click *Save/Apply* to save the configuration

DSL

The DSL feature provides basic and advance configuration to set the DSL parameters. Please contact technician for details before changing any parameters.



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

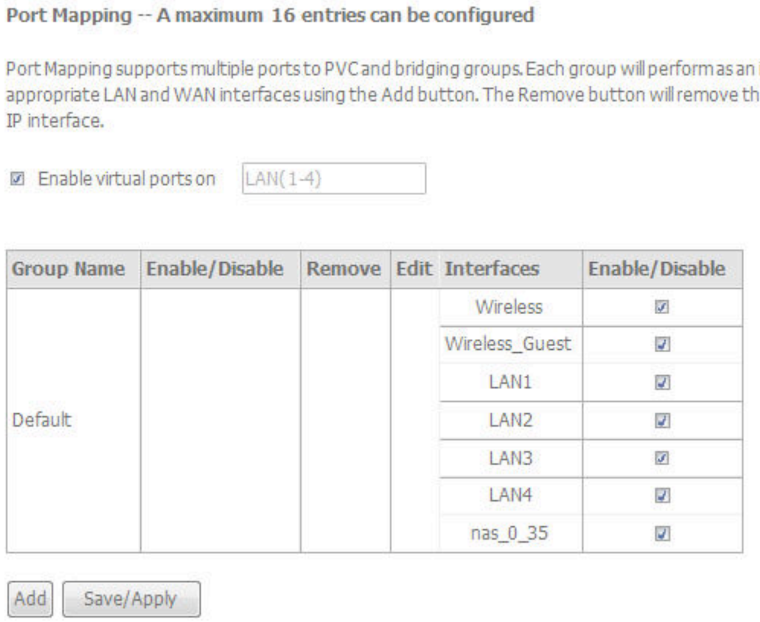
Figure 48: DSL Basic Configuration

Global Setting

- Check to select the *DSL modulation* modes.
- Select the *DSL phone line pair*, inner pair or outer pair. The inner pair is default setting.
- Check to select the *Capabilities*, Bitswap and SRA (Seamless Rate Adaption).
- Click *Apply* to save the configuration
- Click *Advanced Settings* to get details, please contact technician for support.

Port Mapping

The page provides Port Mapping configuration. In default, the LAN1 to LAN4, wireless, virtual wireless_guest and Routed PVC are grouped together as a single Ethernet environment. Port Mapping supports multiple ports to VLAN groups. Each VLAN group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces.



Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an in
appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the
IP interface.

☑ Enable virtual ports on LAN(1-4)

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				Wireless	☑
				Wireless_Guest	☑
				LAN1	☑
				LAN2	☑
				LAN3	☑
				LAN4	☑
				nas_0_35	☑

Figure 49: Port Mapping Configuration

Click *Add* to add VLAN setting.

Check *Remove* and click *Remove* to remove the specified entry.

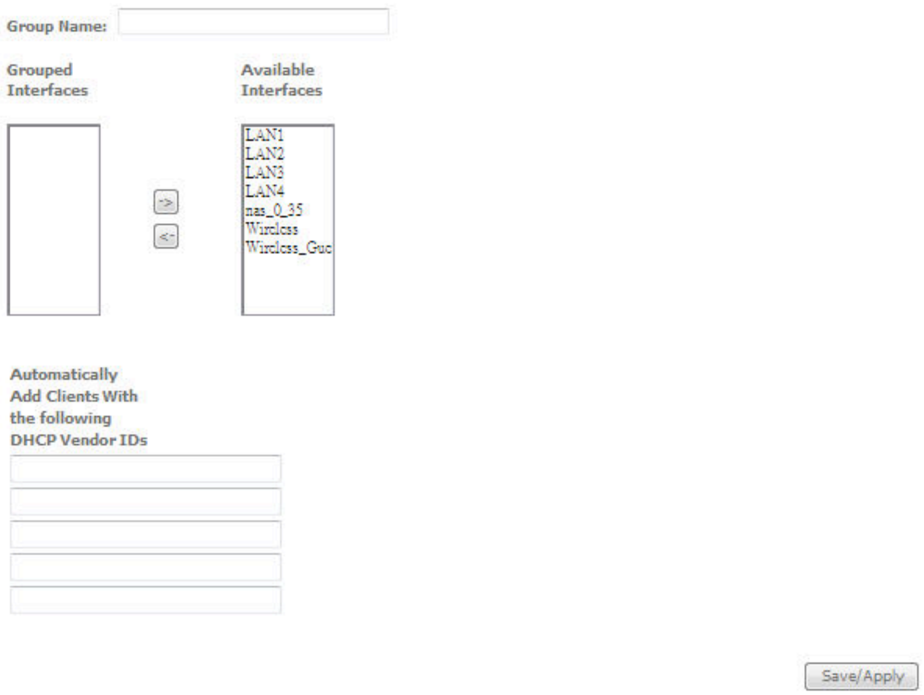


Figure 50: Add a Port Mapping Configuration

Global Setting

- Enter the *Group Name*
- Select the available *LAN ports* from available LAN interfaces into grouped interface. The selected LAN interface will be removed from its original group and joined this new group.
- If you like to add LAN clients to a PVC automatically 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.
- Click *Save/Apply* to save the configuration.

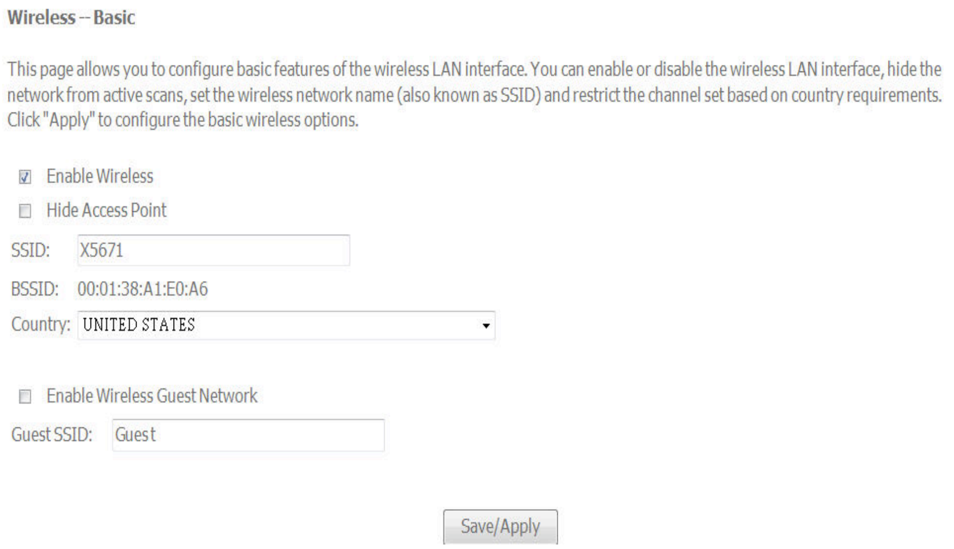
7 Wireless Setup

The Wireless Setup web page menu comprises:

Basic
Security
MAC Filter
Wireless Bridge
Advanced
Quality of Service
Station Information

Basic

The device provides wireless connection to wireless clients. This page allows you to enable the wireless service, hide the network from active scan and set the SSID (Service Set IDentifier). Besides, it allows you to create a virtual wireless AP which could use different SSID and security key.



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" to configure the basic wireless options.

☑ Enable Wireless
□ Hide Access Point
SSID: X5671
BSSID: 00:01:38:A1:E0:A6
Country: UNITED STATES

□ Enable Wireless Guest Network
Guest SSID: Guest

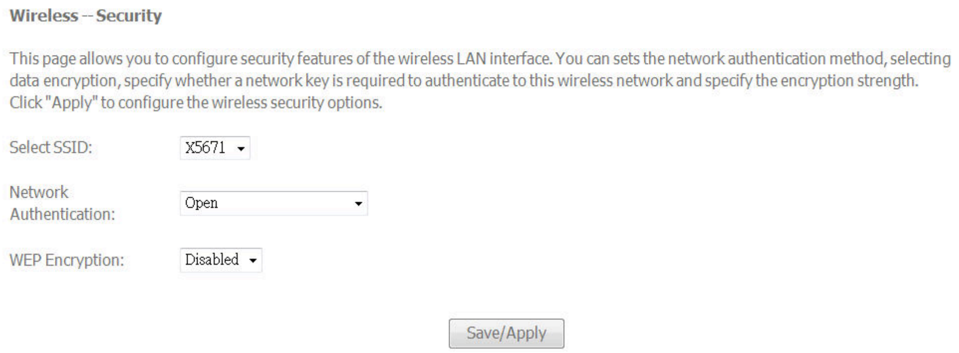
Figure 51: Wireless Setting – Basic

Global Setting

- Check to enable *Wireless feature*
- Check to enable *Hide Access Point* to hide from active scan of wireless client
- Enter the *wireless network name (SSID)*
- The *BSSID* is the MAC address of device
- Select the *Country* from the list
- Check to enable *Wireless Guest Network* to create a virtual wireless AP with different SSID and security key
- Enter the Guest SSID
- Click *Save* to save the configuration

Security

The device provides wireless connection with security including authentication method and data encryption to protect your data in the air.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You can sets 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" to configure the wireless security options.

