

# *User Manual*

## *AR396*

*ADSL2+ Gateway with 4-port Ethernet Switch  
802.11b/g Wireless AP*

Issue 1.0  
31 July 2009

**XAVi Technologies Corporation**

Tel: +886-2-2995-7953

9F, No. 129, Hsing Te Road, Sanchung City,  
Taipei County 241,  
Taiwan

Copyright © 2009, XAVi Technologies Corporation

Information in this manual is subject to change without notice. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or scanning, for any purpose, without the written permission of XAVi Technologies Corporation.

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.

---

# Table of Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
	Features .....	1
	Device Requirements .....	2
<b>2</b>	<b>Getting to know the device .....</b>	<b>3</b>
	Parts Check.....	3
	Front Panel.....	4
	Rear Panel .....	5
<b>3</b>	<b>Connecting your device.....</b>	<b>6</b>
	Connecting the Hardware.....	6
	<i>Step 1. Connect the WAN port to ADSL network .....</i>	<i>7</i>
	<i>Step 2. Connect the Ethernet cable .....</i>	<i>7</i>
	<i>Step 3. Attach the power connector .....</i>	<i>7</i>
	<i>Step 4. Configure your Ethernet PCs.....</i>	<i>7</i>
	<i>Or, step 5. Install a Wireless card and connect Wireless PCs if the device is with wireless interface .....</i>	<i>7</i>
	<i>Next step.....</i>	<i>7</i>
<b>4</b>	<b>Getting Start with the Web pages .....</b>	<b>8</b>
	Accessing the Web pages.....	8
	Testing your Setup.....	10
<b>5</b>	<b>Device Information .....</b>	<b>11</b>
	Summary.....	11
	WAN.....	11
	Statistic.....	12
	Route .....	14
	ARP .....	14
	DHCP .....	14
<b>6</b>	<b>Advanced Setup.....</b>	<b>15</b>
	WAN .....	15
	<i>PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).....</i>	<i>17</i>
	<i>MAC Encapsulation Routing (MER).....</i>	<i>20</i>
	<i>IP over ATM (IPoA).....</i>	<i>21</i>
	<i>Bridging.....</i>	<i>21</i>
	LAN.....	22
	Ethernet Mode .....	23
	NAT (Network Access Translation).....	24
	<i>Virtual Server .....</i>	<i>24</i>
	<i>Port Triggering .....</i>	<i>25</i>

	DMZ .....	26
	Security .....	27
	IP Address Filter .....	27
	Parental Control .....	29
	Quality of Service .....	30
	Queue Configuration .....	31
	QoS Classification .....	32
	Routing .....	33
	Default Gateway .....	33
	Static Route .....	34
	Policy Routing .....	35
	RIP .....	36
	DNS .....	36
	DNS Server .....	36
	Dynamic DNS .....	37
	DSL .....	38
	Interface Grouping .....	38
	IPSec .....	40
	Certificate .....	41
	Local Certificates .....	41
	Trusted CA Certificate .....	43
<b>7</b>	<b>Wireless Setup .....</b>	<b>45</b>
	Basic .....	45
	Security .....	46
	MAC Filter .....	50
	Wireless Bridge .....	50
	Advanced .....	51
	Station Information .....	52
<b>8</b>	<b>Diagnostic .....</b>	<b>53</b>
	Diagnostic .....	53
<b>9</b>	<b>Management .....</b>	<b>54</b>
	Settings .....	54
	Backup .....	54
	Update .....	54
	Restore Default .....	55
	System Log .....	55
	SNMP Agent .....	56
	TR-069 Client .....	56
	Internet Time .....	58
	Access Control .....	58
	Service .....	58
	IP Address .....	59

<i>Password</i> .....	60
Update Software .....	60
Save / Reboot .....	61
<b>Appendix A - Configuring the Network Settings .....</b>	<b>62</b>
Configuring Ethernet (LAN) Card .....	62
<i>Before you begin</i> .....	62
<i>Windows XP PCs</i> .....	62
<i>Assigning static IP addresses to your PCs</i> .....	62
Configuring Wireless LAN card .....	63
<i>Wireless card and drivers</i> .....	63
<i>Configuring wireless device</i> .....	63
<b>Appendix B - Troubleshooting .....</b>	<b>64</b>
Troubleshooting Suggestions.....	64
IP Utilities for diagnostic.....	65
<i>Ping</i> .....	65
<i>Nslookup</i> .....	65
<b>Appendix C - Specification .....</b>	<b>67</b>
<b>Appendix D - Warranties .....</b>	<b>69</b>
<b>Appendix E - Contact information.....</b>	<b>70</b>

# 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.

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

This device complies with Part 15 of the FCC Rules.

