User Manual

X5668

Version: 1.0

XAVi Technologies Corporation
Tel: +886-2-2995-7953
Fax: +886-2-29957954
9F, No. 129, Hsing Te Road, Sanchung City,
Taipei County 241,
Taiwan

XAVi Technologies Corporation 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.

Federal Communication Commission Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

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

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless XAVi expressly approves the changes or modifications.

Table of Contents

Chapter 1

Getting Started

I. Overview

The **X5668** is a multi-mode ADSL2+ router/modem, which is designed to interoperate with DSLAMs from major vendors to meet the worldwide ADSL CPE market requirements.

It complies with ANSI T1.413 issue 2, ITU-T G.dmt, G.lite, G.dmt.bis (ADSL2) and ADSL2+ with up to 24 Mbps downstream link rate. The integrated Ethernet switch features automatic crossover-correction and speed sensing for easily connecting to user's PCs or LAN environment.

II. Features

- Support up to ADSL2+ (G.992.5) with 24 Mbps downstream and 1 Mbps upstream rates
- Integrated one Ethernet port with automatic speed-sensing and crossover correction
- Support Networking protocols such as PPP, NAT, Routing, DHCP server/relay/client
- Configuration and management by Web-browser through the Ethernet interface and remotely through ADSL interface
- Firmware upgradeable through HTTP/TFTP

III. Packaging

This package consists of the following items:

X5668 ADSL device unit

RJ-45 Cable

RJ-11 Cable

AC Adapter

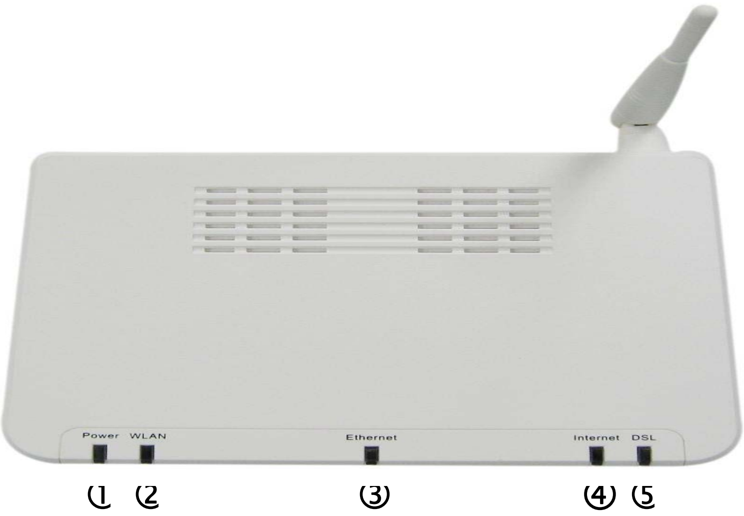
IV. Safety Guidelines

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

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

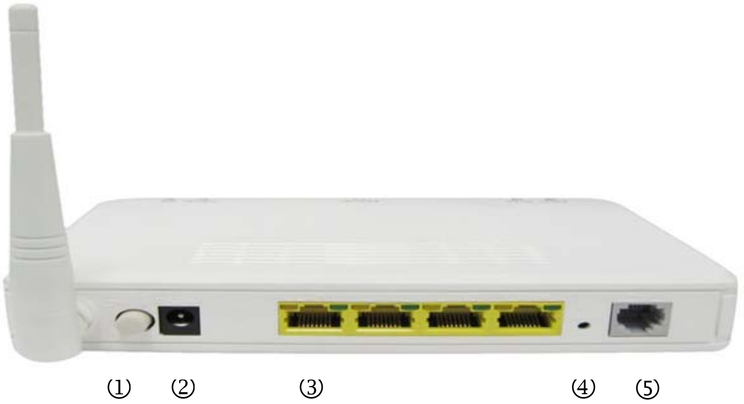
V. Appearance

Front Panel



	Label	Description
①	Power	GREEN off: No power or user forgets to plug power adapter GREEN on: Power on then GREEN lights on RED on: test fail RED lights on
②	WLAN	GREEN off: WLAN disable GREEN on: WLAN enable and stand by GREEN blinking: packets transmitted through
③	Ethernet	GREEN off: No ethernet connected on LAN side GREEN on: 4 ethernet ports, any port connected GREEN blinking: packets transmitted through
④	Internet	GREEN off: No connection to Internet GREEN on: No bridge mode and router mode successes to get IP, then GREEN ON GREEM blinking: Any mode when packets transmitted then GREEN LED blinking. RED on: router mode connection failed to get IP or box is set to be bridge mode then RED lights on
⑤	DSL	GREEN on: phsical layer sync successes GREEN blinking: sync progress GREEN off: cable not connected or no sync

Rear Panel



	Label	Description
①	SWITCH	To turn on / off the power.
②	POWER	Power interface, Connect with power adaptor.
③	LANs	To be connected to a PC network card by a straight-through network cable, also can use a crossover cable to connect to Hub, Switch or Router.
④	Reset	Reset to default settings is located at bottom of router. Press the reset button for 5 seconds while the router is up and running. Then you can reset the modem with the default setting.
⑤	DSL	Connected with phone line or " ADSL" port of the splitter.

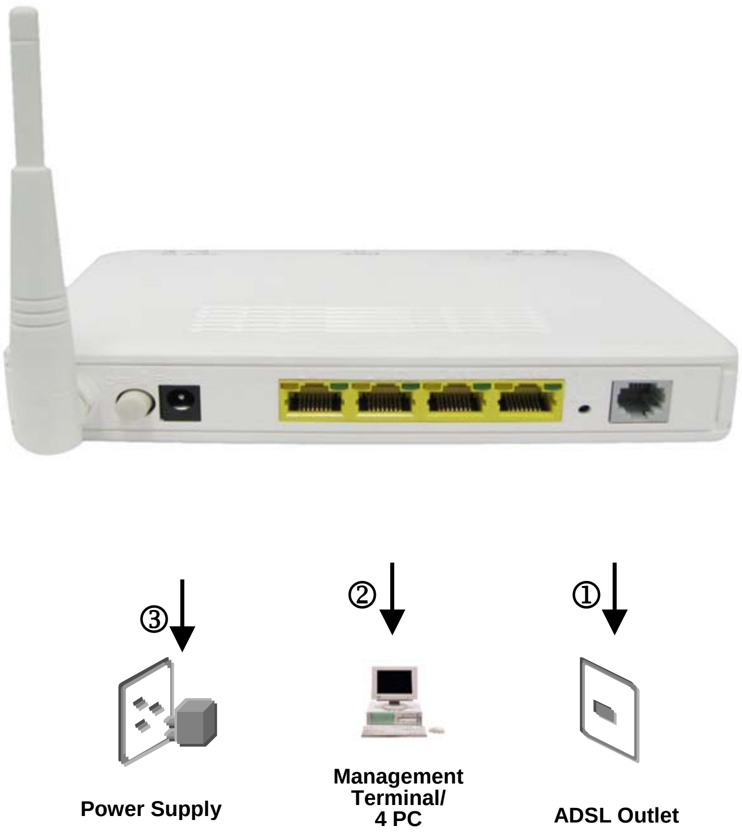
VI. Hardware Installation

Follow the steps below to set up your device:

Step 1: Connect one end of the ADSL cable to the LINE port of ***X5668*** and the other end to the ADSL wall outlet.

Step 2: Use a RJ-45 cable to connect one end to an ETHERNET port of ***X5668*** and the other end to the LAN or a PC with an Ethernet adapter installed.

Step 3: Plug in the AC adapter to the AC power socket, and then connect the DC jack to the POWER inlet of ***X5668.*** Push the SWITCH button to turn it on.



VII. Management

There are several ways that you can make the configuration:

- **Local Ethernet Port (telnet)** – connect the Ethernet port to your local area network or directly to a PC, "telnet" ***X5668*** from any workstation in the LAN. The default local Ethernet IP address is "192.168.1.1". See Chapter 2, Command Line Interface, for more details.
- **Local Ethernet Port (Web browser)** – connect the Ethernet port to your local area network or directly to a PC. Launch your Web browser and enter default local Ethernet IP address "192.168.1.1" into the address bar.
- **ADSL Port from Remote Site** – while the ADSL connection is in service and it is set to router mode, you may remotely "telnet" ***X5668*** from a workstation connected to the equipment.

Note: As operating an ADSL device requires technical know-how and experience, it is recommended that only qualified technical staff manage ***X5668*** Therefore, a password authentication is required when you enter the command line and Web interface. See the *Default Values* section to obtain the password.

VIII. Default Values

X5668 is pre-configured with the following parameters; you may also re-load the default parameters by pressing the reset button on the real panel or by using the **System Commands** link on the Web interface.

Username/Password: admin/admin

Default IP Address

Ethernet (local) IP: 192.168.1.1

Subnet mask: 255.255.255.0

Protocol

RFC1483 Bridge: VPI/VCI: NA/NA

Class (QoS): NA

WAN and ADSL

Local Line Code: Multi Mode

DHCP Server: Disable

DHCP start IP: 192.168.1.2

DHCP end IP: 192.168.1.254

Note: The Username and Password are case-sensitive.

IX. Software Upgrade

You may easily upgrade ***X5668*** embedded software by obtaining the compressed upgrade kit from the service provider and then following the steps for upgrading through a Web-browser:

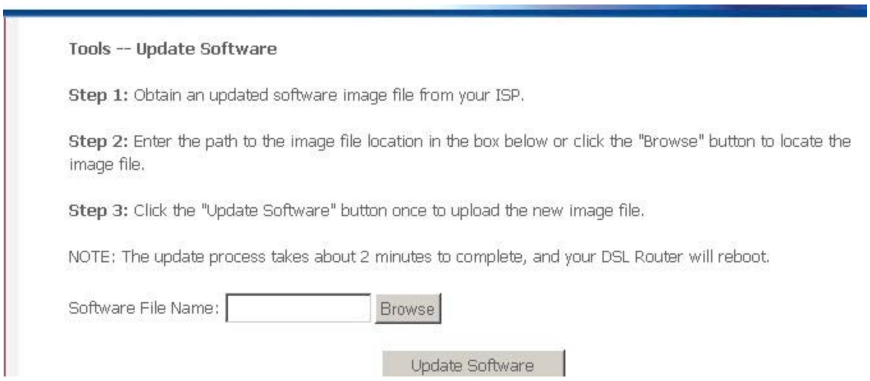
Step 1: Extract the ZIP file for updated firmware.

Step 2: Connect ***X5668*** via the local Ethernet port or remote ADSL link, making sure that the ***X5668*** Ethernet IP address and your terminal are properly configured so that you can successfully "*ping*" ***X5668***. The default local IP address is "192.168.1.1".

Step 3: Launch the Web browser (IE or Netscape), and enter the default IP address 192.168.1.1 into the address bar to access the Web management page.

Step 4: Click on the **Management** link on the navigation bar and then on the **Update Software** link below it.

Step 5: Click on the **Browse** to select the appropriate firmware and then click on the **Update Software** button. The upgrade process may take about 60 seconds. Do not reset the device while



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:

Chapter 2

Web Management Interface

I. Overview

The Web Management Interface is provided to let the configuration of ***X5668*** as easily as possible. It provides a user-friendly graphical interface through a Web platform. You can configure bridge or router functions to accommodate your needs. In the section below, each configuration item is described in detail.

II. Preparation

Step 1: Please refer to the hardware installation procedure in Chapter 1 to install ***X5668***.

Step 2: You should configure your PC to the same IP subnet as the ***X5668***.
Example: ***X5668***: 192.168.**1.1**
Your PC: 192.168.**1.2**

Step 3: Connect your PC to ***X5668*** and make sure that the PING function is working properly. The default IP address of this device is 192.168.1.1

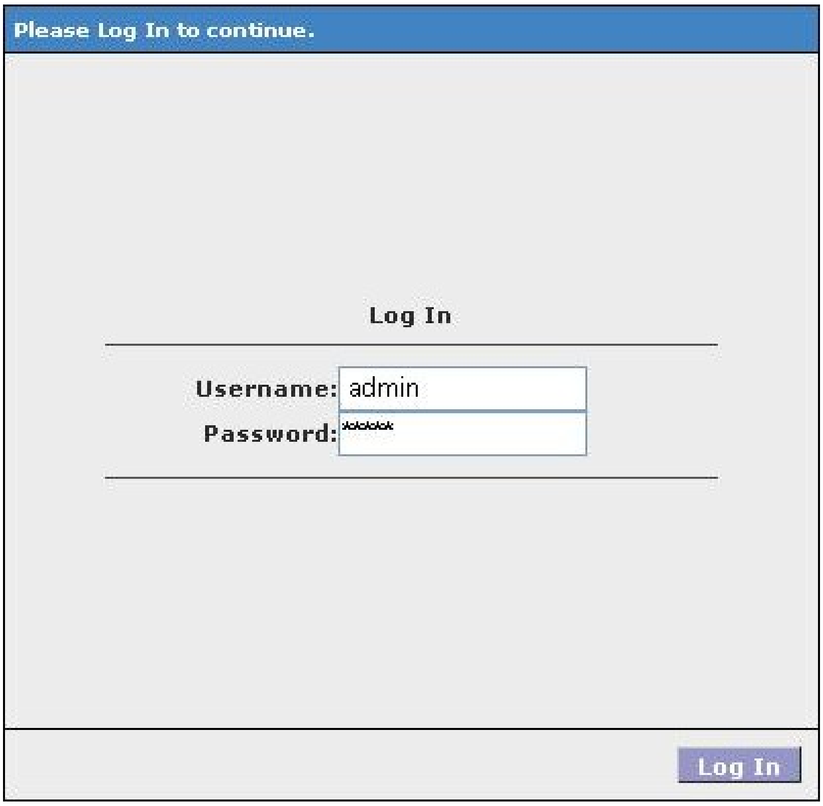
Step 4: Launch the Web browser (IE or Netscape), and enter the default IP address 192.168.1.1 into the address bar to access the Web management page.

Step 5: The **Login** dialog box will appear first.

1. Login

- The **Enter Network password** window will appear when starting the configuration. With the window active, type **admin** for both **User name** and **Password**, and then click on the **OK** button.

Note: The username and password are case-sensitive.



Please Log In to continue.