Select SSID: X5671

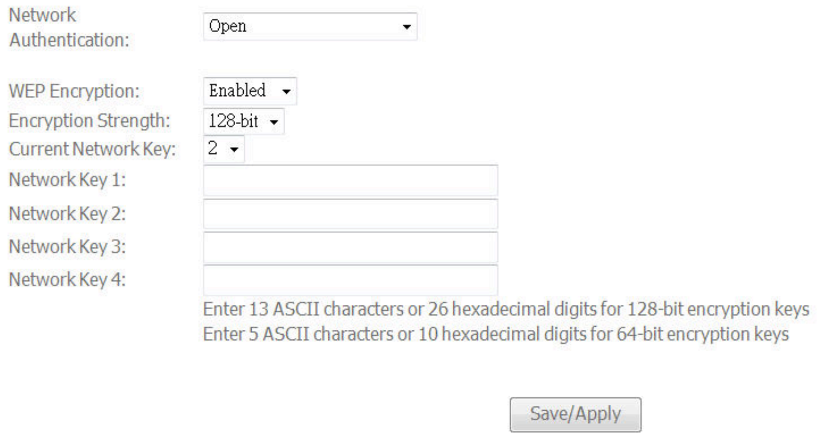
Network Authentication: Open

WEP Encryption: Disabled

Figure 52: Wireless Setting – Security

Global Setting

- Select the SSID from the list, then set the related security parameters
- Select the method of Network Authentication. It could be OPEN (none), Shared, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, Mixed WPA2/WPA-PSK
- Select the method of *WEP Encryption* if *Network Authentication* is Open. Select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary if WEP Encryption is enabled.



Network Authentication: Open

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 2

Network Key 1:

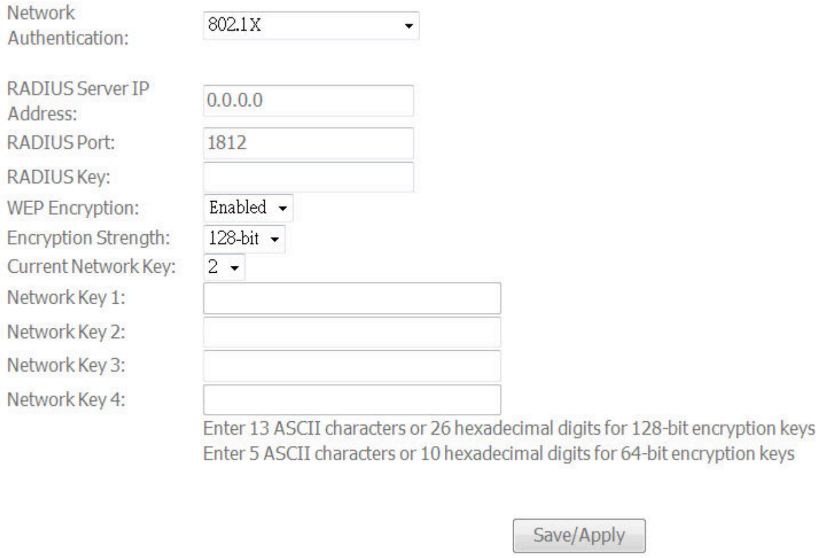
Network Key 2:

Network Key 3:

Network Key 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

- If the *Network Authentication* is Shared. Select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary as the same as *Network Authentication* is Open and *WEP Encryption* is enabled.
- If the *Network Authentication* is 802.1X, enter the *IP address* and *Port number* of Radius server, *Radius Key*, enable or disable *WEP encryption*. If *WEP Encryption* is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.



Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 2

Network Key 1:

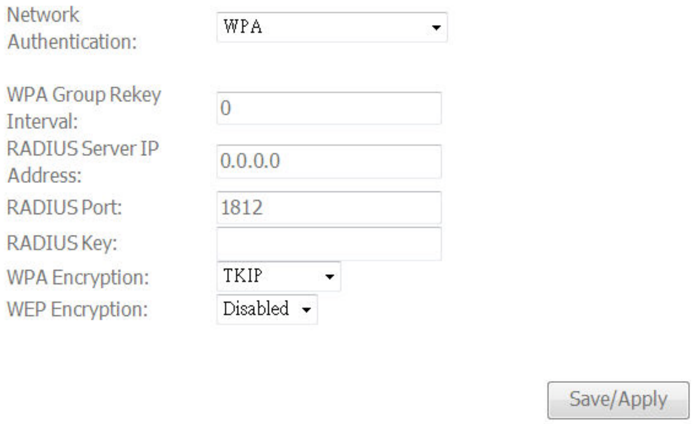
Network Key 2:

Network Key 3:

Network Key 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

- If the *Network Authentication* is WPA, enter *WPA Group Rekey Interval*, the *IP address* and *Port number* of Radius server, *Radius Key*, WPA Encryption Method (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.



Network Authentication: WPA

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

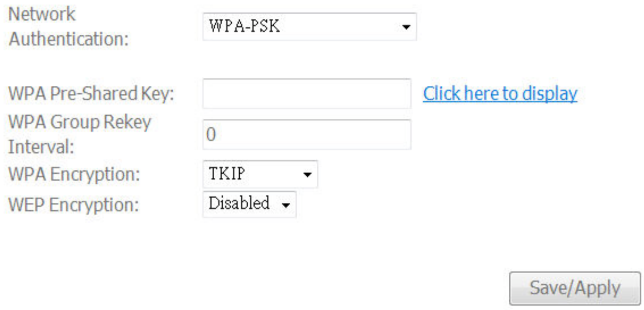
RADIUS Port: 1812

RADIUS Key:

WPA Encryption: TKIP

WEP Encryption: Disabled

- If the *Network Authentication* is WPA-PSK (pre-shared key), enter the WPA Pre-Shared Key and enter *WPA Group Rekey Interval*, *WPA Encryption Method* (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.



Network Authentication: WPA-PSK

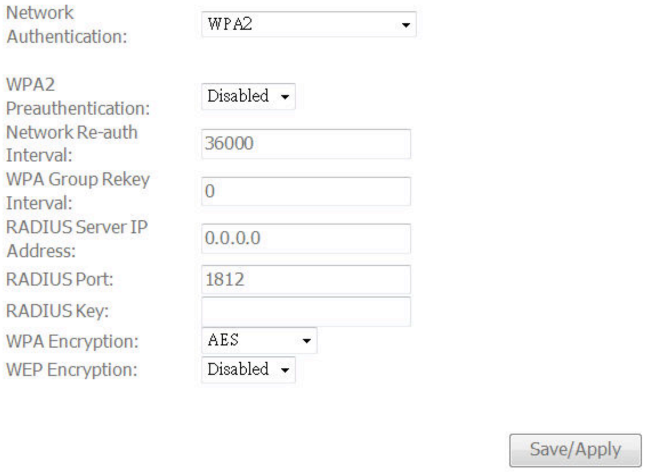
WPA Pre-Shared Key: Click here to display

WPA Group Rekey Interval: 0

WPA Encryption: TKIP

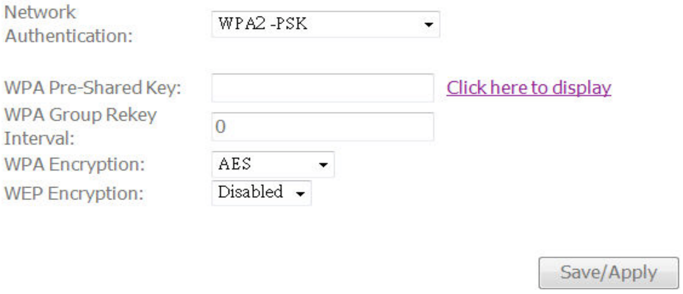
WEP Encryption: Disabled

- If the *Network Authentication* is WPA2, select Enable or Disable for *WPA2 Pre-authentication*, enter value of Network Re-Auth Interval, enter value of *WPA Group Rekey Interval*, the *IP address* and *Port number* of Radius server, *Radius Key*, WPA Encryption Method (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.