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

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

## **FCC/IC Radiation Exposure Statement:**

This equipment complies with FCC/IC RSS-102 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.

Country Code selection feature to be disabled for products marketed to the US/CANADA

This Class **[B]** digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe **[B]** est conforme à la norme NMB-003 du Canada.

# 1 Introduction

Congratulations on becoming the owner of the **AR396** gateway. You will now be able to access the Internet using your high-speed connection.

The **AR396** is a gateway integrating ADSL2+, 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 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 **AR396** 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 (**AR396**) 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:

- ▶ High Speed Asymmetrical Data Transmission on Twisted Copper Pair Wire
- ▶ Service providers can deploy ADSL rapidly over existing wire infrastructure
- ▶ Integrates the phone filter
- ▶ Compatible and interoperable with most central office site ADSL DSLAM or Multi-service Access Systems.
- ▶ 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 for auto-provisioning and configuration.
- ▶ Upgradeable through HTTP (web browser)

## Device Requirements

---

In order to use the device, 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 in PC.



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.*




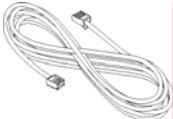
## 2 Getting to know the device

### Parts Check

---

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

- ▶ **The device (AR396)**
- ▶ **Ethernet cable**
- ▶ **Standard phone line cable**
- ▶ **Power adapter**

	AR396 device
	RJ-45 Cable
	RJ-11 Cable
	Power adapter

**Figure 1: Package Contents**

## Front Panel

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



**Figure 2: Front Panel and LEDs**

Connector and LED definitions from left to right:

Label	Color	Function
Power	Green or Red	Off : No power On (Green) : Power on On (Red): Self-test fails
Alarm	Red	On: DSL is not connected
LAN 1 ~ 4	Green	On : LAN link established and active Off : No LAN link Blink : Data being transmitted
WiFi	Green	On : WLAN service is enabled Off : WLAN service is disabled Blink : Data being transmitted
DSL	Green	On : Physical layer sync up successfully. Off : No connection or no signal Blink : Physical sync up progress
Internet	Green or Red	Off : No connection to Internet On (Green) : The device gets an IP address successfully in router mode Blink : Data being transmitted. On (Red) : PPP Authentication of the device failed. Or it can not get an IP address in ROUTER mode.

## Rear Panel

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



**Figure 3: Rear Panel Connections**

Connector definition:

Label	Function
Phone	Connects to phone set
Line	Connects to the ADSL line
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
Reset	A reset button to restart the device or reset to default settings: <ol style="list-style-type: none"> <li>1. Restart - Press the reset button for 1 second while the router is up and running.</li> <li>2. Reset to Default Settings - Press the reset button for 5 seconds while the router is up and running.</li> </ol>
Power Switch	ON/OFF switch
Power Jack	Connects to the supplied power adapter
Antenna	Connects to the 802.11b/11g enabled wireless devices in LAN