Log In

Username: admin

Password: *****

2. Quick Setup

This model supports Quick Setup for user to set up the modem/router to work with the provide service from ISP or TELCO.

STEP1> Click the "Quick Setup", This Quick Setup will guide you through the steps necessary to configure your DSL Router.

STEP2> Select the check box "DSL Auto-connect" to enable DSL Auto-connect process. If you want to input VPI/VCI and choose the protocol to connect your service, just leave this check box disable, then input VPI, and VCI numbers. Click "Next" to go to next step.

STEP3> Choose the Connect Type, the specific page will show up, refer to chapter "WAN Setup" to go ahead next STEP for different configuration.

<Note> If the configuration is bridge encapsulation, there is no need to configure any more parameters. Only need to use the third party dial-up software to connect the Internet.

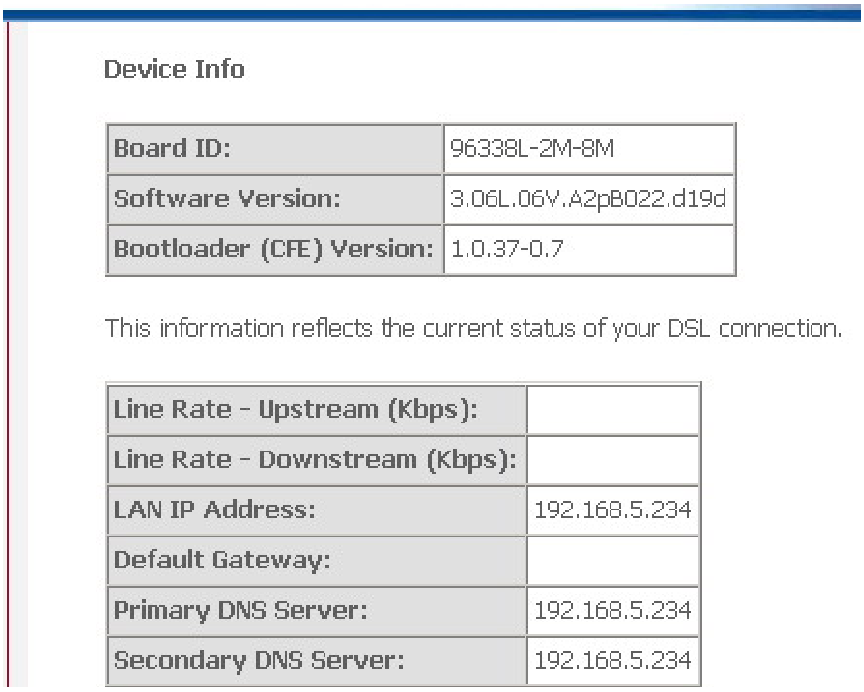
This model supports：PPPoA、PPPoE、MER、IPoA、Bridging. For detail configuration information, please check the following chapters configuration guide.

3. Device Info

Device Info is used to show the main information inside the router. There are few pages below will be provided for the detailed data.

"Summary" will show

a. Board ID
b. Software Version
c. Bootloader Version
d. Line Rate
e. LAN IP Address
f. Default Gateway
g. Primary DNS Server
h. Secondary DNS Server



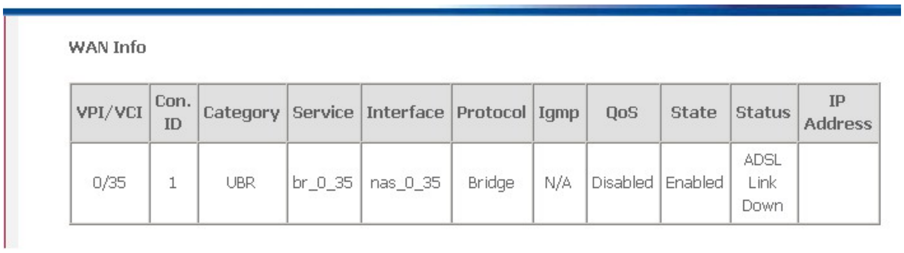
Device Info

Board ID:	96338L-2M-8M
Software Version:	3.06L.06V.A2pB022.d19d
Bootloader (CFE) Version:	1.0.37-0.7

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.5.234
Default Gateway:	
Primary DNS Server:	192.168.5.234
Secondary DNS Server:	192.168.5.234

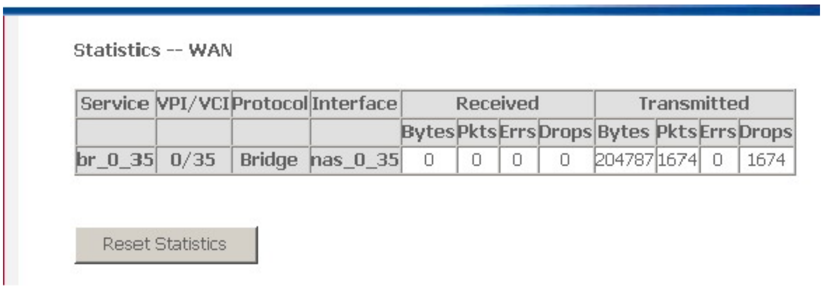
"WAN Info" will show the related information about connection ID, ATM QoS setting if the VPI/VCI is configured already.



WAN Info

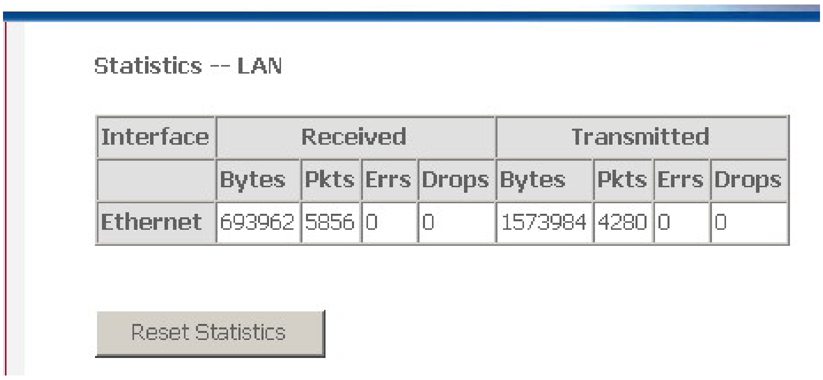
VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address
0/35	1	UBR	br_0_35	nas_0_35	Bridge	N/A	Disabled	Enabled	ADSL Link Down	

"Statistics" will show the receive/transmit packets on LAN side and WAN side, ATM related interface statistics, ADSL physical layer related data. On the page, BER test on ADSL can be done by click the button "ADSL BER Test"



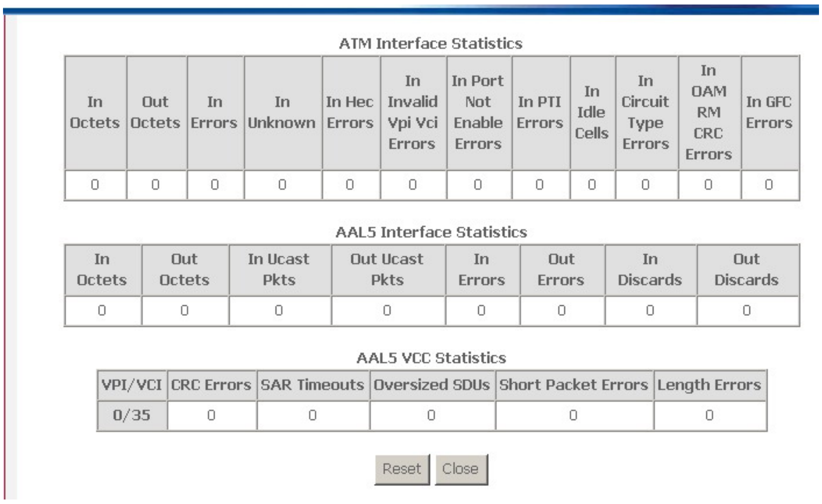
Statistics -- WAN

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	204787	1674	0	1674



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	693962	5856	0	0	1573984	4280	0	0



ATM Interface Statistics

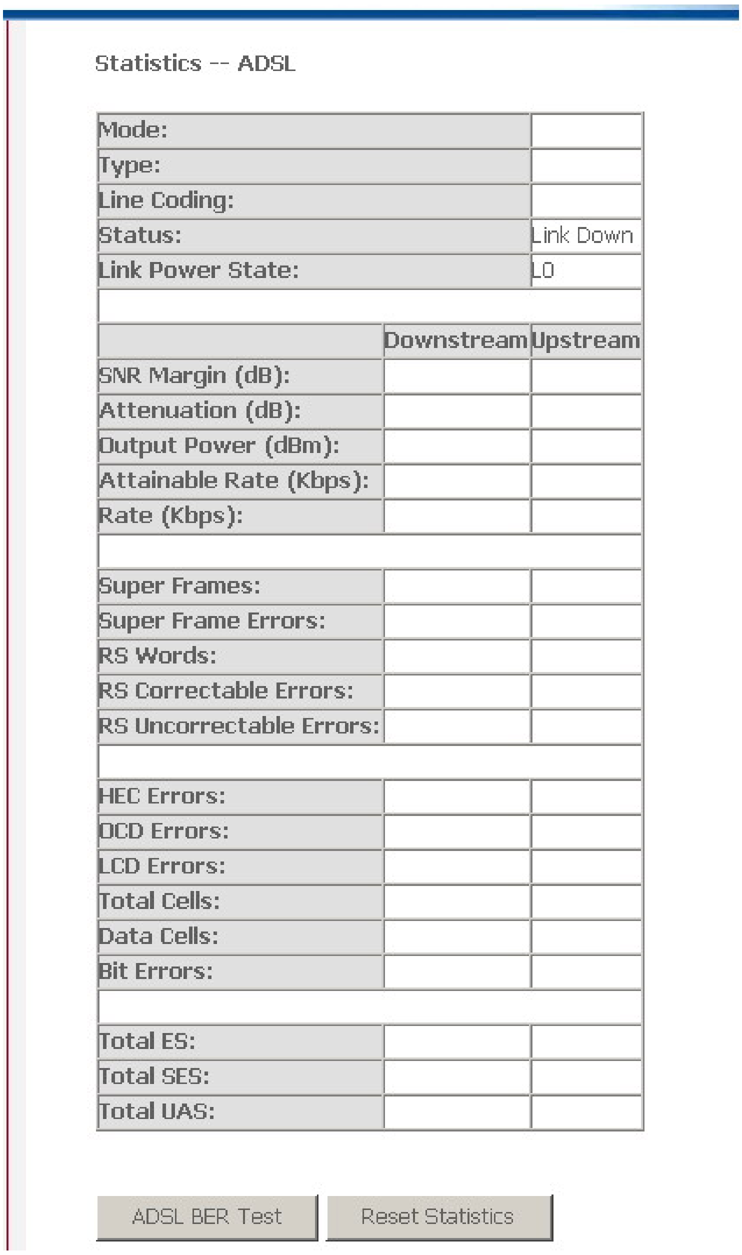
In Octets	Out Octets	In Errors	In Unknown	In Hec Errors	In Invalid Vpi Vci Errors	In Port Not Enable Errors	In PTI Errors	In Idle Cells	In Circuit Type Errors	In OAM RM CRC Errors	In GFC Errors
0	0	0	0	0	0	0	0	0	0	0	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

AAL5 VCC Statistics

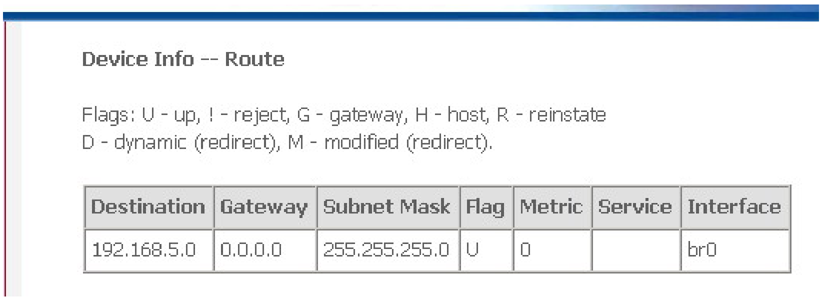
VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0/35	0	0	0	0	0



Statistics -- ADSL

Mode:		
Type:		
Line Coding:		
Status:		Link Down
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

"Route" will show the configured routing rules.

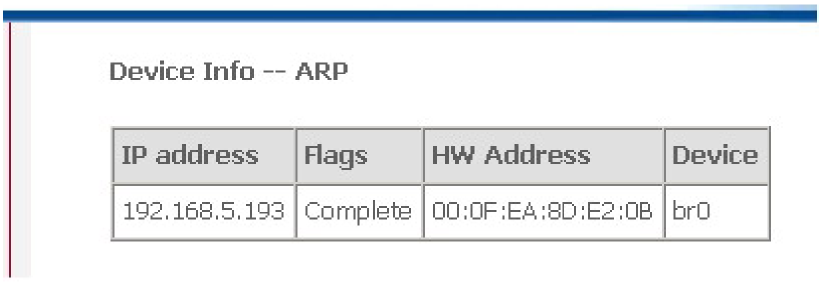


Device Info -- Route

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

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.5.0	0.0.0.0	255.255.255.0	U	0		br0

"ARP" will show the current ARP data.



Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.5.193	Complete	00:0F:EA:8D:E2:0B	br0

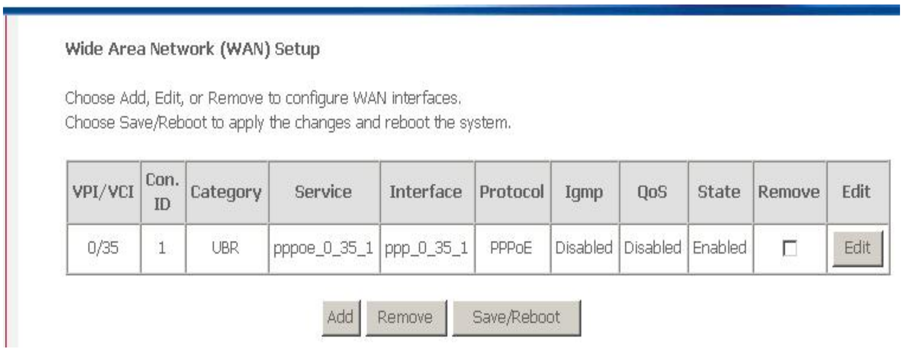
4. Advanced Setup

To check "Advance Setup", several sub-menus will show up. They are "WAN", "LAN", "Routing", "DSL", etc. Depending different setting mode, the sub-menus will be different. The sections below introduce the setting for each page.