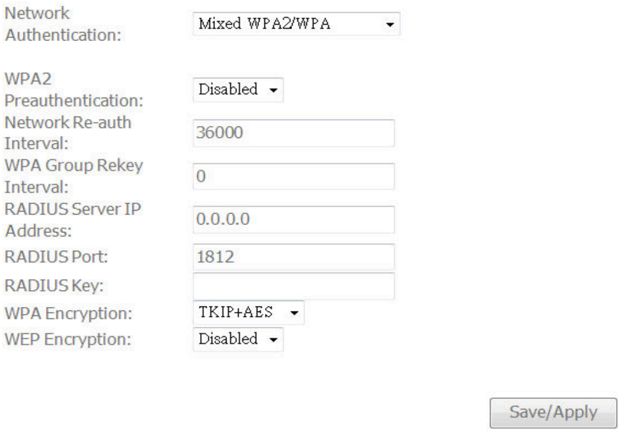
Network Authentication:	WPA2
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	AES
WEP Encryption:	Disabled

- If the *Network Authentication* is WPA2-PSK (pre-shared key), enter the WPA Pre-Shared Key and enter *WPA Group Rekey Interval*, *WPA Encryption Method* (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.



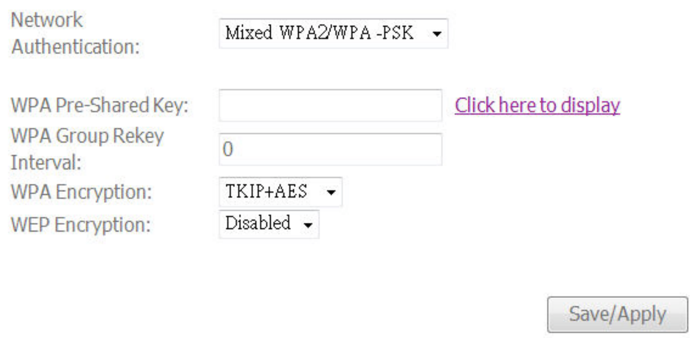
Network Authentication:	WPA2 -PSK
WPA Pre-Shared Key:	
WPA Group Rekey Interval:	0
WPA Encryption:	AES
WEP Encryption:	Disabled

- If the *Network Authentication* is mixed WPA2/WPA, select Enable or Disable for *WPA2 Pre-authentication*, enter value of Network Re-Auth Interval, enter value of *WPA Group Rekey Interval*, the *IP address* and *Port number* of Radius server, *Radius Key*, WPA Encryption Method (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary.



Network Authentication:	Mixed WPA2/WPA
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

- If the *Network Authentication* is Mixed WPA2/WPA-PSK (pre-shared key), enter the WPA Pre-Shared Key and enter *WPA Group Rekey Interval*, *WPA Encryption Method* (TKIP, AES, TKIP+AES), enable or disable *WEP encryption*. If WEP Encryption is enabled, select the *Encryption Strength* with 64bits or 128bits, select the current *Key Index* and enter the key and four keys when necessary

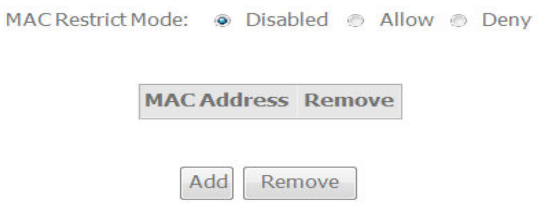


Network Authentication:	Mixed WPA2/WPA -PSK
WPA Pre-Shared Key:	Click here to display
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

- Click Save/Apply to save the configuration.

MAC Filter

With this configuration, you could allow or deny wireless to access the device by wireless MAC address filtering feature. It is disabled as default.



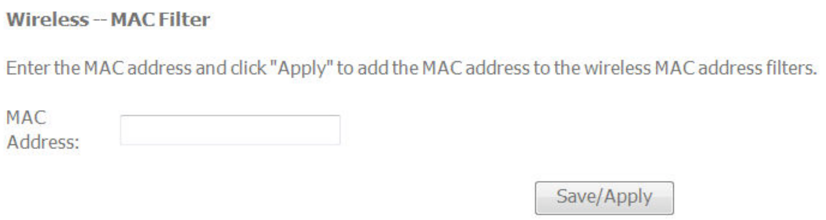
MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

Figure 53: Wireless MAC Filter Configuration

Global Setting

- Select the *MAC Restrict Mode* from one of Disable (no MAC filter), Allow (only those PCs with MAC addresses in the table can surf Internet) and Deny (only those PCs with MAC addresses in the table can not surf Internet).
- Click *Add* to add an entry or *Remove* to remove the specified entry.



Wireless -- MAC Filter

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

MAC Address:

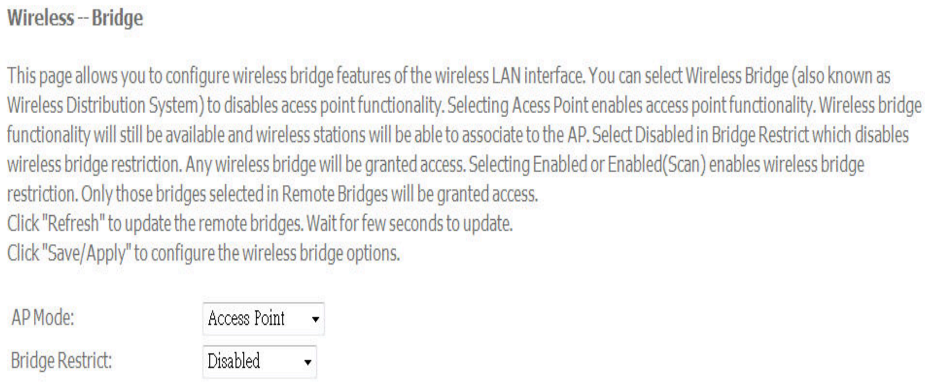
Figure 54: Add a Wireless MAC Address

Global Setting

- Enter the *MAC Address of wireless client*
- Click Save/Apply to save the configuration.

Wireless Bridge

The wireless bridge feature is also known as WDS, Wireless Distribution System).



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 disables acess point functionality. Selecting Acess 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 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.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.

AP Mode:	Access Point
Bridge Restrict:	Disabled

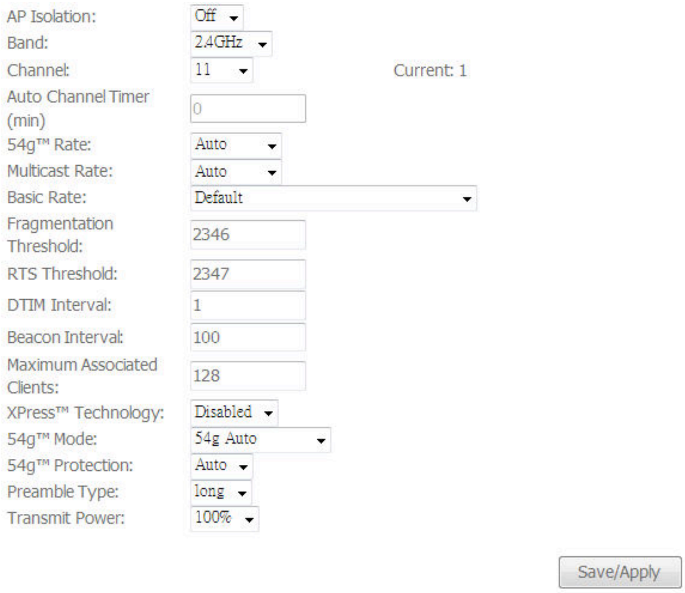
Figure 55: Wireless Bridge Configuration

Global Setting

- Set the *AP mode* as Access Point or Wireless Bridge
- When the *AP mode* is set to Wireless Bridge, the *Wireless Restrict* determine where it can communicate with all other wireless bridges and also wireless clients (set *Bridge Restrict* is Disabled) or just the specified MAC addresses of below wireless bridge devices (set *Bridge Restrict* is Enable).
- Click Reflash to get the updated information
- Click *Save/Apply* to save the configuration

Advanced

This page allows you to configure advanced parameters for wireless communication.



AP Isolation:	Off	
Band:	2.4GHz	
Channel:	11	Current: 1
Auto Channel Timer (min)	0	
54g™ Rate:	Auto	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Maximum Associated Clients:	128	
XPress™ Technology:	Disabled	
54g™ Mode:	54g Auto	
54g™ Protection:	Auto	
Preamble Type:	long	
Transmit Power:	100%	

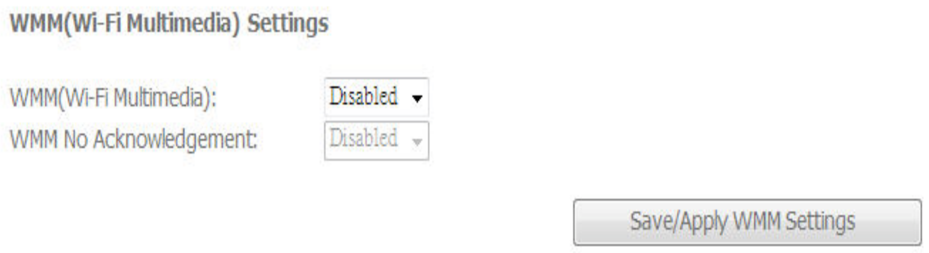
Figure 56: Wireless Setting – Advanced

Global Setting

- Enable *AP Isolation* if you do not want AP to be able to communicate with each other.
- Set the W*ireless Communication Band*. If you do not know it, please it as default.
- Select the *channel* from the list
- Enter the value of *Auto Channel Timer*
- Set the *54g Rate* (Wireless Communication Rate), AUTO means to use the highest rate if possible)
- Set the *Rate for Multicast Packets*, AUTO means to use the highest if possible.
- Set the *Basic Rate*
- Set the *Fragmentation Threshold* values from 256 to 2364 bytes. If the value is too small, it may cause a result in poor performance.
- Set the *RTS (Ready to Send) Threshold*
- Set *DTIM Interval.* DTIM stands for Delivery Traffic Indication Message. This is a beacon and is a countdown informing wireless clients of the next window for listening to broadcast and multicast messages. It is a wake-up interval for clients in power-saving mode.
- Set *Beacon Interval*. The interval in milliseconds between beacon transmissions.
- Set the *Maximum Associated Wireless Client*
- Set *XPress Technology* enabled or disabled.
- Set *54g Mode* to 54g Auto, 54g Performance, 802.11b, 54g LRS (limited rate support).
- Set *54g Protection* to AUTO if there are 802.11g and 802.11b coexisting in the wireless network.
- Set *Afterburner Technology*
- Set *Preamble Type*. A preamble is a signal that sync up the timing between devices.
- Set *Transmission Power*. Larger value means more coverage.

Quality of Service

The device provides wireless quality of service, Wi-Fi Multimedia.



WMM(Wi-Fi Multimedia) Settings

WMM(Wi-Fi Multimedia): Disabled

WMM No Acknowledgement: Disabled

Figure 57: Wireless Setting – Quality of Service

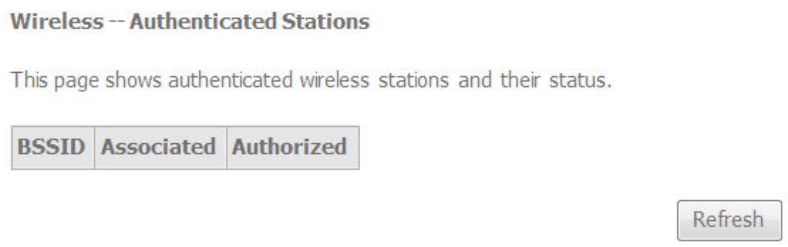
Global Setting

- Select to enable or disable *WMM (Wi-Fi Multimedia)*
- Select to enable or disable *WMM No Acknowledgement*. Enabling no-acknowledge can result in more efficient throughput but high error rates

- Click *Save/Apply* to save the configuration

Station Information

The table shows up whole associated wireless clients the device and their status.



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

BSSID	Associated	Authorized

Figure 58: Wireless Setting – Station Information

Global Setting

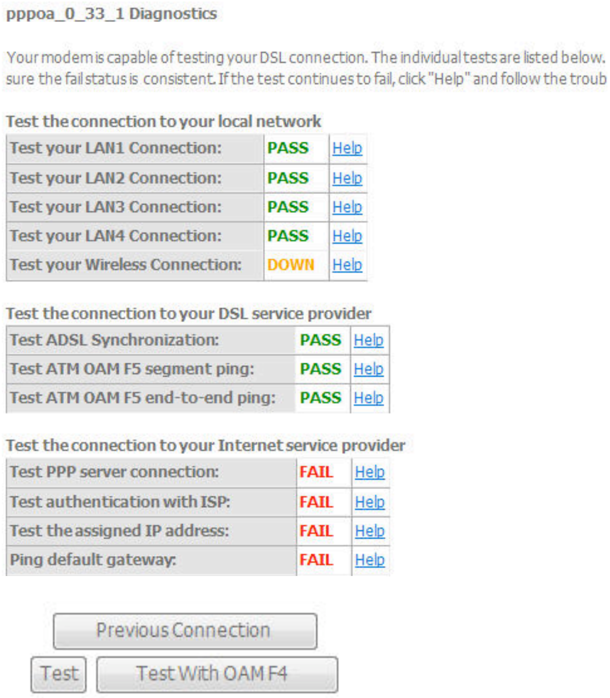
- Click Refresh to get the latest updated information

8 Diagnostic

The Diagnostic web page provides the connection check in physical layer and upper layer. The result is helpful to figure out the problem if you have problem to surf Internet.

Diagnostic

This page will show up the result of diagnostic in physical layer like WAN port and also upper layer of PPP if ISP provides the PPP access protocol.



pppoa_0_33_1 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below.
sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troub

Test the connection to your local network

Test your LAN1 Connection:	PASS	Help
Test your LAN2 Connection:	PASS	Help
Test your LAN3 Connection:	PASS	Help
Test your LAN4 Connection:	PASS	Help
Test your Wireless Connection:	DOWN	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	PASS	Help
Test ATM OAM F5 segment ping:	PASS	Help
Test ATM OAM F5 end-to-end ping:	PASS	Help

Test the connection to your Internet service provider

Test PPP server connection:	FAIL	Help
Test authentication with ISP:	FAIL	Help
Test the assigned IP address:	FAIL	Help
Ping default gateway:	FAIL	Help

Figure 59: Diagnostic Result

Global Setting:

- Click the *Connection* to test another connection.
- Click the *Test* to test it again
- Click *Test with OAM F4* to verify the DSL link.

9 Management

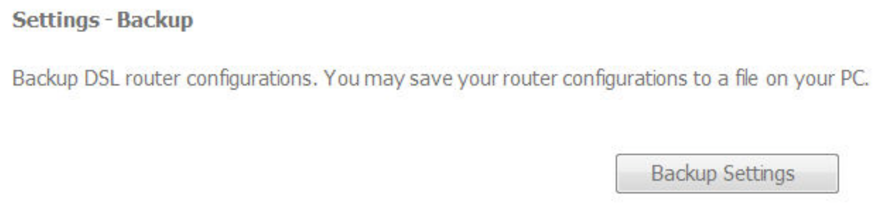
The Management web page menu comprises:

Settings
System Log
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot

Settings

This page allows you to backup the current configuration of the device, update the configuration, and restore default configuration (factory setting).

Backup



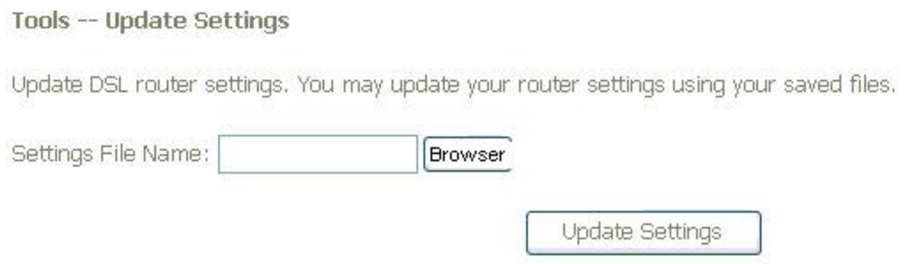
Settings - Backup

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

Figure 60: Backup Settings

Click Backup Settings to backup the current settings of the device into file in PC.

Update



Tools -- Update Settings

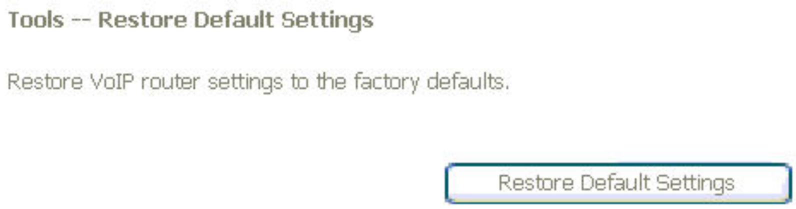
Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

Figure 61: Restore Default Settings

Click *Browser* to specify the configuration file (settings) in PC and click *Update Settings* to upload the settings to the device.