4.1 WAN

Click "WAN" on the left manual. Access "WAN" configuration page.

- Note: At most eight connections can be set. If you need to add a new connection, please delete or modify an existing connection.

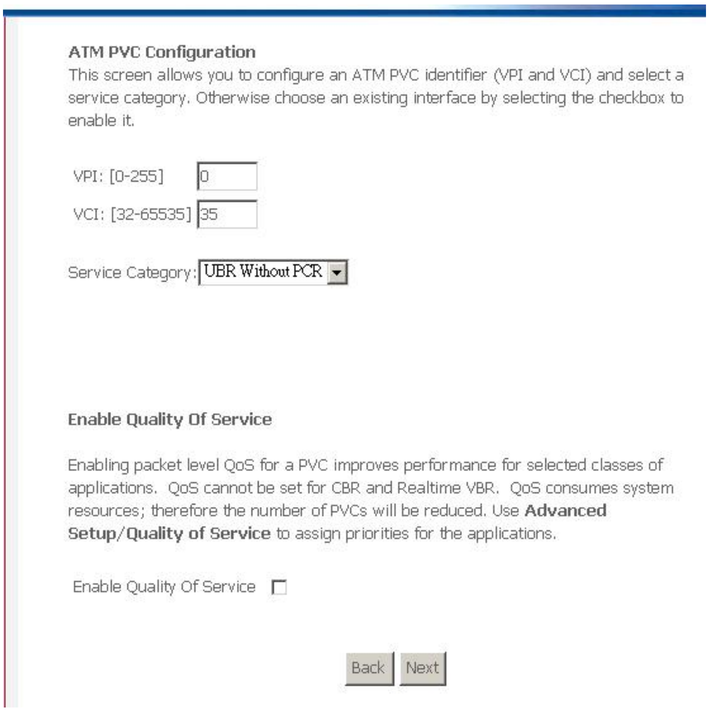


Wide Area Network (WAN) Setup

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

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/35	1	UBR	pppoe_0_35_1	ppp_0_35_1	PPPoE	Disabled	Disabled	Enabled	□	Edit

Click on the next connection, which you want to modify. Press "Edit" button, enter the configure guide.



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] 35

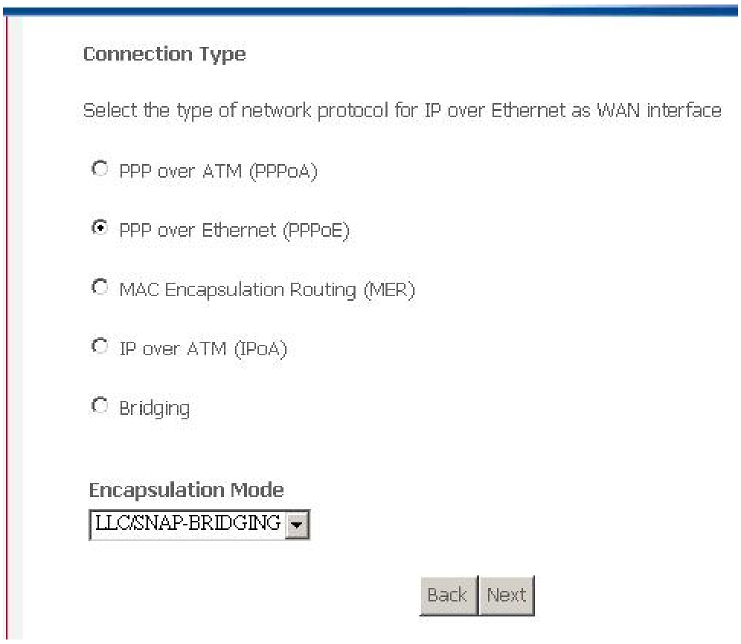
Service Category: UBR Without PCR

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 □

- The value of VPI and VCI should be provided by your ISP. After to input the PVC value, press "Next" into "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

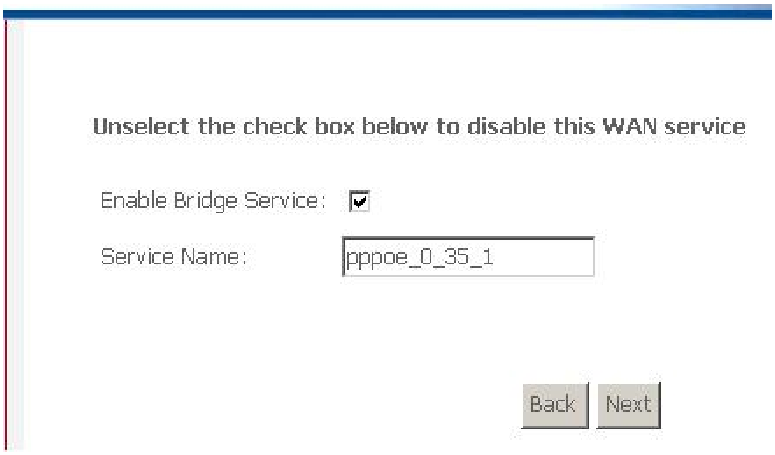
The model supports five protocols. Choose the protocol which is provided by ISP and PVC encapsulation, click "Next" enter to the protocol configure. Below, the configuration of the five protocols is introduced.

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging

- Some connection lines need to confirm the LLC or VC, if you can't confirm, please don't modify the default value or ask your ISP.

4.1.1 BRIDGE CONFIGURATION

Select the Bridging mode. Then press "Next" to specify the Service Name, and select the "Enable Bridge Service".

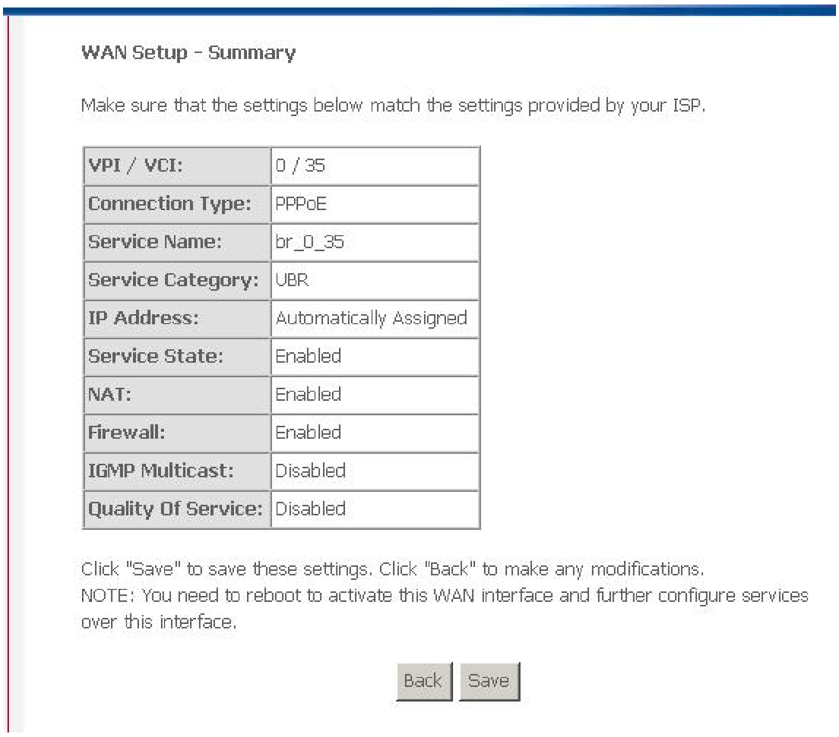


Unselect the check box below to disable this WAN service

Enable Bridge Service: ☑

Service Name: pppoe_0_35_1

Press "Next" to "WAN configuration", click "save" to save configuration, if you need to modify the parameter, click "back".



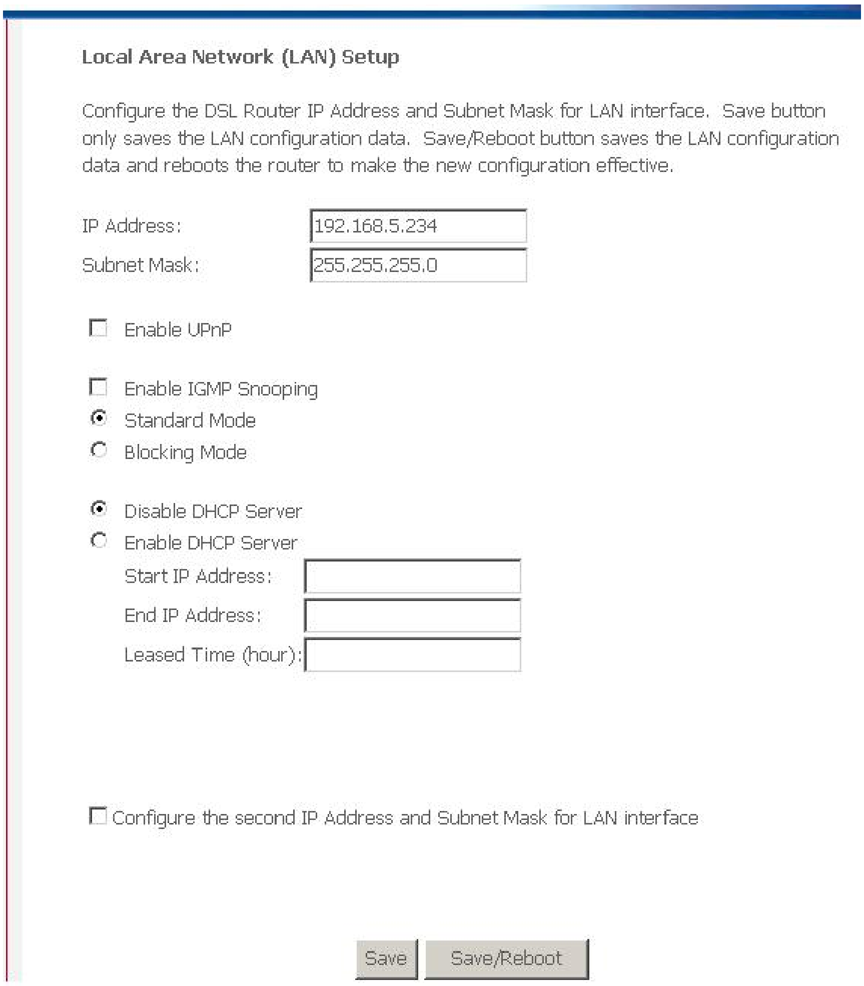
WAN Setup - Summary

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

VPI / VCI:	0 / 35
Connection Type:	PPPoE
Service Name:	br_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
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.

Note：When you use bridge mode, please close "DHCP SERVER".



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. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: 192.168.5.234

Subnet Mask: 255.255.255.0

□ Enable UPnP

□ Enable IGMP Snooping

● Standard Mode

○ Blocking Mode

● Disable DHCP Server

○ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

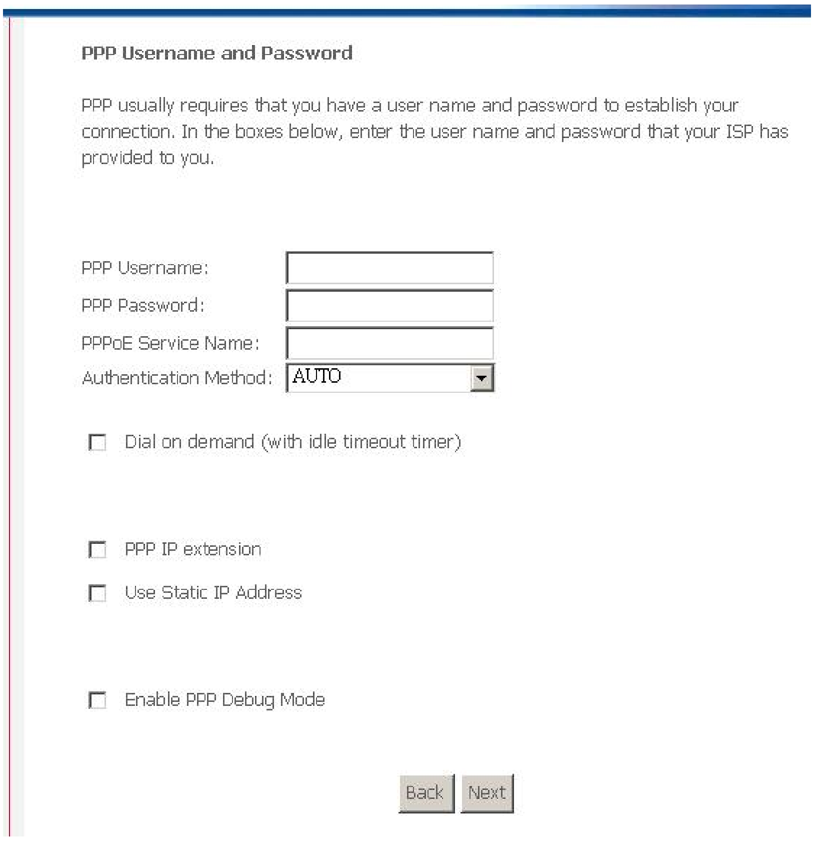
□ Configure the second IP Address and Subnet Mask for LAN interface

4.1.2 PPPoE CONFIGURATION

PPPoE is also known as RFC 2516. It is a method of encapsulating PPP packets over Ethernet.

PPPoA is also known as RFC2364 and named as Peer to Peer Protocol over ATM. As PPPoE, it also includes all the features of PPP. Although it's based on ATM protocol, the setting of all the other parameters is similar with PPPoE. So we only describe PPPoE in detail here.

In Figure 3.4, select PPP over Ethernet (PPPoE), press "Next step" entering the configuring
interface.