Restore Default



Tools -- Restore Default Settings

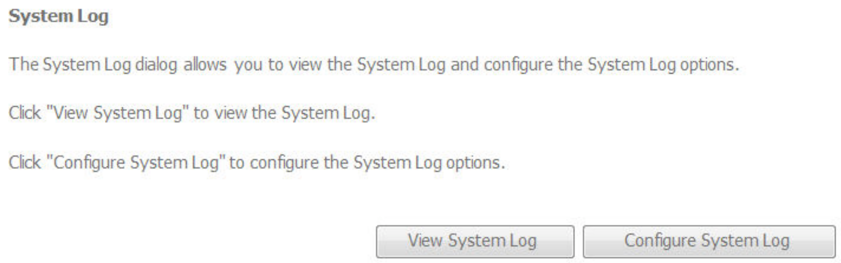
Restore VoIP router settings to the factory defaults.

Figure 62: Restore Default Settings

Click Restore Default Settings to restore the factory default settings.

System Log

This page allows you to view system log and also configure system log that way you want to see.



System Log

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

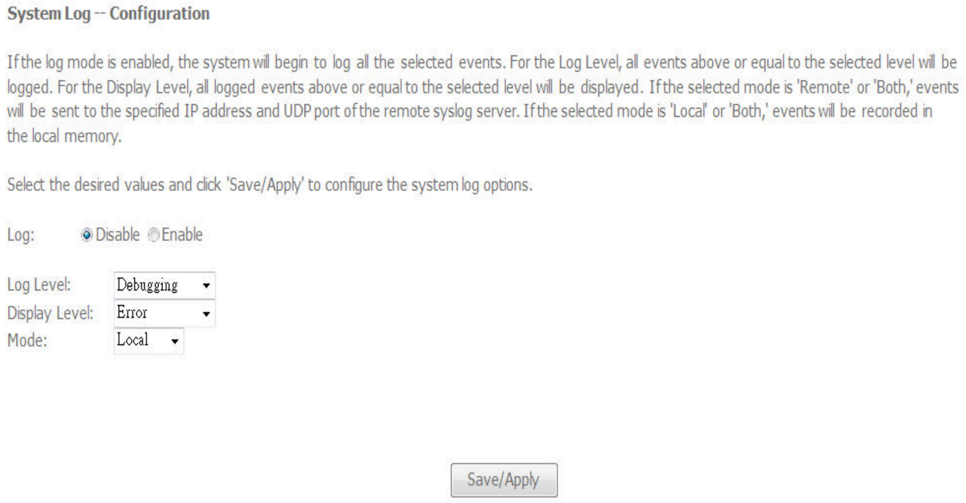
Click "View System Log" to view the System Log.

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

Figure 63: Management Configuration – System Log

Global Setting

- Click *View System Log* to view system log
- Click *Configure System Log* to configure the way you want to see



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 'Save/Apply' to configure the system log options.

Log: ● Disable ○ Enable

Log Level: Debugging

Display Level: Error

Mode: Local

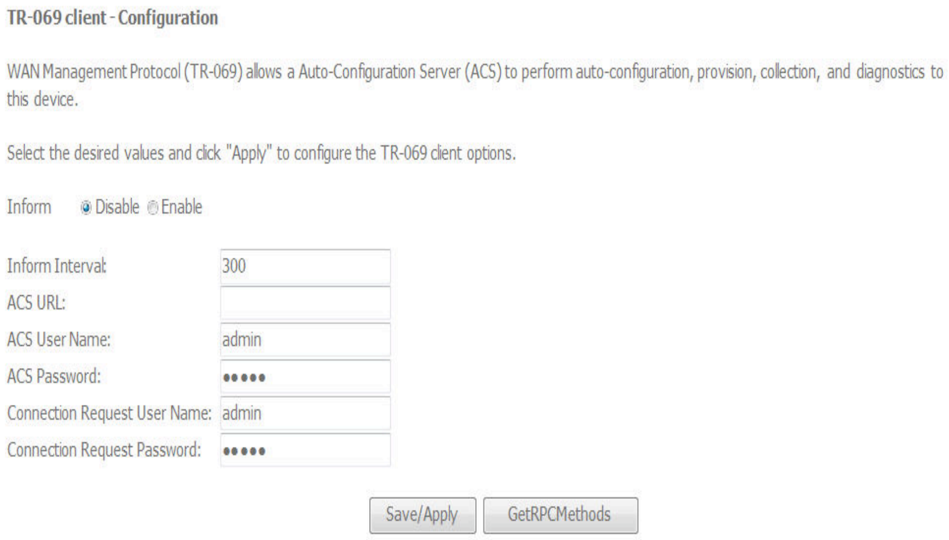
Figure 64: Management Configuration – Configure System Log

Global Setting

- Select to *Enable Log* function or not
- Select *Log Level* from the list
- Select *Display Level* from the list
- Select *Mode* from the list
- Click *Save/Apply* to save the configuration.

TR-069 Client

This page allows you to access TR-069 ACS (Auto-Configuration Server). The ACS can provision, configure, and diagnostic the device from remote site.



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" to configure the TR-069 client options.

Inform ● Disable ○ Enable

Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	•••••
Connection Request User Name:	admin
Connection Request Password:	•••••

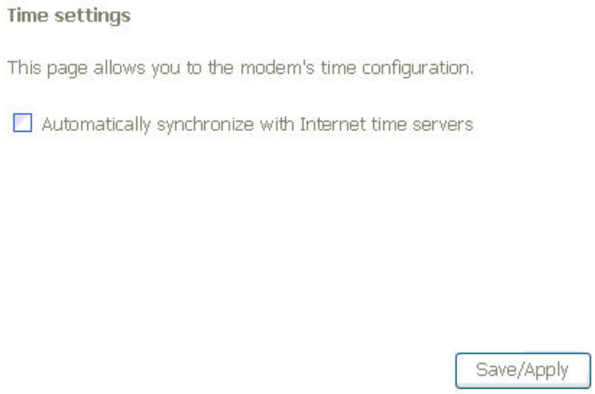
Figure 65: Management Configuration – Firmware Upgrade

Global Setting

- Select to *Enable* or *Disable* to send *Inform* packet to ACS.
- Enter the *Inform Interval* number of seconds. The Inform packet will be sent to ACS periodically.
- Enter the *ACS URL* to reach ACS
- Enter the *ACS User Name* and *Password*
- Enter the *Connection Request User Name* and *Password*
- Click *Save/Apply* to save the configuration

Internet Time

This page allows you to sync up the real time clock from Internet. .



Time settings

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

☐ Automatically synchronize with Internet time servers

Figure 66: Internet Time Configuration

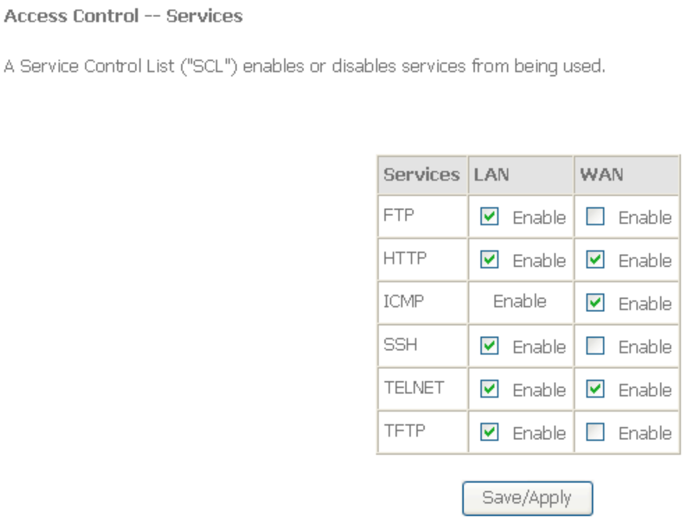
Global Setting

- Check to *Automatically synchronize with Internet time servers*
- Click *Save* to save your settings

Access Control

This submenu provides you local (LAN) or remote (WAN) access to the device. This may help the IT support staff to configure the router locally or remotely.

Service



Access Control -- Services

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

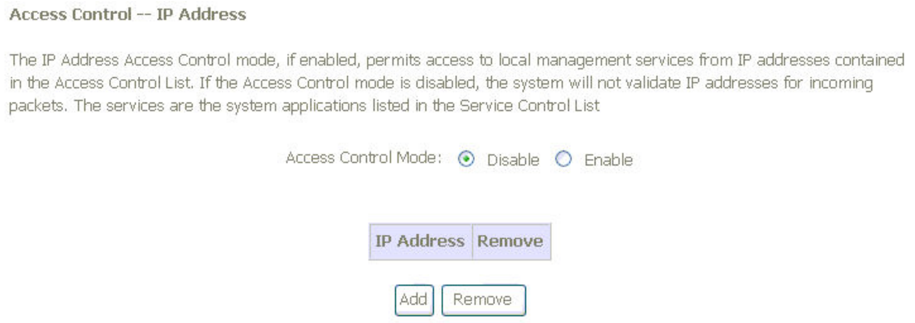
Services	LAN	WAN
FTP	☑ Enable	☐ Enable
HTTP	☑ Enable	☑ Enable
ICMP	Enable	☑ Enable
SSH	☑ Enable	☐ Enable
TELNET	☑ Enable	☑ Enable
TFTP	☑ Enable	☐ Enable

Figure 67: Management Configuration – Access Control: Service

Global Setting:

- Specify the method by which you wish to access the router locally or remotely by selecting it. The following are the methods available for local and remote access:
    - FTP
    - HTTP
    - ICMP (Ping)
    - SSH
    - TELNET
    - TFTP
- Click *Save/Apply* to save the configuration.

IP Address



Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: ● Disable ○ Enable

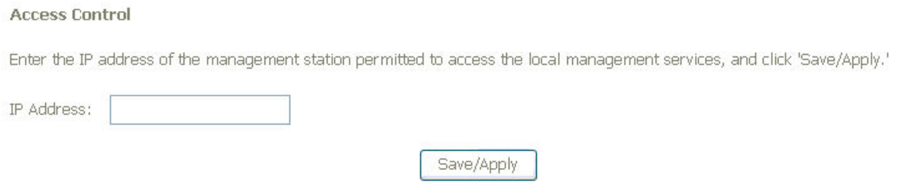
IP Address	Remove

Figure 68: Management Configuration – Access Control: IP Address

Click to enable or disable Access Control by IP address.

Click *Add* to add IP address.

Check *Remove* and click *Remove* to remove the specified entry.



Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

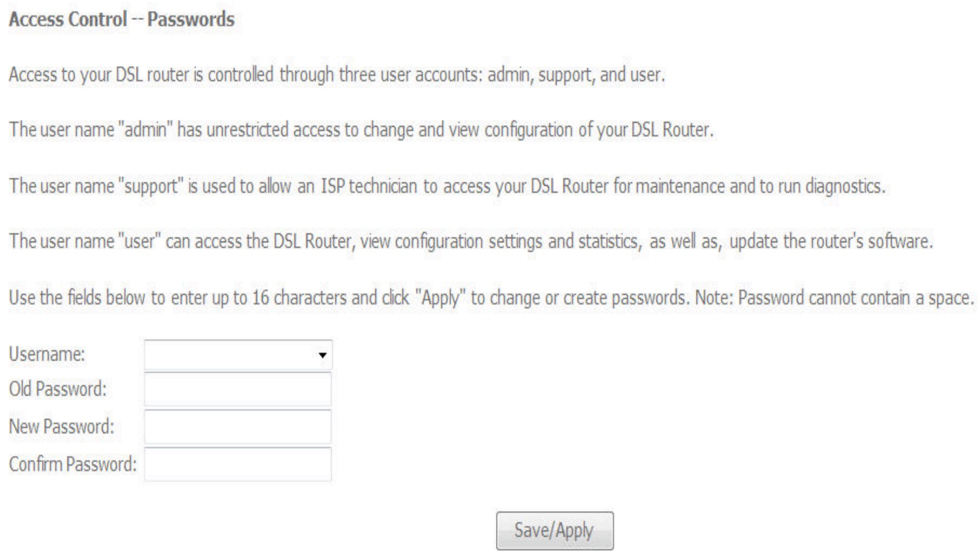
Figure 69: Management Configuration – Access Control: Add IP Address

Global Setting:

- Add the IP Address which is permitted to access the device and execute the management service.
- Click Save/Apply to save the settings.

Password

There are three levels of access accounts: admin, support, and user. The user name “admin” has unrestricted access to change and view configuration of the device. The user name “support” is used to allow an ISP technician to access the device for maintenance and to run diagnostics. The user name “user” can access the device, view configuration settigns and statistics, as well as updaet the device software.



Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

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

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:	
Old Password:	
New Password:	
Confirm Password:	

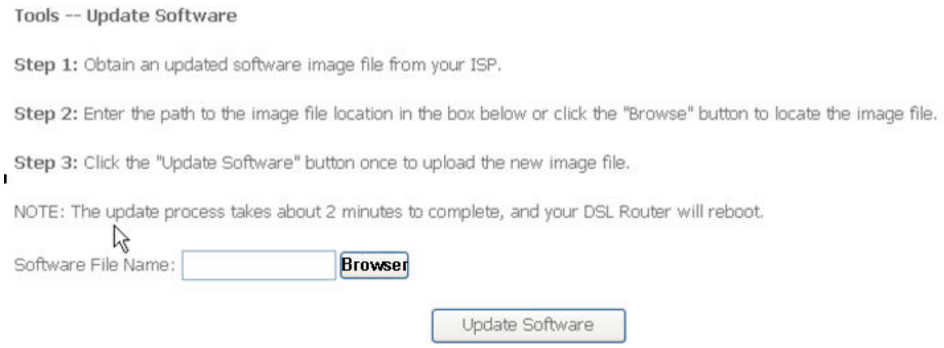
Figure 70: Management Configuration – Access Control: Password

Global Setting:

- Select the level of *Username*
- Enter the *Old Password*
- Enter the *New Password* and *Confirm Password*
- Click *Save/Apply* to save the configuration.

Update Software

This page allows you to upgrade the software (firmware).



Tools -- Update Software

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 DSL Router will reboot.

Software File Name:

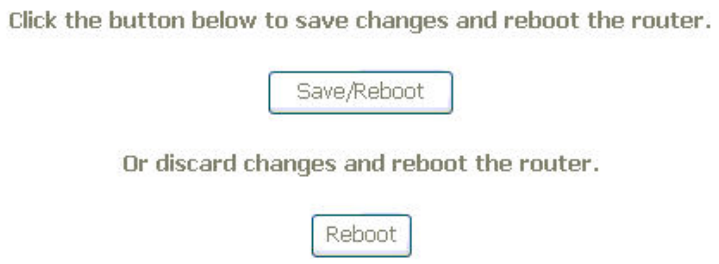
Figure 71: Management Configuration – Update Software

Global Setting:

- First of all, you have to get the updated software (firmware) from ISP or manufacture.
- Click *Browser* to specify the location and filename
- Click *Update Software* to start the process. It could take minutes to complete it.

Save / Reboot

This page allows you to save current configuration and reboot to use the settings.



Click the button below to save changes and reboot the router.

Or discard changes and reboot the router.

Figure 72: Management Configuration – Save/Reboot (no picture)

Global Setting

- Click *Save/Reboot to* save the changes and reboot the device.
- Click Reboot to discard changes and reboot the device only

Appendix A - Configuring the Internet Settings

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

Configuring Ethernet PCs

Before you begin

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

Note

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

Assigning static Internet information to your PCs section.

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

Windows® XP PCs

In the Windows task bar, click the *Start* button, and then click *Control Panel*.

Double-click the Network Connections icon.

In the *LAN or High-Speed Internet* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. (Often, this icon is labelled *Local Area Connection*).The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Ensure that the check box to the left of the item labelled *Internet Protocol TCP/IP* is checked and click *Properties*.

In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labelled Obtain an IP address automatically. Also click the radio button labelled Obtain DNS server address automatically.

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

Windows 2000 PCs

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

In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

Double-click the Network and Dial-up Connections icon.

In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*. The *Local Area Connection Properties* dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.

If Internet Protocol (TCP/IP) does not display as an installed component, click *Install.*

In the *Select Network Component* Type dialog box, select *Protocol*, and then click *Add.*

Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.

If prompted, click *OK* to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.

In the *Control Panel*, double-click the Network and Dial-up Connections icon.

In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.

In the Local Area Connection Properties dialog box, select *Internet Protocol (TCP/IP),* and then click *Properties*.

In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labelled Obtain an IP address automatically. Also click the radio button labelled Obtain DNS server address automatically.

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

Windows Me PCs

In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

Double-click the Network and Dial-up Connections icon.

In the Network and Dial-up Connections window, right-click the Network icon, and then select Properties. The Network Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.

If Internet Protocol (TCP/IP) does not display as an installed component, click Add.