PPP Username and Password

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

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

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Use Static IP Address

□ Enable PPP Debug Mode

- PPP Account: Your account from ISP to access Internet.
- Password: Input the password assigned by your ISP.
- PPPoE server name: Server name of network ISP. No need to set.
- Authentication Mode: Authentication mode of network ISP. Default is AUTO.
- Connection on demand: When this mode is selected, the connection

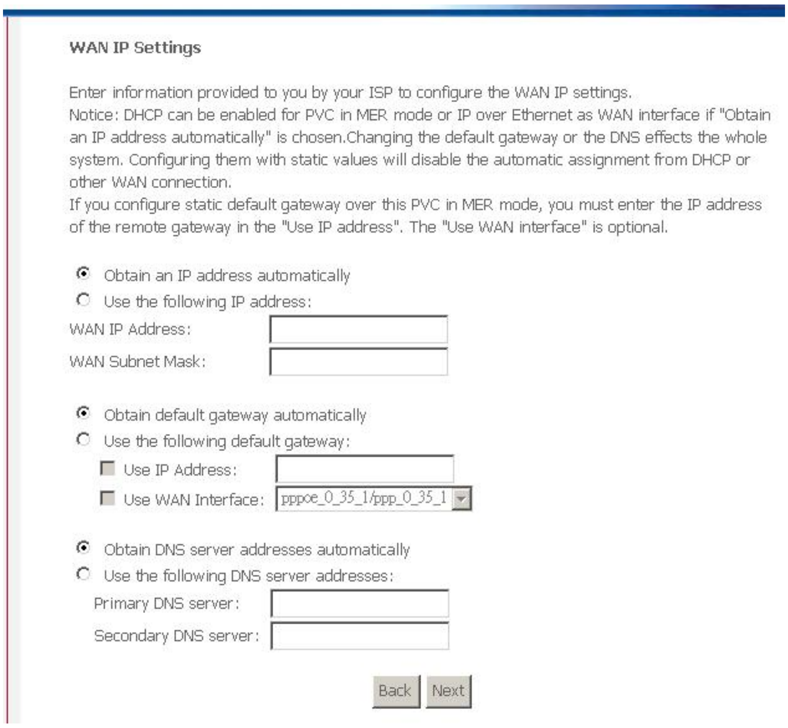
that has no traffic within assigned disconnect timeout (e.g. 1 minute) will be automatically disconnected. The connection will be activated again when traffic arrives. This function is advantageous for users who are charged with online time. It should be noticed that some programs automatically link to Internet. Computer will send data to network when infected by virus. Connection will not be disconnected under these data streams.

- Disconnect timeout: When "Connection on demand" is selected, this input box indicates that after how long the connection will be disconnected in the absence of traffic. If the value is 0, connection will not be disconnected.

Press "Next step" when configuration is finished. The following operation is same with Figure 3.5. Notice that PPPoE mode does not work until the modem is reset.

4.1.3 MAC Encapsulation Routing (MER)

Selecct MAC Encapsulation Routing (MER), press "Next", and the configuration can be queried from your ISP.



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 chosen.Changing the default gateway or the DNS effects 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 "Use IP address". The "Use WAN interface" is optional.

● 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:	pppoe_0_35_1/ppp_0_35_1

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

Primary DNS server:	
Secondary DNS server:	

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

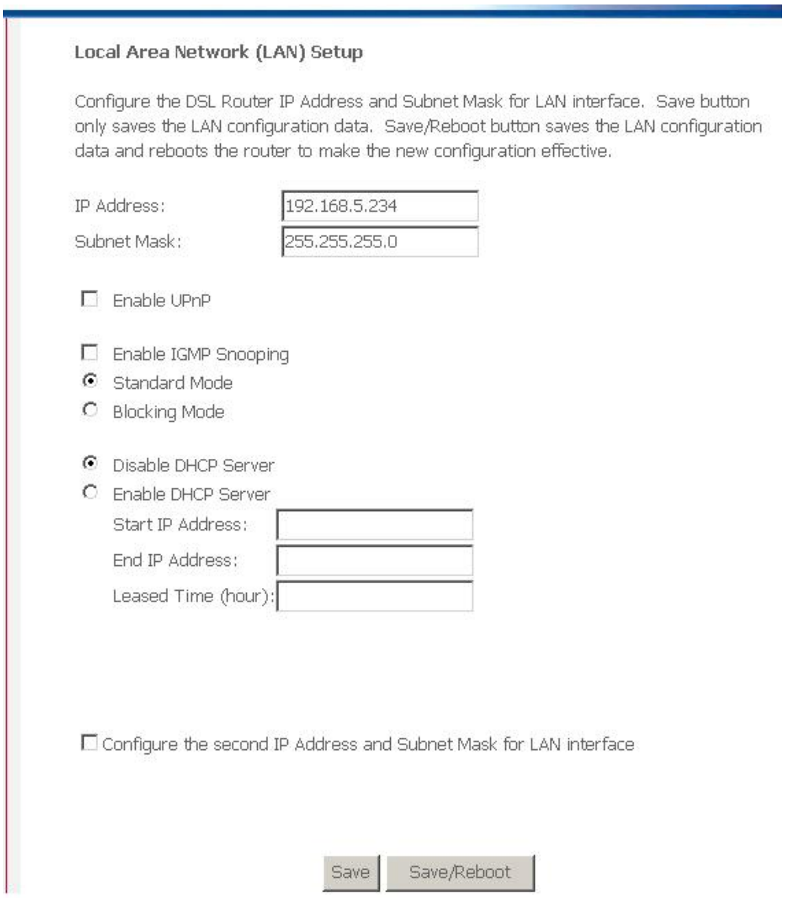
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.

Changing the default gateway or the DNS, this will affect 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 "Use IP address". The "Use WAN interface" is optional.

4.2 LAN

Click "LAN" below "Advanced Setup" on the manual. Access "LAN" configuration page. The local port settings are used to



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. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: 192.168.5.234

Subnet Mask: 255.255.255.0

□ Enable UPnP

□ Enable IGMP Snooping

● Standard Mode

○ Blocking Mode

● Disable DHCP Server

○ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

□ Configure the second IP Address and Subnet Mask for LAN interface configure the LAN IP address, DHCP server and relay settings.

- **IP Address**: Enter the IP address.
- **Netmask**: Enter the subnet mask for the IP address.

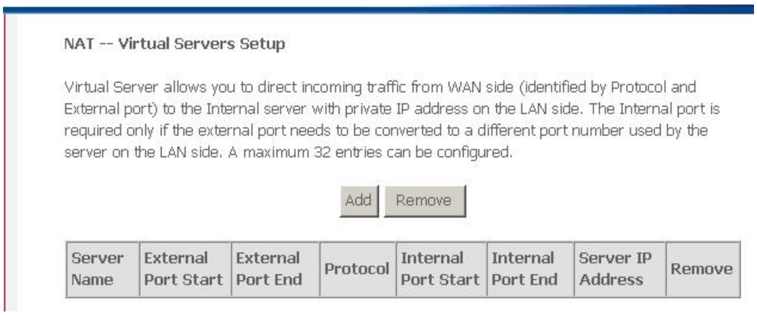
- **Enable IGMP Snooping**: To enable or disable IGMP Snooping by this setting. When the setting is enalbe, the model will snoop IGMP packets and set the related setting on switch to make sure the packets form video server will be multi-casted to the join port not all ports. This way will prevent the video streams generate packets storm.
- **Enable DHCP Server:** This setting to enable/disable DHCP server.
- **Start IP Address**: Enter the first IP for the address pool.
- **End IP Address**: Enter the last IP for the address pool.
- **Lease Time**: Enter the value in hours definign how long an IP address can be assigned to a host.
- **Enable DHCP Relay:** This setting to enable/disable DHCP server.
- **Relay IP**: Enter the IP address of the DHCP relay server.

4.3 NAT

There are three pages to set NAT related functions include Virtual Servers, Port Triggering, DMZ Host. The following sections will describe page by page.

4.3.1 Virtual Servers

Access "Virtual Servers" to enter the page below. This page is used to open related ports for specific applications. This page allows you to configure the port forwarding feature of this device. This feature works in conjuction with NAT/PAT and the firewall.



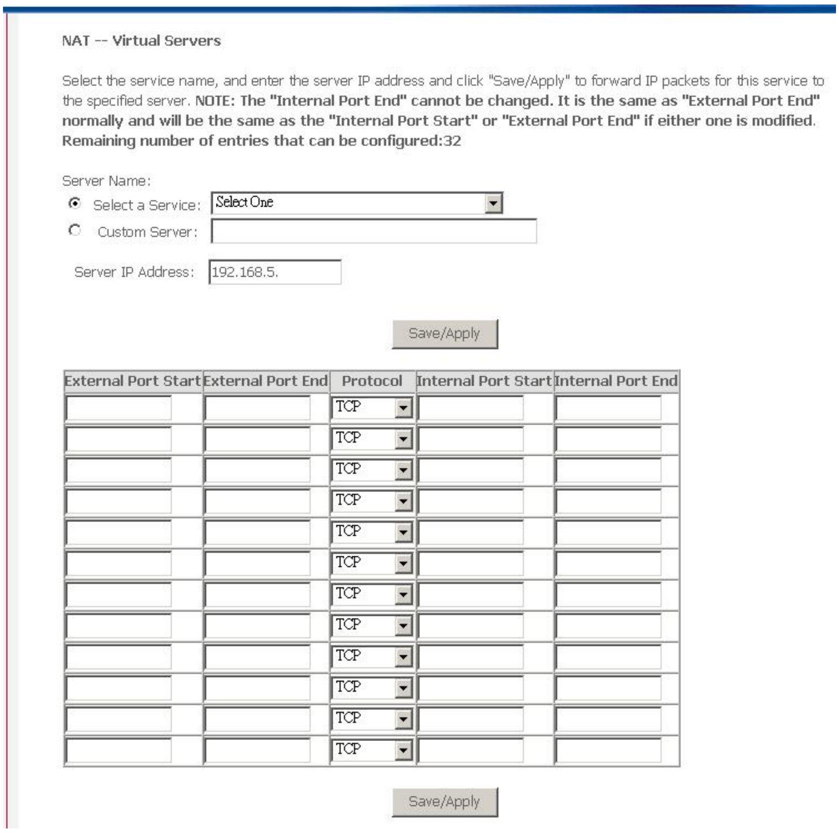
NAT -- Virtual Servers Setup

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

Port fowarding can be used to provide local services for networks or node on the Internet in order to use special applications or play games.

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.



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: 192.168.5.

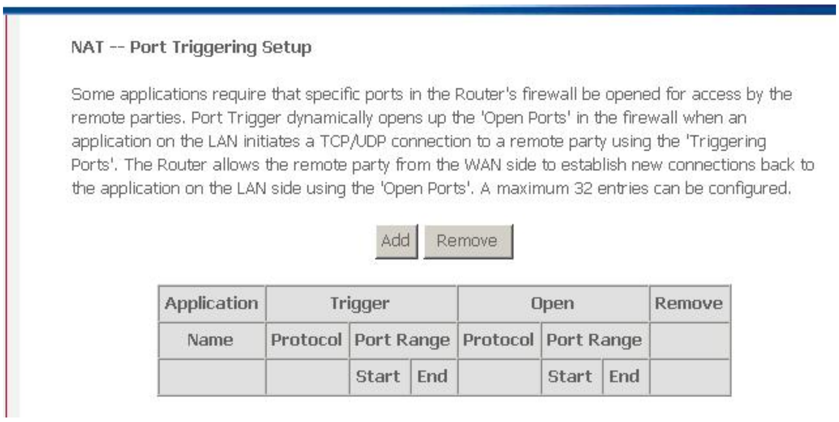
Save/Apply

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

Save/Apply

4.3.2 Port Triggering

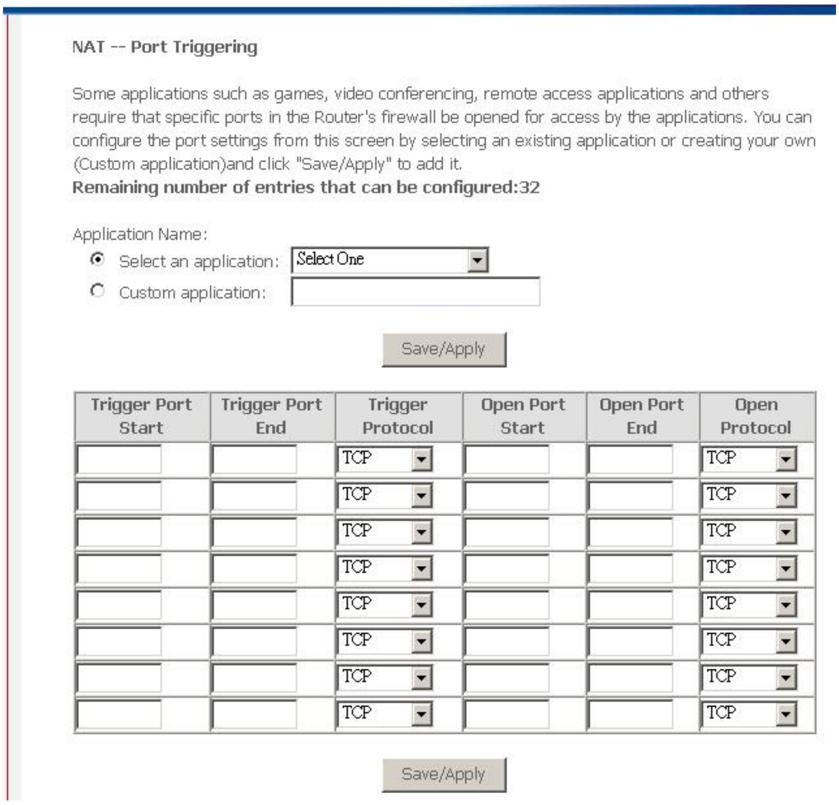
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router 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.



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	



NAT -- Port Triggering

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

Remaining number of entries that can be configured:32

Application Name:

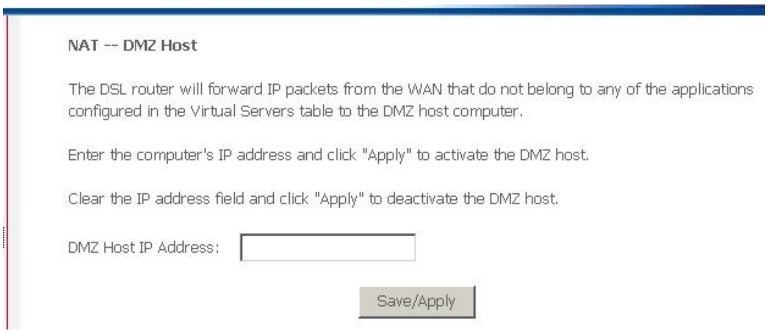
● Select an application: Select One

○ Custom application:

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

4.3.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer. Enter the computer's IP address and click "Apply" to activate the DMZ host. Clear the IP address field and click "Apply" to deactivate the DMZ host.



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 Virtual Servers table to the DMZ host computer.

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:

4.4 Security

Click "Security" below "Advanced Setup" on the left manual. There are two setting items, MAC Filtering or IP Filtering and Parental Control. MAC Filter and IP filtering are exclusive. If the model is set to router mode, then IP Filtering page will show up. If the model is set to bridge mode, the MAC Filtering page will show up.

4.5 Routing

Click "Routing" below "Advanced Setup" on the left manual. Access "Routing" configuration page. There are two sub-pages, "Default Gateway" and "Static Route".

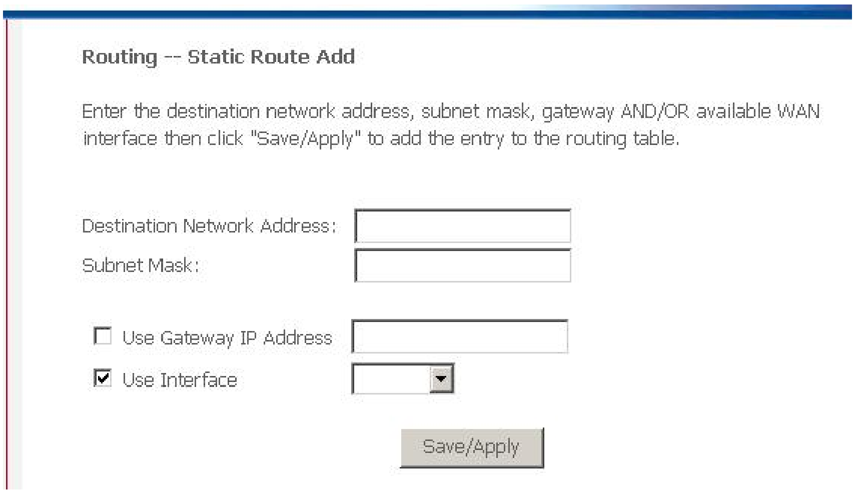
4.5.1 Default Gateway

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.

4.5.2 Static Route

- Click on the **Static Routes** link on the navigation bar to view the static routes table and configure this setting.
- Press "Add" to add the routing table for static routing.
- Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.



Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

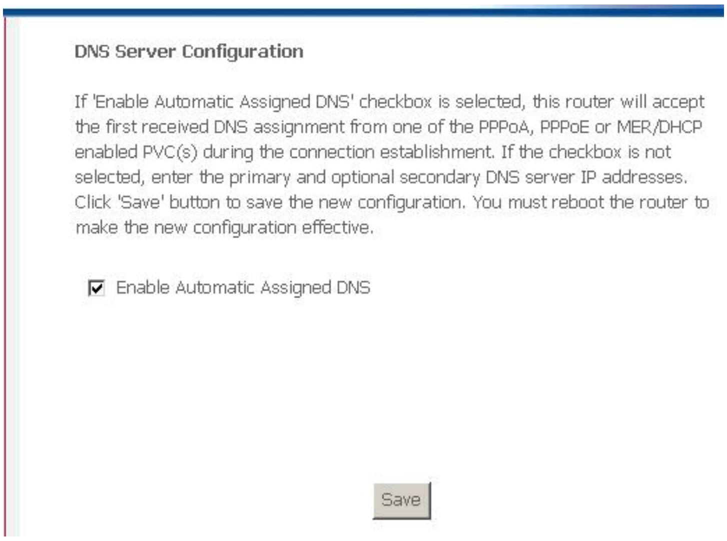
□ Use Gateway IP Address

☑ Use Interface

4.6 DNS

4.6.1 DNS Server

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.



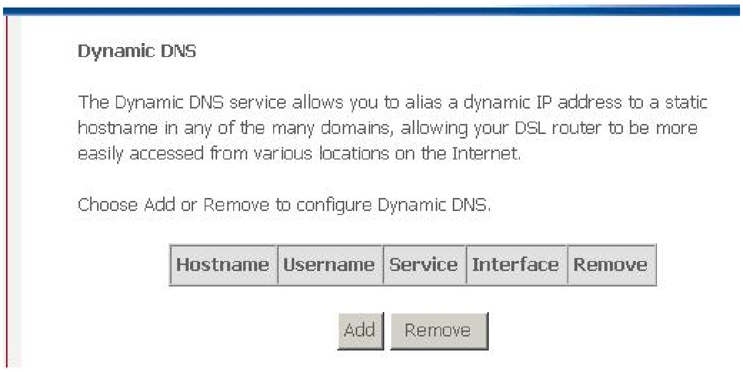
DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

☑ Enable Automatic Assigned DNS

4.6.2 Dynamic DNS

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



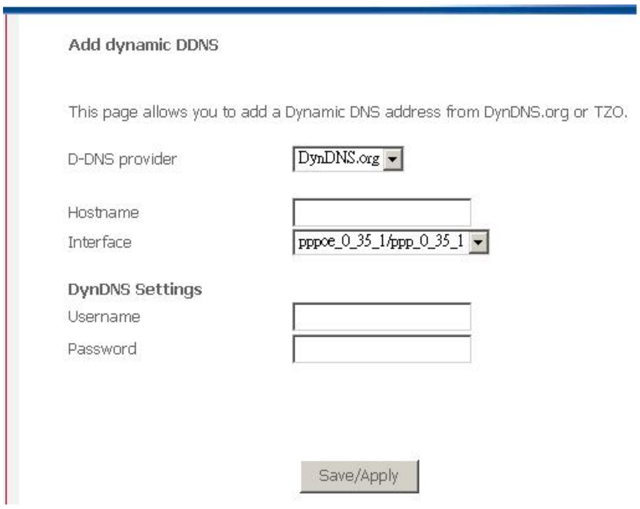
Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Choose Add or Remove to configure Dynamic DNS.



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: pppoe_0_35_1/ppp_0_35_1

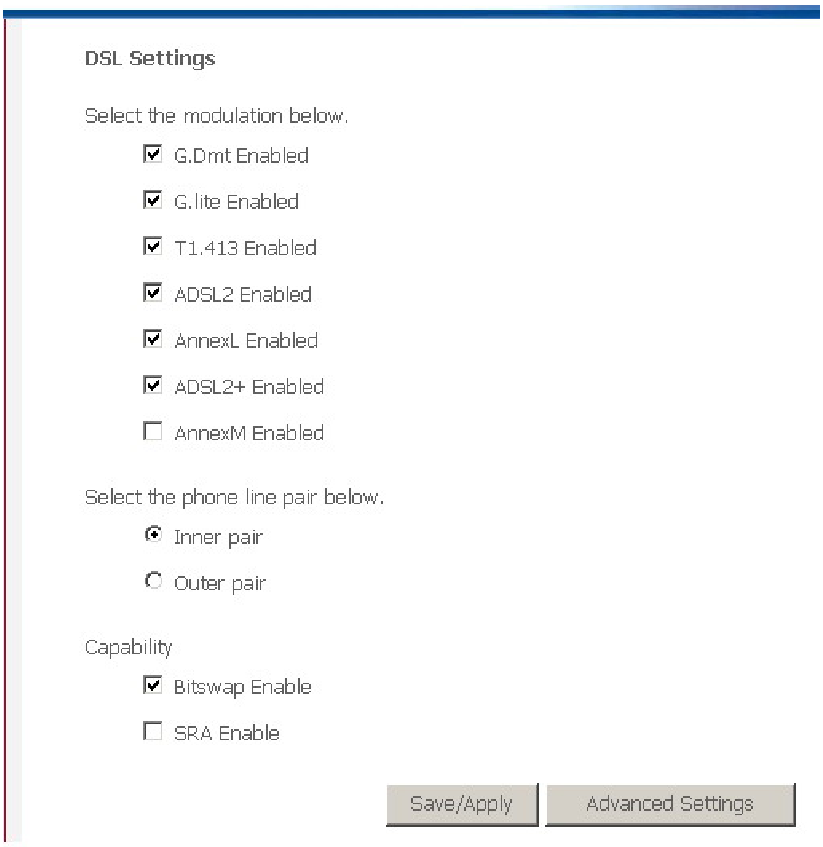
DynDNS Settings

Username:

Password:

4.7 DSL

Click "DSL" below "Advanced Setup" on GUI. There are DSL related settings on the page. The detailed, please check to your service provider.



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.

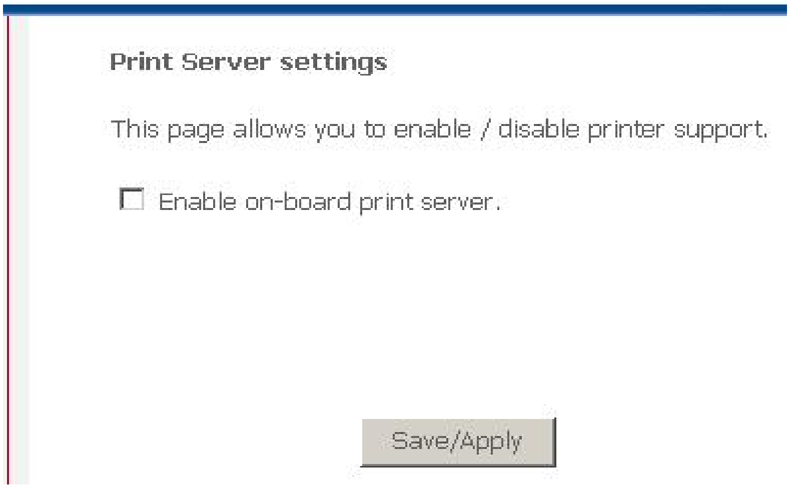
- ● Inner pair
- ○ Outer pair

Capability

- ☑ Bitswap Enable
- ☐ SRA Enable

4.8 Print Server

This page allows you to enable / disable printer support. To connect the USB printer with USB host connector and check "Enable on-board print server". The printer can be shared on LAN side.



Print Server settings

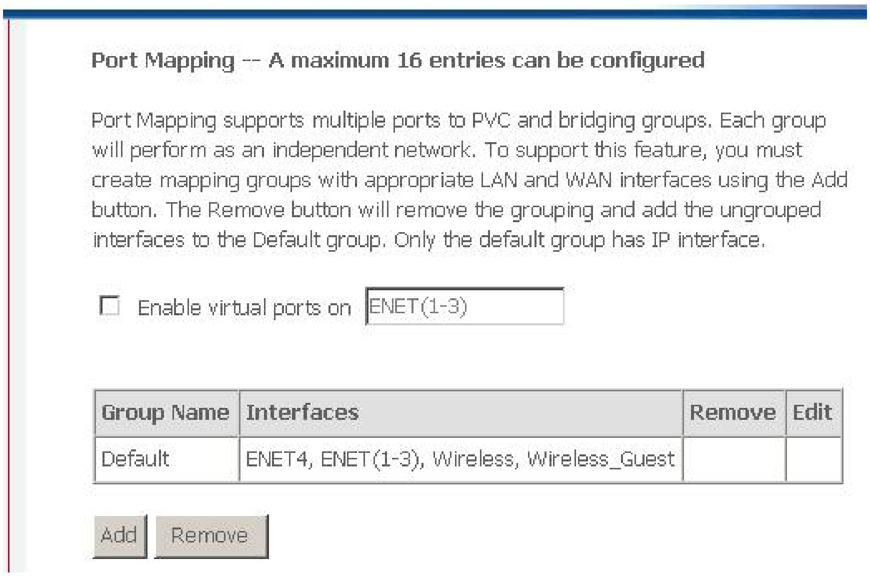
This page allows you to enable / disable printer support.

☐ Enable on-board print server.

4.9 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 independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.



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 independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

□ Enable virtual ports on ENET(1-3)

Group Name	Interfaces	Remove	Edit
Default	ENET4, ENET(1-3), Wireless, Wireless_Guest		

4.9.1 Port Mapping Configuration

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

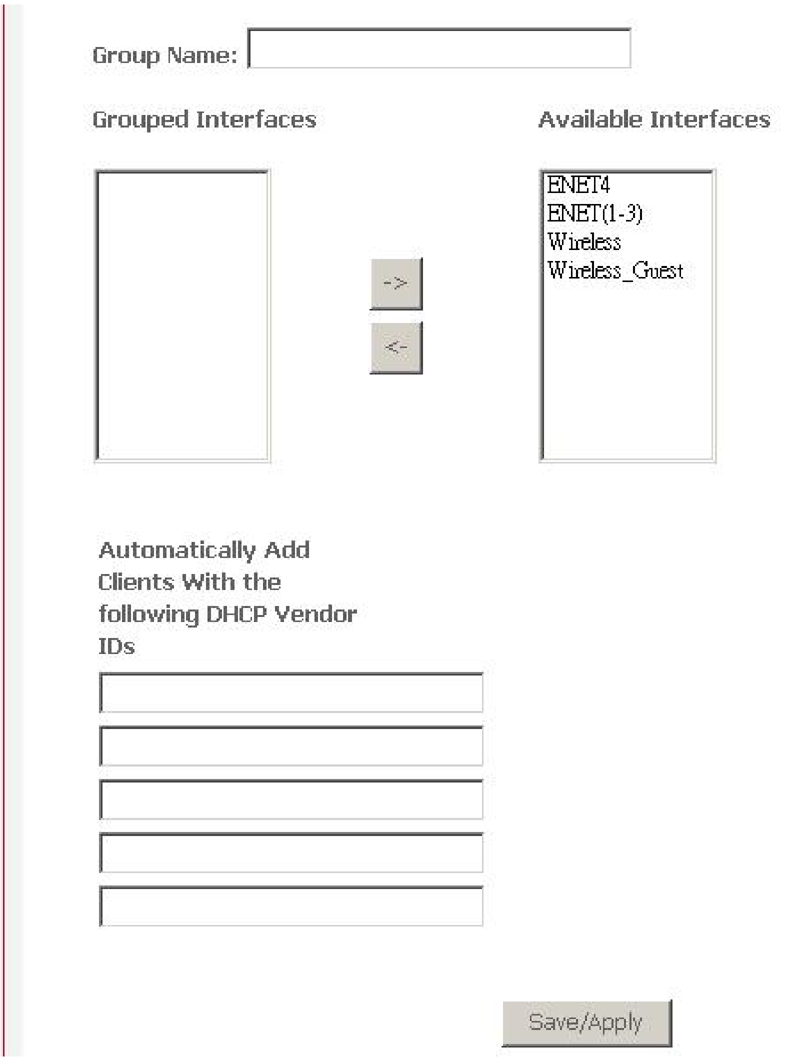
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

Note that these clients may obtain public IP addresses

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

Note that the selected interfaces will be removed from their existing groups and added to the new group.