In the Select Network Component Type dialog box, select Protocol, and then click Add.

Select Microsoft in the Manufacturers box.

Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click OK. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.

If prompted, click OK to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.

In the Control Panel, double-click the Network and Dial-up Connections icon.

In Network and Dial-up Connections window, right-click the Network icon, and then select Properties.

In the Network Properties dialog box, select TCP/IP, and then click Properties.

In the TCP/IP Settings dialog box, click the radio button labelled Server assigned IP address. Also click the radio button labelled Server assigned name server address.

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

Windows 95, 98 PCs

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

In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

Double-click the Network icon. The *Network* dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.

If TCP/IP does not display as an installed component, click *Add.* The Select Network Component Type dialog box displays.

Select *Protocol*, and then click *Add…*The Select Network Protocol dialog box displays.

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

Click *OK* to return to the Network dialog box, and then click *OK* again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

Click *OK* to restart the PC and complete the TCP/IP installation. Next, configure the PCs to accept IP information assigned by the device.

Open the Control Panel window, and then click the Network icon.

Select the network component labelled TCP/IP, and then click *Properties*. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

In the TCP/IP Properties dialog box, click the IP Address tab.

Click the radio button labelled Obtain an IP address automatically.

Click the DNS Configuration tab, and then click the radio button labelled *Obtain an IP address automatically*.

Click *OK* twice to confirm and save your changes. You will be prompted to restart Windows.

Click *Yes*.

Windows NT 4.0 workstations

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

In the Windows NT task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

In the Control Panel window, double click the Network icon.

In the *Network dialog* box, click the *Protocols* tab. The *Protocols* tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.

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

In the *Select Network Protocol* dialog box, select *TCP/IP*, and then click *OK*. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

Click *Yes* to continue, and then click *OK* if prompted to restart your computer. Next, configure the PCs to accept IP information assigned by the device.

Open the Control Panel window, and then double-click the Network icon.

In the *Network* dialog box, click the *Protocols* tab.

In the *Protocols* tab, select *TCP/IP*, and then click *Properties*.

In the Microsoft TCP/IP Properties dialog box, click the radio button labelled Obtain an IP address from a DHCP server.

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

Assigning static Internet information to your PCs

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

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

You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).

You maintain different subnets on your LAN (subnets are described in Appendix B).

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

The IP address and subnet mask of each PC

The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the device. By default, the LAN port is assigned the IP address 192.168.1.1. (You can change this number or another number can be assigned by your ISP.)

The IP address of your ISP's Domain Name System (DNS) server.

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

Note

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

Configuring Wireless PCs

You need to configure the operating system installed on your Wireless PCs using the same procedure described for Configuring Ethernet PCs section.

Positioning the wireless PCs

The wireless network cards used determine the maximum distance between your wireless PCs and your device. Guidelines on positioning the hardware components of your wireless network should be provided by your network card provider.

Wireless PC cards and drivers

Each PC on your wireless LAN must be fitted with a wireless access card. You must also install the corresponding driver files for your particular wireless card on your PC. You should receive driver files and instructions on how to install them together with your wireless card.

Configuring PC access to your Wireless device

Before you start configuring your Wireless PC, you must ensure that you have:

A Wireless access card for each of the PCs

Corresponding wireless access card driver software files

The configuration steps below will vary depending on both the operating system and wireless card installed on the PC. These steps provide a basic outline, however you should refer to the documentation provided with your wireless access card for specific instructions.

To configure Wireless PCs:

Install the wireless access card.

Install the wireless driver software files.

Configure the following wireless parameters on each of the wireless PCs:

- Set the adapter to use infrastructure mode. This configures the PCs to access each other and the Internet via the device.

Configure the SSID and channel to match the SSID and channel previously configured on the device.

Your wireless network can now communicate with the Internet via the device.

Appendix B - Troubleshooting

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

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

Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
LEDs	
Power LED does not illuminate after product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connected to the device and a wall socket/power strip.
LINK LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the device. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
Internet Access	
My PC cannot access the Internet	Run a health check on your device. Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: ● Check that the gateway IP address on the computer is your public IP address (see Current Status on page 1 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. ● Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
My LAN PCs cannot display web pages on the Internet.	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the device is correct, and then you can use the ping utility, discussed on page 61, to test connectivity with your ISP's DNS server.
Web pages	

Problem	Troubleshooting Suggestion
I forgot/lost my user ID or password.	If you have not changed the password from the default, try using "admin" as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing three times the Reset Default button on the front panel of the device. Then, type the default User ID and password shown above. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
I cannot access the web pages from my browser.	Use the ping utility, discussed in the following section, to check whether the PC can communicate with the device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the device**.**
My changes to the web pages are not being retained.	Be sure to use the *Confirm Changes* function after any changes.

Diagnosing Problem using IP Utilities

Ping

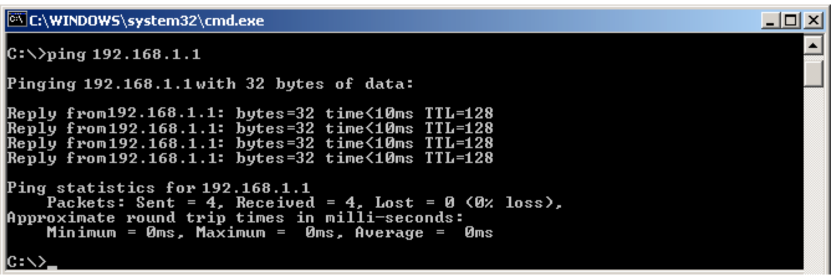
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer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

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

ping 192.168.1.1

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

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



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from192.168.1.1: bytes=32 time<10ms TTL=128
Reply from192.168.1.1: bytes=32 time<10ms TTL=128
Reply from192.168.1.1: bytes=32 time<10ms TTL=128
Reply from192.168.1.1: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.1
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

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

Using the ping command, you can test whether the path to the device is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

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

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

Nslookup

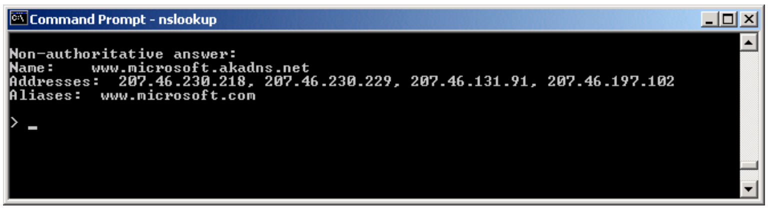
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then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