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



Group Name:

Grouped Interfaces

Available Interfaces

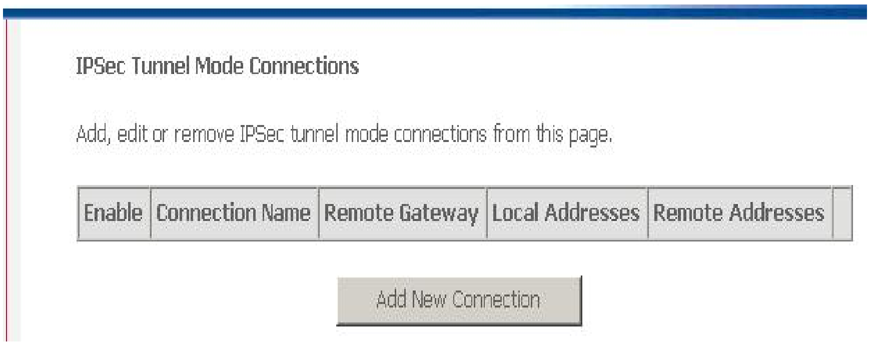
ENET4
ENET(1-3)
Wireless
Wireless_Guest

Automatically Add Clients With the following DHCP Vendor IDs

4.10 IPSec

Tunnel Mode Connections

Add, edit or remove IPSec tunnel mode connections from this page.

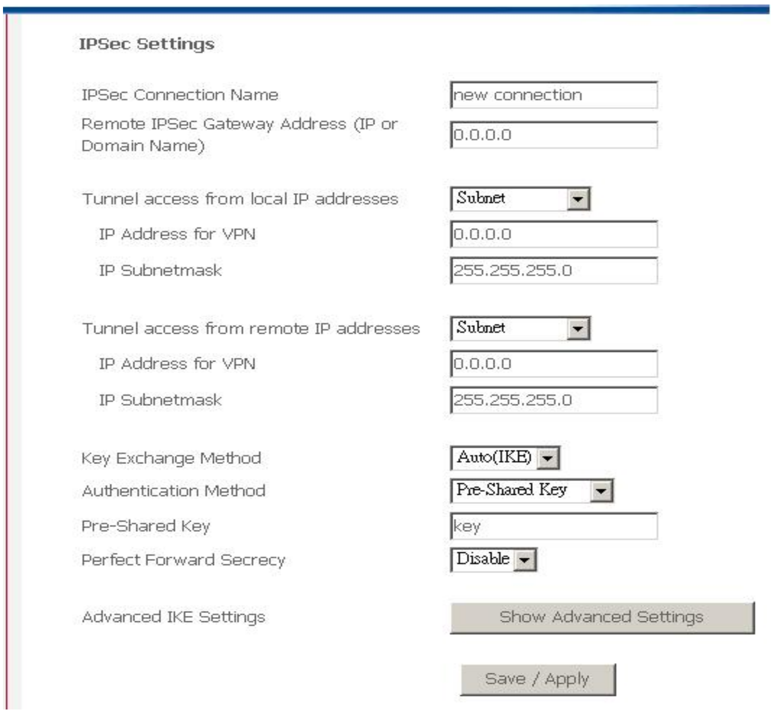


IPSec Tunnel Mode Connections

Add, edit or remove IPSec tunnel mode connections from this page.

Enable	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	

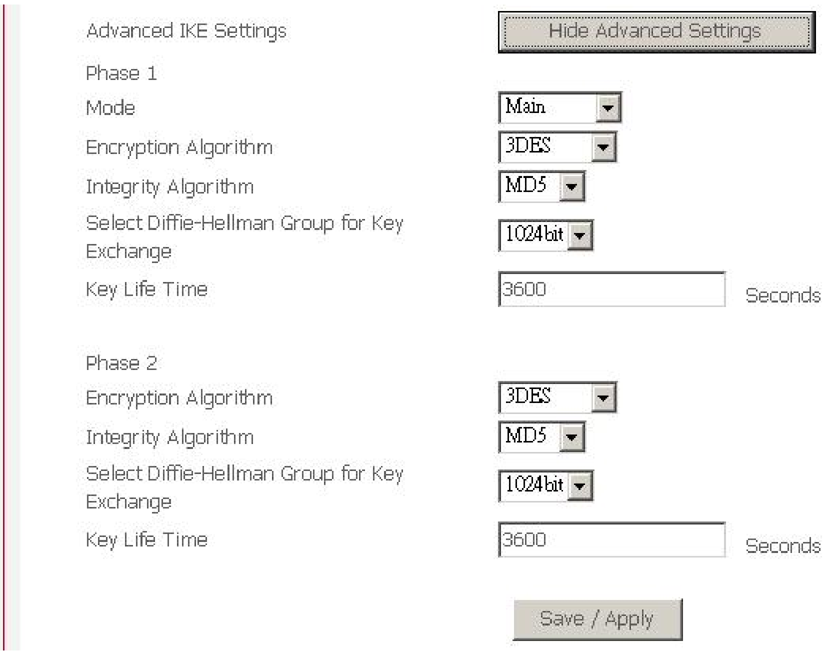
4.10.1 IPSec Settings



IPSec Settings

IPSec Connection Name	new connection
Remote IPSec Gateway Address (IP or Domain Name)	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings

4.10.2 Show Advanced Settings



Advanced IKE Settings

Phase 1

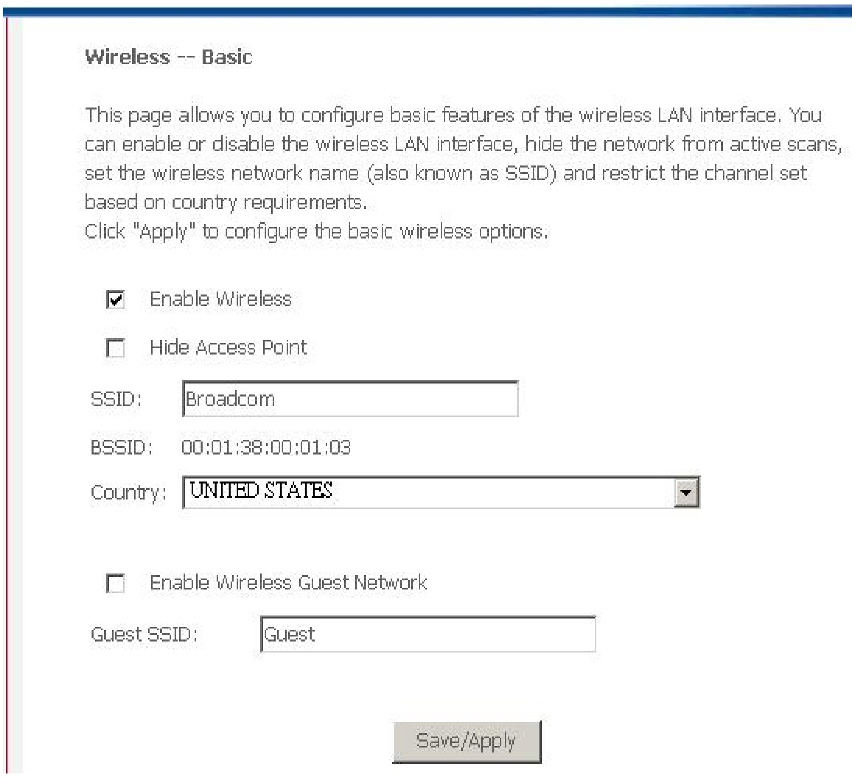
Mode	Main	
Encryption Algorithm	3DES	
Integrity Algorithm	MD5	
Select Diffie-Hellman Group for Key Exchange	1024bit	
Key Life Time	3600	Seconds

Phase 2

Encryption Algorithm	3DES	
Integrity Algorithm	MD5	
Select Diffie-Hellman Group for Key Exchange	1024bit	
Key Life Time	3600	Seconds

5. 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.



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: Broadcom

BSSID: 00:01:38:00:01:03

Country: UNITED STATES

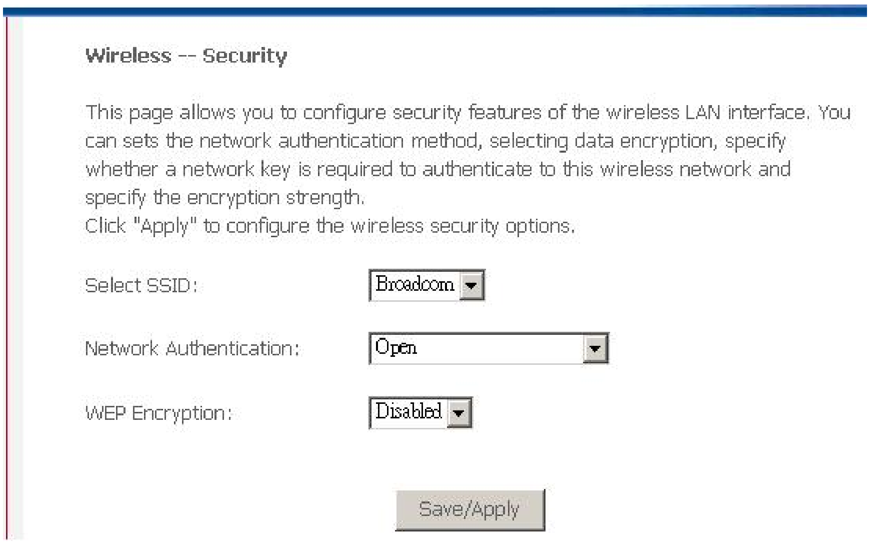
□ Enable Wireless Guest Network

Guest SSID: Guest

5.1 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.



Wireless -- Security

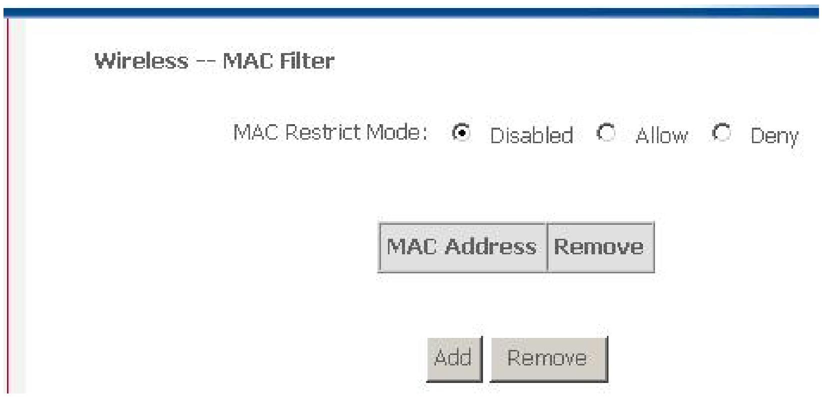
This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

Select SSID: Broadcom

Network Authentication: Open

WEP Encryption: Disabled

5.2 MAC Filter



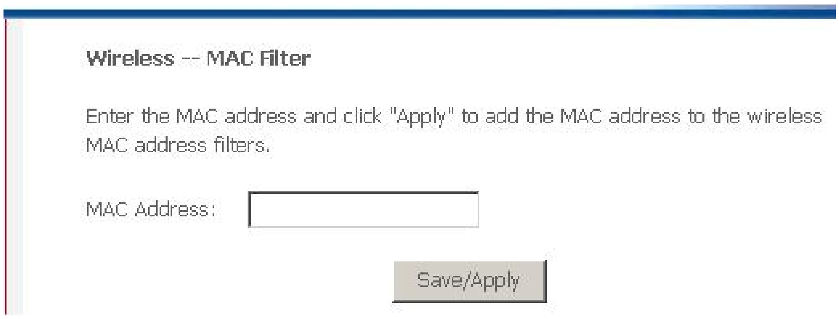
Wireless -- MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

5.2.1

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



Wireless -- MAC Filter

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

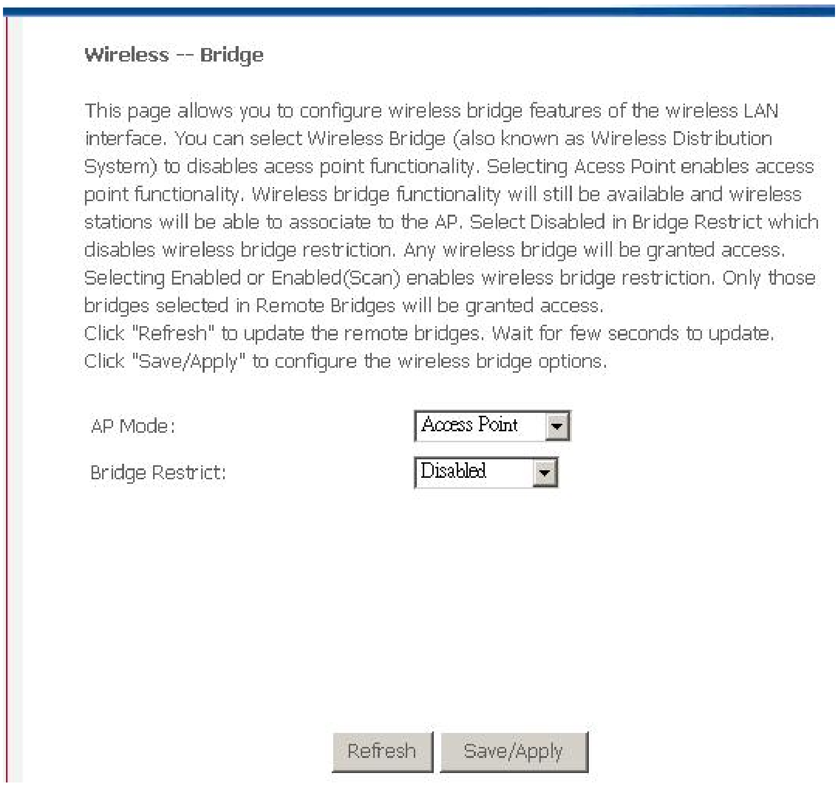
MAC Address:

5.3 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.



Wireless -- Bridge

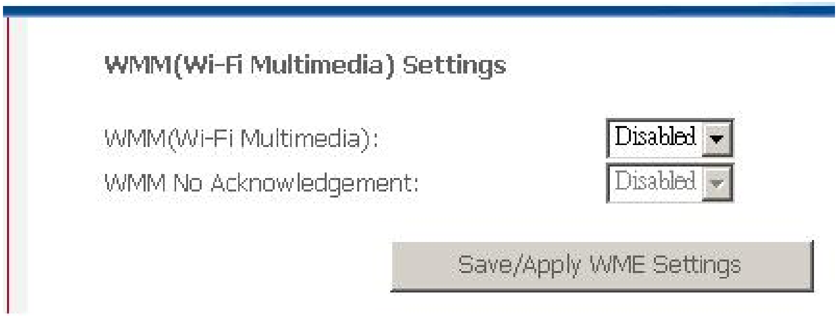
This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables acess point functionality. Selecting Acess Point enables access point functionality. Wireless bridge functionality will still 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

5.4 Quality of Service

WMM(Wi-Fi Multimedia) Settings



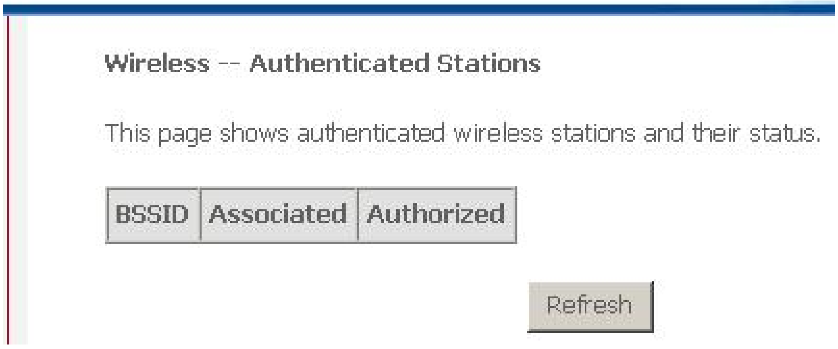
WMM(Wi-Fi Multimedia) Settings

WMM(Wi-Fi Multimedia): Disabled

WMM No Acknowledgement: Disabled

5.5 Station Info

Authenticated Stations



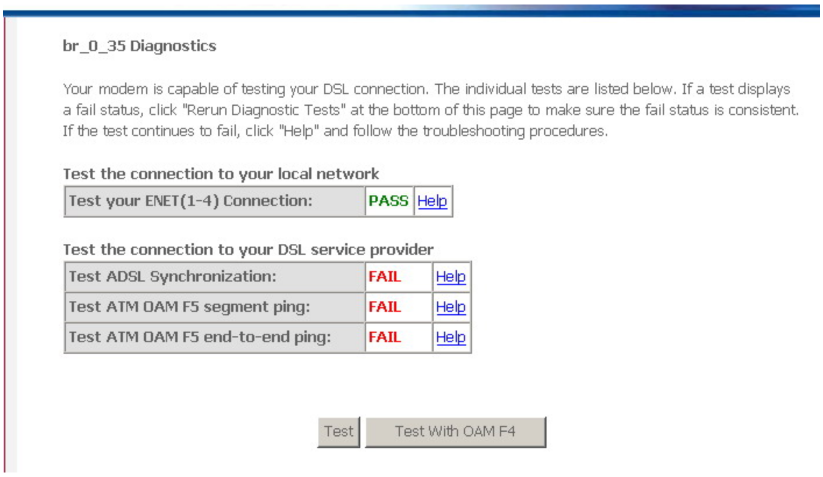
Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

BSSID	Associated	Authorized

6.Diagnostics

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



br_0_35 Diagnostics

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

Test the connection to your local network

Test your ENET(1-4) Connection:	PASS	Help

Test the connection to your DSL service provider

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

7.Management

The model supports 5 management setting. They are

1) Settings Backup
2) System Log
3) Access Control
4) Update Software
5) Save/Reboot

The sections below will describe these setting page by page.

7.1 Settings

When you click Settings, another 3 items will show up, there are

1) Backup

2) Update

3) Restore Default

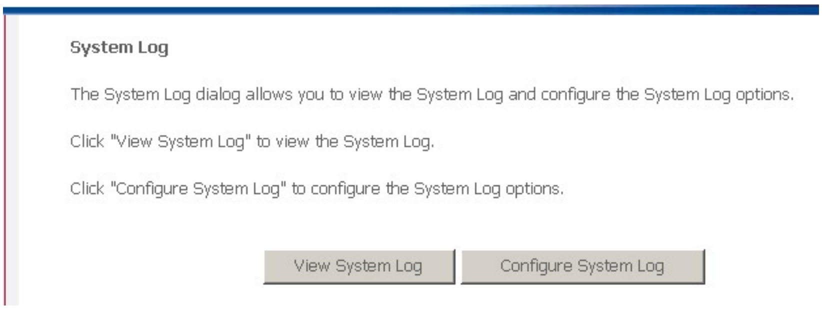
First one, the page "Backup" is used to backup DSL router configurations. You may save your router configurations to a file on your PC.

To access page "Update", this is use to update DSL router settings. You may update your router settings using your saved files.

To restore all setting to factory default, you can access page "Restore Default" to recovery all setting as factory initialised values.

7.2 System Log

To use System Log function, user must at first enable the feature by button "Configure Syslog". The page below will show up.

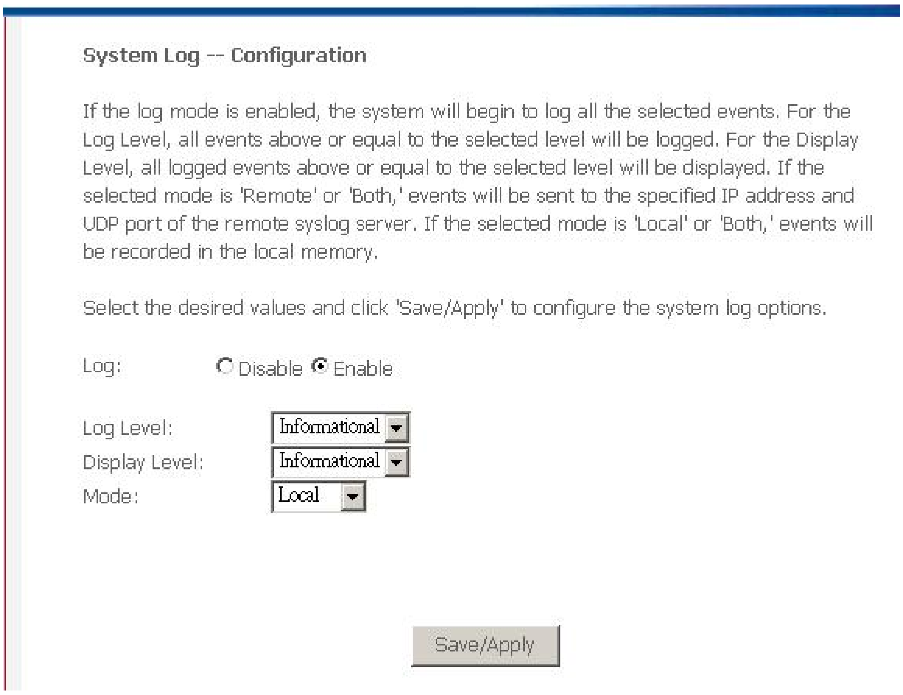


System Log

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.



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: Informational

Display Level: Informational

Mode: Local

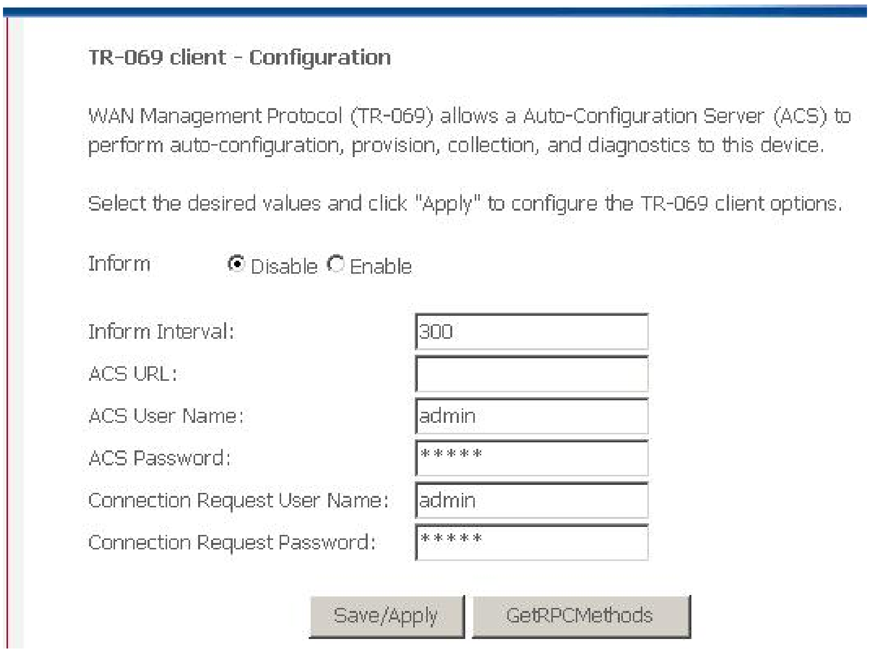
To check "Enable" to enable this function and choose Log Level, Display Level, Mode, then press "Save/Apply". Access "View System Log" to check the logged data on table.

7.3 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.



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:	*****

7.4 Internet Time

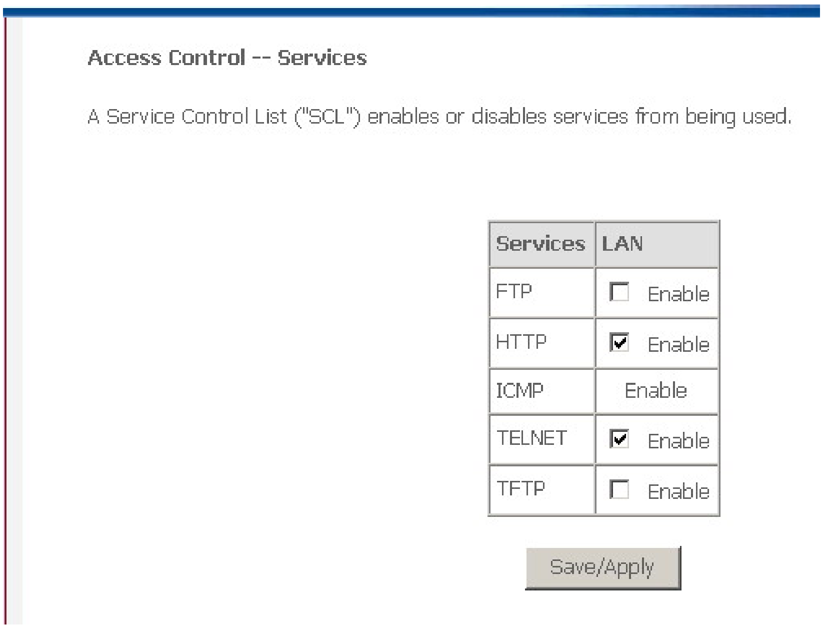
To check "Automatically synchronize with Internet time servers", two NTP server setting will show up for user to choose one of servers in list or assign by self.

"Time zone offset" must be assigned your time zone for your router/modem to get your real local time.

7.5 Access Control

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

Page "Service" is used to enable/disable the specified service such as FTP, HTTP, ICMP, TELNET and TFTP. User also can specify the service is from LAN to WAN or WAN to LAN.



Access Control -- Services

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

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

Page "IP address" is used to specify the permission of the local IP address to access web GUI and re-edit the configuration for the managed router/modem. If to leave it blank, then every LAN address can access the device.

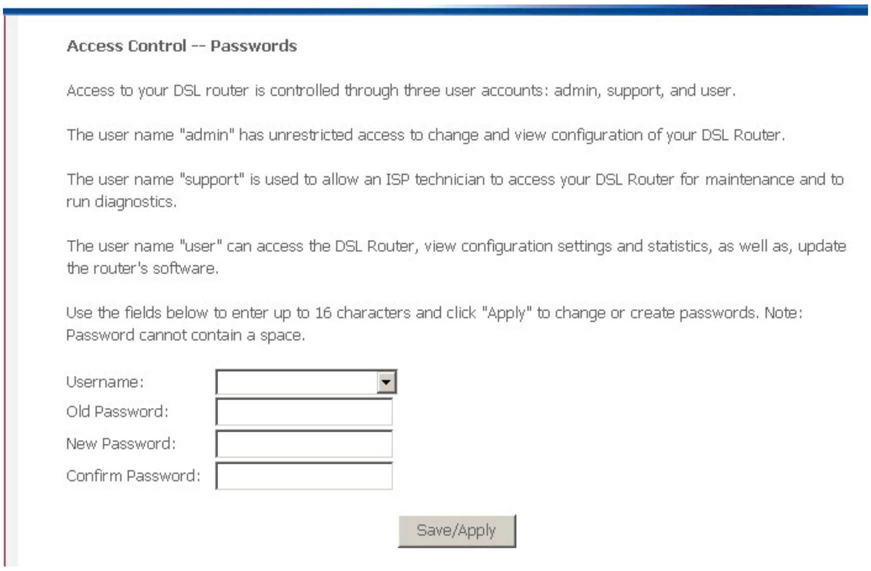
Page "Passwords", Access to your DSL router is controlled through three user accounts: admin, support, and user.

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.