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

Nslookup

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

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



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

> _
```

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

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

Appendix C – Glossary

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

	types of data. See routing.
Broadband	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
Broadcast	To send data to all computers on a network.
DHCP	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP relay	Dynamic Host Configuration Protocol relay A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. See DHCP.
DHCP server	Dynamic Host Configuration Protocol server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.
Digital	Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See analog.
DNS	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, www.yahoo.com is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See domain name.
Domain name	A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See DNS.
Download	To transfer data in the downstream direction, i.e., from the Internet to the user.
DSL	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
Encryption keys	See network keys
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, twisted pair.

FTP	File Transfer Protocol A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.
Gbps	Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
Host	A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See web browser, web site.
Hub	A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.
ICMP	Internet Control Message Protocol An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IEEE	The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.
Internet	The global collection of interconnected networks used for both private and business communications.
Intranet	A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP	See TCP/IP.
IP address	Internet Protocol address The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See domain name, network mask.
ISP	Internet Service Provider A company that provides Internet access to its customers, usually for a fee.
LAN	Local Area Network. A network limited to a small geographic area, such as a home or small office.

LED	Light Emitting Diode An electronic light-emitting device. The indicator lights on the front of the device are LEDs.
MAC address	Media Access Control address The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; NN:NN:NN:NN:NN:NN.
Mask	See network mask.
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
NAT	Network Address Translation A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.
Network	A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.
Network keys	(Also known as encryption keys.) 64-bit and 128-bit encryption keys used in WEP wireless security schemes. The keys encrypt data over the WLAN, and only wireless PCs configured with WEP keys that correspond to the keys configured on the device can send/receive encrypted data.
Network mask	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See binary, IP address, subnet.
NIC	Network Interface Card An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See Ethernet, RJ-45.
Packet	Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
Ping	Packet Internet (or Inter-Network) Groper A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
Port	A physical access point to a device such as a computer or router, through which data flows into and out of the device.
PPP	Point-to-Point Protocol A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the device uses two forms of PPP called PPPoA and PPPoE. See PPPoA, PPPoE.

PPPoA	Point-to-Point Protocol over ATM One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.
PPPoE	Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.
Protocol	A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.
Remote	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
RIP	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.
RJ-11	Registered Jack Standard-11 The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.
RJ-45	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
Routing	Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.
SDNS	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See DNS.
Subnet	A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See network mask.
Subnet mask	A mask that defines a subnet. See network mask.
TCP	See TCP/IP.
TCP/IP	Transmission Control Protocol/Internet Protocol The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.
Telnet	An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.

TFTP	Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
TKIP	Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.
Triggers	Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them. Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.
Twisted pair	The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See 10BASE-T, 100BASE-T, Ethernet.
Unnumbered interfaces	An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a router-id that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.1.1). The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.
Upstream	The direction of data transmission from the user to the Internet.
VC	Virtual Circuit A connection from your DSL router to your ISP.
VCI	Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See VC.
VDSL	Very High Speed Digital Subscriber Line It provides faster transmission rate and is capable of supporting high bandwidth applications like IPTV and bandwidth consumed applications.
VPI	Virtual Path Identifier Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See VC.

WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the device, WAN refers to the Internet.
Web browser	A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See HTTP, web site, WWW.
Web page	A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page. See hyperlink, web site.
Web site	A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See hyperlink, web page.
WEP	Wired Equivalent Privacy (WEP) encrypts data over WLANs. Data is encrypted into blocks of either 64 bits length or 128 bits length. The encrypted data can only be sent and received by users with access to a private network key. Each PC on your wireless network must be manually configured with the same key as your device in order to allow wireless encrypted data transmissions. Eavesdroppers cannot access your network if they do not know your private key. WEP is considered to be a low security option.
Wireless	Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. See wireless LAN.
Wireless LAN	A wireless LAN (WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.
WPA	Wi-Fi Protected Access WPA is an initiative by the IEEE and Wi-Fi Alliance to address the security limitations of WEP. WPA provides a stronger data encryption method (called Temporal Key Integrity Protocol (TKIP)). It runs in a special, easy-to-set-up home mode called Pre-Shared Key (PSK) that allows you to manually enter a pass phrase on all the devices in your wireless network. WPA data encryption is based on a WPA master key. The master key is derived from the pass phrase and the network name (SSID) of the device. It provides improved data encryption and stronger user authentication. The mode of WPA supported on your device is called Pre-Shared Key (PSK), which allows you to manually enter a type of key called a pass phrase.
WWW	World Wide Web Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.

Appendix D - Specification

A1. Hardware Specifications

- ■ LAN Interface
- Four port 10/100BaseT Ethernet Switch (4 * RJ-45 connectors), IEEE 802.3u with MDI/MDIX auto-detection
- Integrated 802.11b/g WLAN Access Point

- ■ WAN VDSL2 Line Interface
- Compliant with VDSL2 and support 8a/8b/8c/8d, 17a and 30a
- Connection Loops: One (pair wire)
- Connector: RJ-11

- ■ Indicators
- PWR – Green LED indicates power and operation. Red LED indicates failure.
- DSL – Green LED indicates broadband connection
- Internet – Green LED indicates PPP connection and RED indicates PPP failure or device in BRIDGE mode.
- Ethernet – Green LED indicates LAN connection
- WLAN – Green LED indicates wireless AP enabled

- ■ Environment
- Operation Temperature: 0°C ~ 45°C
- Operation Humidity: 5% ~ 95%
- Storage Temperature: -20 ~ +85°C
- Storage Humidity: 5%~95%

- ■ Power
- AC Adapter: Input 110/220VAC, 50/60Hz; Output 12VDC 1.50A

- ■ Certificates
- CE, CB (TBD)

A2. Software Specifications

- Bridging
  - Transparent Bridging and spanning(IEEE 802.1D) with at least 32 MAC addresses
  - RFC2684 (RFC 1483) Bridged
  - Bridge filtering with per-port extensions
- Routing
  - IP routing and PPP supported
  - PAP and CHAP for user authentication in PPP connection
  - RFC2684 (RFC1483) Routed
  - MAC Encapsulated Routing (MER)
  - DHCP client, server and relay agent
  - DNS relay
- Wireless LAN
  - Supports 802.1x; WEP; WEP2; WPA; WPA2; TKIP; AES;
  - Hidden SSID
  - WMM for advanced Quality of Service
  - Supports TKIP and AES
- Firewall
  - Support NAT and DMZ
  - Protection against IP and MAC address spoofing
  - UPnP NAT traversal and VPN / IPSec pass-through
- Configuration and Network Management Features
  - DHCP client and server for IP management
  - UPnP Internet Gateway Device (IGD) compliance
  - WEB for local or remote management
  - HTTP for firmware upgrade and configuration
  - Embedded syslog
  - Support TR-069 with parameters: DeviceInfo, ManagementServer, Time, IPPingDiagonostic, etc

Note: The hardware and software specifications are subjected to change without notices.

Appendix E - Warranties

B1. Product Warranty

Inteno Broadband Technology AB warrants that the xDSL unit will be free from defects in material and workmanship for a period of twelve (12) months from the date of shipment.

Inteno Broadband Technology AB shall incur no liability under this warranty if

– The allegedly defective goods are not returned prepaid to Inteno Broadband Technology AB within thirty (30) days of the discovery of the alleged defect and in accordance with Inteno Broadband Technology AB' repair procedures; or

– Inteno Broadband Technology AB' tests disclose that the alleged defect is not due to defects in material or workmanship.

Inteno Broadband Technology AB' liability shall be limited to either repair or replacement of the defective goods, at Inteno Broadband Technology AB' option.

Inteno Broadband Technology AB MARKS NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE USER'S DOCUMETATION. INTENO SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

B2. Warranty Repair

1. During the first three (3) months of ownership, Inteno Broadband Technology AB will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, Inteno Broadband Technology AB will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced products shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. Inteno Broadband Technology AB will ship surface freight. Expedited freight is at customer's expense.
2. The customer must return the defective product to Inteno Broadband Technology AB within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, Inteno Broadband Technology AB will bill the customer for the product at list price.

B3. Out-of-Warranty Repair

Inteno Broadband Technology AB will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

Appendix F - Regulation

FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 to the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, used, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense. The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless Inteno expressly approves the changes or modifications.

FCC Part 15 Notice with Wireless

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Warning: Operation is subject to the following two conditions:
1) This device may not cause harmful interference.
2) This device must accept any interference received including interference that may cause undesired operation.

FCC Part 68 Notice

This equipment complies with Part 68 of FCC Rules. On the base unit of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. IF REQUESTED, THIS INFORMATION MUST BE GIVEN TO THE TELEPHONE COMPANY.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to you line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in it is facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

NOTICE: The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or an electronic device to send any message via a telephone fax machine, unless such a message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission the following information:

- ✓ The date and time of transmission
- ✓ Identification of either business, business entity or individual sending message
- ✓ Telephone number of either the sending machine, business entity or individual

Warning: Users should not attempt to make such connections themselves, but should contact appropriate electric inspection authority, or electrician, as appropriate.
Do not use any other power adapter except the one that accompanies the unit. Use of other adapter could result in damage to the unit. To prevent electronic shock, please do not open the cover.

UL Safety Regulations

- ✓ Disconnect TNV circuit connector or before removing cover or equivalent.
- ✓ Disconnect TNV circuit connector(s) before disconnecting power.
- ✓ Do not use this product near water for example, near a bathtub, washbowl, and kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- ✓ Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening.
- ✓ Do not use the telephone to report a gas leak in the vicinity of the leak.
- ✓ Use only the power cord batteries indicated in this manual. Do not dispose of batteries in a fire, as they may explode. Check with local codes for possible special disposal instructions.

No. 26 AWG Telephone Line Cord shall either be provided with the equipment or shall be described in the safety instruction. If fuse (F1) is not present, see the caution statement listed below:

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Appendix G - Contact information

You can help us serve you better by sending us your comments and feedback. Listed below are the addresses, telephone and fax numbers of our offices. You can also visit us on the World Wide Web at www.inteno.se for more information. We look forward to hearing from you!

HEADQUARTER

Inteno Broadband Technology AB
Tel: +46 8 579 190 00
Drivhjulsvägen 22, SE-126 30, Hägersten, Sweden

NORWAY OFFICE

Inteno Broadband Technology AS
Tel: +47 67 91 19 30
Solheimveien 36, N-1473, Lørenskog, Norway

FINLAND OFFICE

Vaasa

Oy Netmedia Finland Ab
Vaasanpuistikko 18, 3.kerros
PL 98, 65101 VAASA
Tel: +358 6 3181 300

Helsinki

Oy Netmedia Finland Ab
Rälssintie 10
00720 HELSINKI
Tel: +358 9 347 8540

V1.0XA567107C