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:

7.6 Update Software

You may easily upgrade ***X5668*** embedded software by obtaining the compressed upgrade kit from the service provider and then following the steps for upgrading through a Web-browser:

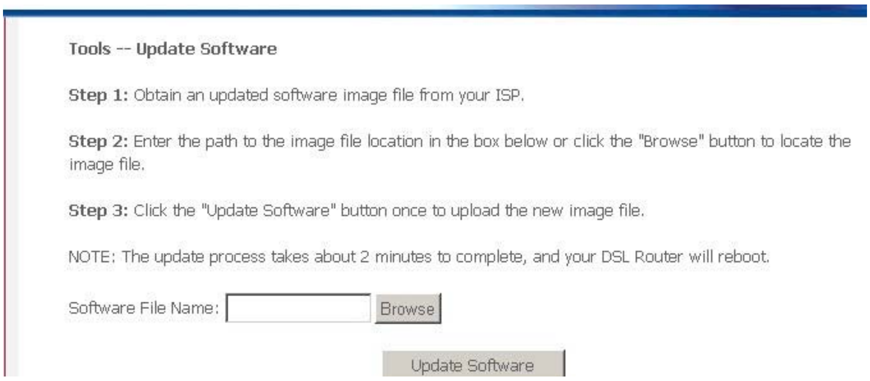
Step 1: Extract the ZIP file for updated firmware.

Step 2: Connect ***X5668*** via the local Ethernet port or remote ADSL link, making sure that the ***X5668*** Ethernet IP address and your terminal are properly configured so that you can successfully "*ping*" ***X5668***. The default local IP address is "192.168.1.1".

Step 3: Launch the Web browser (IE or Netscape), and enter the default IP address 192.168.1.1 into the address bar to access the Web management page.

Step 4: Click on the **Management** link on the navigation bar and then on the **Update Software** link below it.

Step 5: Click on the **Browse** to select the appropriate firmware and then click on the **Update Software** button. The upgrade process may take about 60 seconds. Do not reset the device while



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:

7.7 Save/Reboot

Click “Save/Reboot” button to store the setting before and reboot system to use the setting.

Chapter 3 Supplementary Services

3.1 Call Forward

3.1.1 Call Forward Unconditional

Call Forward Unconditional (CFU), this enables the customer to have all incoming calls, which are addressed to his number, forwarded to another number.

To configure CFU to any number :
Activation: * 21 * number #

Deactivation: # 21 #

For the duration that Call Forward Unconditional is enabled a stuttering dial tone shall be played instead of the normal dial tone when picking up the phone.

3.1.2 Call Forward No Response

Call Forward No Response (CFNR) enables the customer to have all incoming calls, which meet with no reply and are addressed to his number, forwarded to another number.

To configure CFNR to any number :
Activation: * 61 * number # (forwarding after 30 s)
or: * 61 * number * ss # where ss (5-60 s) is the time until forwarding
Deactivation: # 61 #

3.1.3 Call Forward on Busy

Call Forward Busy Subscriber (CFBS) enables the customer to have all incoming calls, which meet with busy and are addressed to his number, forwarded to another number.

To configure CFBS to any number :
Activation: * 67 * number #
Deactivation: # 67 #

3.2 Secret Number, Calling Line Identification Restriction (CLIR)

CLIR must work together with all bonus services. All calls origination from the subscriber in conjunction with services Call Forwarding, Enquiry service, CCBS and *69# must be marked secret for a subscriber with secret number.

3.2.1 Static Configuration

Secret Number is an extra service and customers are charged an additional monthly fee. It must be possible to provision from remote if CLIR is enabled or disabled for each call on the Analog Telephone Adapter (ATA).

3.2.2 On per call basis

Caller Line Identification Restriction (CLIR) enables a calling party to prevent presentation, on a call by call basis, of his number to the called party. This is in Sweden a regulatory requirement for an operator to provide.
Activation: # 31 # is dialed immediately before the called party number.

3.3 Call Waiting

Call Waiting (CW) enables a busy customer to be notified of a new incoming call that is in a waiting position. This feature must be provisioned to disabled. The customer has the choice to enable this service.

The customer then has the choice of accepting, rejecting or ignoring the waiting call, making use of switching orders based on R.

When the user presses R (hook flash) a new dial tone shall be sent to the customer.

3.3.1 Call Waiting customer configuration

Activation: * 43 #

Deactivation: # 43 #

Call Waiting is permanently enabled or disabled until disabled / enabled again. E.g. not on a per call basis. These setting shall survive a reboot, reconfiguration, software upgrade and any other imaginable actions that can be performed with the ATA.

3.3.2 Force Busy

To reject the new call without answering it: R (dial tone) 0. The CPE will send a Busy signal to the calling party.

R0 shall also temporarily deactivate the call waiting service for the rest of the active call. When the subscriber hangs up the service shall automatically be activated again.

3.3.3 Pickup and Release old

To release the old call and take the new call: R (dial tone) 1

3.3.4 Pickup and put old on hold

To place the old (current) call on hold and take the new call: R (dial tone) 2

3.3.5 Switch between 2 active calls

To switch between the old and the new call: R (dial tone) 2

3.3.6 Timeout

When the customer receives a call when in a conversation, and chooses to ignore the call waiting notification, the calling party will receive a Busy signal after 24 seconds.
R0 shall also temporarily deactivate the call waiting service for the rest of the active call. When the subscriber hangs up the service shall automatically be activated again.

3.4 Three Party Conference

Three party conference can be invoked from Call waiting or Enquiry services.
When the subscriber has two active calls, one on hold and

one in conversation state, it shall be possible to connect all three into a three party conference.

To connect to both the old and the new call: R (dial tone) 3

This shall not be possible in Call waiting state, i.e. before the subscriber has answered the waiting call. Both calls must be answered before they are connected into a conference.

When a three party conference is invoked the conference warning tone shall be sent to all three parties every 15 seconds throughout the call.

It must be possible for the controlling subscriber (the one invoking the service) to switch back to a two party state with one call on hold and one in conversation mode by R (dial tone) 2 in conference state. All other actions (R plus any other digit) shall be disregarded in this state.

If the controlling subscriber hangs up the calls are released immediately.
If any of the non-controlling subscribers hang up in conference state the disconnection rules for normal calls shall be followed, i.e. a calling subscriber is released immediately and a called subscriber is disconnected after 90 seconds

3.5 Call Transfer

The Call Transfer enables the customer to transfer the current call to another third party.
Procedure: When A and B are engaged in a call, if A wants to transfer the call to C, so B and C can make a conversation. A presses R and dial *90*Number#, when B hear the ring back tone, the call will be disconnected and A hears the reorder tone and hangs up the call. The call is transferred.

3.6 Enquiry service

The Enquiry service ENQ enables the customer to interrupt communications on an existing call, make a new call and then subsequently, switch between the old and new call, release one call or connect all three parties into a three party conference..

Procedure: Two parties are engaged in a call. One of the parties (the active party) places the other on hold by pressing R. The active party receives dial tone and makes a call to a new party. After the new party has replied, the active party may return to the old party by pressing R1 and switch between the old and new party by pressing R2. If the new party does not reply, the active party may stop the call attempt and return to the party on hold by pressing R.

3.7 Call Back Busy Subscriber (Busy)

Call Back Busy Subscriber (CCBS) enables a calling customer (A), encountering a busy destination (B), to have the retry dialing automatically until destination becomes idle, without having to make a new call attempt.

Activation: press 5 when encountering a busy tone
Deactivation: # 37 # deactivates all CCBS

The ATA shall reattempts the last made call every 60 seconds. The B Party alerts the original calling customer (A) with a ringing signal when the busy destination (B) becomes idle, if within 30 minutes. When the original calling customer answers, the former busy called party will start ringing. Timeout for call back ringing signal to A and B-side shall be 60 seconds. After the timeout both sides must be disconnected from the call.
B must have the possibility to make a new call before A answers the call back.

3.8 Call Back last number called (Call Return)

The customer has the possibility to press *69# to call back the last number that called. It is not possible to call secret numbers.

If the subscriber calling *69# has a secret number (CLIR) the A-number must be sent as secret number.

The call shall be made only with the user part of the stored FROM header toward the default proxy server. This call shall be screened through the dial plans to screen any call blocking functionality enabled.

Appendix A – Technical Specifications

Hardware

- **Local Interface**
  - Four 10/100 Base-T Ethernet ports in RJ-45 connector, comply with IEEE 802.3u
  - Integrated 802.11g WLAN Access Point with external antenna,

backward compatible with 802.11b

- **WAN Interface**
  - 2-wire loop with 100 ohms line impedance in RJ-11 connector
  - G.994 compliant
  - G.992.1 (G.dmt) – Annex A, B, and C compliant
  - G.992.2 (G.lite) – Annex A and C compliant
  - ANSI T1.413 compliant
  - G.992.3 (ADSL2) compliant, supporting Annex A, B, C, L and M
  - G.992.5 (ADSL2+) compliant, supporting Annex A, B, C and M
  - I.432 ATM physical layer compliant
- **Indicators**

Front panel (all LEDs in green color)

- **PWR** – ON when the power supply is properly connected.
- **WLAN** – Blinking while WLAN is transmitting data, and ON when WLAN port is active.
- **Ethernet-**
- **Internet-**
- **DSL-**

Rear panel

- Each Ethernet port got speed (10/100) and activity indicators.

- **OAM&P**
  - Through Web browser, remotely or locally
  - One hidden console port (RS-232) for maintenance
- **Environment**
  - Operation Temperature: 0°C ~ 45°C
  - Operation Humidity: 5% ~ 95% (non-condensing)
  - Storage Temperature: -20°C ~ +85°C
  - Storage Humidity: 5% ~ 95% (non-condensing)
- **Power**
  - AC adapter :Input 120 VAC/60Hz or 230VAC/50Hz; Output 12VDC 1A
  - Power consumption: Less than 15 watts
- **Physical Dimensions**
  - (W × D × H) t.b.d
- **Certificates**
  - CE, CB (TBD)

Software

ATM

- AAL0, AAL5, OAM, RM and Transparent cell types
- Traffic shaper/scheduler: priority scheduling; per-VCC queuing; UBR/CBR/VBR shaping based on Peak Cell Rate(PCR), Sustained Cell Rate (SCR), and Maximum Burst Tolerance; Minimum Cell Rate Shaping; Multi-priority AAL Queuing
- Full 24-bit Virtual Port Identifier (VPI)/Virtual Circuit Identifier (VCI) support
- 16 Virtual Channel Connections (VCCs)
- Payload Encapsulation:
  - RFC2684 / RFC1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5
  - RFC2225 / RFC1577, Classical IP and ARP over ATM (IPoA)
  - RFC2364, PPP over AAL5 (PPPoA)

Bridging

- RFC2684 / RFC1483 bridged PDU encapsulation
- Transparent bridging (IEEE 802.1D) with at least 32 MAC addresses
- Bridge filtering with per-port extensions

Routing

- RFC2684 / RFC1483 bridged and routed PDU encapsulations
- MAC Encapsulated Routing (MER)
- Support Point-to-Point Protocol (including PPPoA and PPPoE) and user authentication via PAP, CHAP or MS-CHAP
- Routing Information Protocol (RIP) v1 and v2, static route
- DHCP client, server and relay agent
- NAT / PAT – RFC1631 with support for extensive ALGs
- DNS relay

Firewall

- NAT: 16 sessions, DMZ and ALGs
- Stateful Packet Inspection (SPI) with DOS protection - Ping of Death, SYN Flood LAND
- Protection against IP and MAC address spoofing
- UPnP NAT traversal and VPN / IPSec pass-through

Wireless

- Supports 802.1x; WEP; WEP2; WPA; WPA2; TKIP; AES; 802.11i
- Hidden SSID
- WMM for advanced Quality of Service

- AES in hardware
- 125 High Speed Mode: Standards-plus performance enhancement delivers best real-world performance as the client card use the same 125 High Speed Mode

■ **Configuration and Network Management**

- SNMP GETs, SETs and TRAPs for four groups in MIB-II
- Embedded syslog; SNTP with DHCP options
- UPnP Internet Gateway Device (IGD) compliance
- Management and configuration via Web / HTTP
- Firmware upgrade using HTTP or TFTP
- Support TR-069 and with parameters: DeviceInfo, ManagementServer, Time, IPPingDiagonostic, etc
- Support TR-104

Note:

Not every listed feature will be included in the shipping product.

Appendix B – Warranties

B1. Product Warranty

XAVi Technologies warrants that the ADSL unit will be free from defects in material and workmanship for a period of twelve (12) months from the date of shipment.

XAVi Technologies shall incur no liability under this warranty if

- The allegedly defective goods are not returned prepaid to XAVi Technologies within thirty (30) days of the discovery of the alleged defect and in accordance with XAVi Technologies' repair procedures; or
- XAVi Technologies' tests disclose that the alleged defect is not due to defects in material or workmanship.

XAVi Technologies' liability shall be limited to either repair or replacement of the defective goods, at XAVi Technologies' option.

XAVi Technologies 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. XAVi 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, XAVi Technologies 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, XAVi Technologies 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. XAVi Technologies will ship surface freight. Expedited freight is at customer's expense.
2. The customer must return the defective product to XAVi Technologies within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, XAVi Technologies will bill the customer for the product at list price.

B3. Out-of-Warranty Repair

XAVi Technologies 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.

C2. IC CS-03 Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements as prescribed in appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, users should make sure that it is permissible to be connected to the facilities of the local telecommunications company. An acceptable method of connection must be used to install the equipment. The customer should be aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning: Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority or an electrician.

C3. 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.

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.xavi.com.tw for more information. We look forward to hearing from you!

WORLD HEADQUARTER
XAVi Technologies Corporation
9F, No. 129 Hsing Te Road, Sanchung City
Taipei County 241, Taiwan
Tel: +886-2-2995-7953 Fax: +886-2-2995-7954

USA BRANCH OFFICE
53 Parker
Irvine, CA 92618
Tel: +1-949-380-7550 Fax: +1-949-380-9204

S.AMERICA OFFICE
Tel: +55 -11-4485-3143

EUROPEAN BRANCH OFFICE
Oehleckerring 6B, 22419 Hamburg, Germany
Tel: +49-40-514400-53 Fax: +49-40-514400-79

5, Place de la Pyramide
Tour Ariane, La Defense 9
92088 Paris-La Defense Cedex
France
Tel 1: +33-1-55-68-11-08 Fax: +33-1-55-68-10-00
Tel 2: +33-1-55-68-11-09

CHINA SUBSIDIARY
Room 401, Floor 4, #608 ZhaoJiaBang Road,
Shanghai, 200031
Tel: +86-21-6431-8800 Fax: +86-21-6431-7885

Issued Date: October 10, 2006