# 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

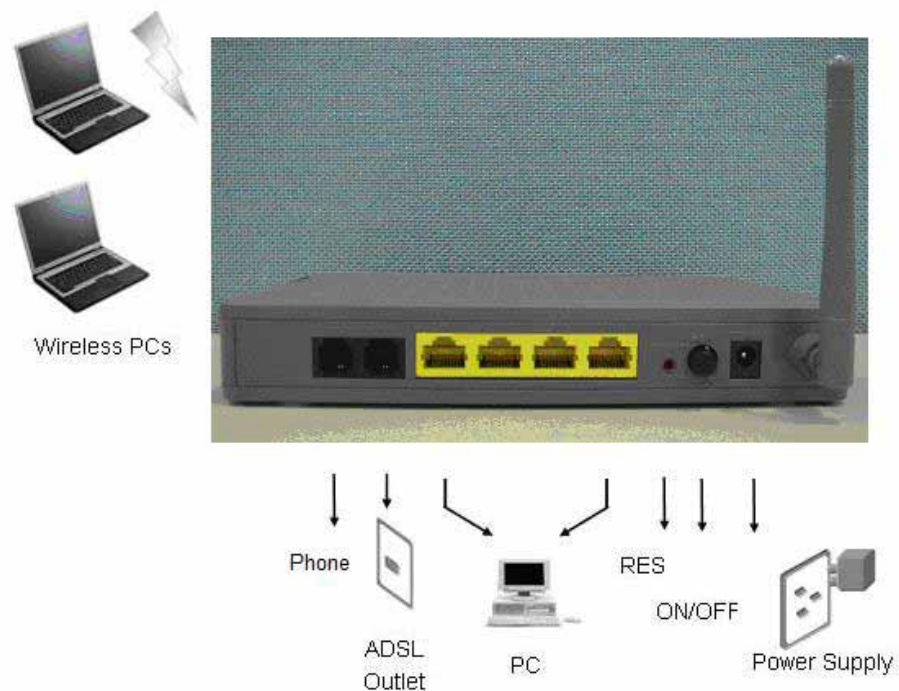
This section describes how to connect the device to the power outlet and your computer(s) or network.



**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**

**Step 1. Connect the WAN port to ADSL network**

Connect the WAN port to the DSL 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. 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-sensitive.



**Figure 5: Login Page**

The Menu comprises:

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

---

### Device Info

---

Summary

WAN

Statistics

Route

ARP

DHCP

**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, Ethernet Mode, NAT, Security, Parental Control, Routing, DNS, DSL, Interface Group, IPSec and Certificate.

### Advanced Setup

- WAN
- LAN
- Ethernet Mode
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- Interface Group
- IPSec
- Certificate

**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 and Station Info.

### Wireless

- Basic
- Security
- MAC Filter
- Wireless Bridge
- Advanced
- Station Info

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

### Diagnostics

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

### Management

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

## 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	Solid red to indicate that the device is turned on. If this light is not on, check the power cable attachment.
Wireless (WiFi)	Solid green to indicate that the Wireless LAN function is operational.
LAN	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.



# 5 Device Information

The Device Information web page menu includes the following submenus:

**Summary**

**WAN**

**Statistics**

**Route**

**ARP**

**DHCP**

## Summary

---

The Summary Page of the device shows the following information, Firmware version, Product name, Serial number, Hardware version, Software version, Bootloader version,, Wireless driver version, and MAC address. Besides, LAN IP, Default gateway, Primary DNS server and Secondary DNS server are shown too.

### Device Info

ZHONE Firmware:	01.00.03
Produce Name:	6219-X1-xxx
Serial Number:	0123456789
Hardware Version:	
Software Version:	3-12-01-30113_3.01ZHT13.A2p8025c1.d20k_rc2
Bootloader (CFE) Version:	1.0.37-12.5.0
Wireless Driver Version:	4.174.64.19.cpe1.1sd
LAN MAC Address:	00:01:38:03:05:08

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
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, VLAN Mux., UBR/CBR/VBR and so on), Protocol,

IGMP enabled or disabled, QoS enabled or disabled, WAN port state, DSL link status, and IP address of WAN port.

## WAN Info

Port/VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IPv4 Address
0/0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Enabled	Disabled	Enabled	DSL 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, and ADSL.

## Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	4275302	35994	0	0	17473318	37588	0	0
Wireless	0	0	0	0	0	0	0	0

Reset Statistics

**Figure 8: Device LAN Port Statistic Information**

## Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted				
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	
pppoe_0_0_35_1	0/0/35	PPPoE	ppp_0_0_35_1	0	0	0	0	0	0	0	0	0

Reset Statistics

**Figure 9: Device WAN Port Statistic Information**

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

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

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

Figure 10: Device ATM Statistic Information

Statistics -- ADSL

Mode:		
Type:		
Line Coding:		
Status:	Link Down	
Link Power State:	LO	
	<b>Downstream</b>	<b>Upstream</b>
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:		

Figure 11: Device ADSL 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 12: 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
192.168.1.44	Complete	00:0C:76:C4:D1:2F	br0

**Figure 13: Device ARP Table Information**

## DHCP

---

The DHCP Page of the device shows the DHCP table which DHCP server of device assigns the IP address to the PC requesting an IP address. The DHCP table contains Hostname, MAC address, IP address and Expires In.

### Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

**Figure 14: Device DHCP Table Information**

# 6 Advanced Setup

The Advance Setup menu includes the sub menus WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Interface Group, IPSec and Certificate.

**WAN**

**LAN**

**Ethernet Mode**

**NAT**

**Security**

**Parental Control**

**Quality of Service**

**Routing**

**DNS**

**DSL**

**Interface Group**

**IPSec**

**Certificate**

## WAN

---

You can configure your internet connection from this page. This page displays the details of existing internet connection. Please refer below for more details. There are three connection types can be configured including PPP over Ethernet (PPPoE), IP over Ethernet, and Bridging.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Enabled	Disabled	Enabled	<input type="checkbox"/>	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]   
 VCI: [32-65535]

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 - ATM PVC 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 Quality of Service if Service Category is UBR without PCR, UBR 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
- UBR With PCR
- CBR
- Non Realtime VBR
- Realtime VBR

**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**

LLCSNAP-BRIDGING ▾

Back Next

**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 Bridging.
- ▶ 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, enter the user name and password that your ISP has provided to you.

PPP Username:   
 PPP Password:   
 PPPoE Service Name:   
 Authentication Method: **AUTO** ▾  
 PPP MTU [128-1492]:

Dial on demand (with idle timeout timer)  
 Inactivity Timeout (minutes) [1-4320]:

PPP IP extension  
 Use Static IP Address  
 IP Address:

Retry PPP password on authentication error  
 Enable PPP Debug Mode  
 Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

Back Next

**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* (AUTO, PAP, CHAP, or MSCHAP) used during negotiation, default is AUTO.
- ▶ Enter the PPP MTU (Maximum Transmission Unit) size between 128 and 1492. Default is 1492.
- ▶ 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.
- ▶ 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 Fullcone NAT

Public IP of NAT:

Enable Firewall

#### Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

#### Enable MAC Clone

Enable MAC Clone

**Figure 20: WAN Service, PPPoA or PPPoE NAT Configuration**

Network Access Translation (NAT), IGMP Multicast and MAC Clone settings:

- ▶ Check to enable *NAT* feature which allows multiple PCs to surf Internet simultaneously with one public WAN port IP address.
- ▶ Check to enable *Fullcore NAT* if necessary



- ▶ Select the *Public IP of NAT* from Interface IP address or Manual IP address. If it is manual IP address, enter the associated IP address.
- ▶ Check to enable Firewall feature
- ▶ 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.
- ▶ Check to enable *MAC Clone* feature and enter the associated MAC address.
- ▶ 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.

PORT / VPI / VCI:	0 / 0 / 38
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Quality Of Service:	Enabled

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 Summary, PPPoA or PPPoE Configuration**

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

## MAC Encapsulation Routing (MER)

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 IPv4 Address:   
 WAN Subnet Mask:

Obtain default gateway automatically  
 Use the following default gateway:  
 Use IPv4 Address:   
 Use WAN Interface:

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 to set the NAT, IGMP multicast and MAC Clone settings, please refer above descriptions in PPPoE configuration for details.

The page of Network Address translation (NAT), IGMP multicast and MAC Clone settings will show up and then 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. with static values will disable the automatic assignment from other WAN connection.

WAN IP Address:

WAN Subnet Mask:

Use the following default gateway:

Use IP Address:

Use WAN Interface:

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 page of Network Address translation (NAT), IGMP multicast and MAC Clone settings will show up and then *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:

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

IP Address:   
 Subnet Mask:

- Enable UPnP
- Enable IGMP Snooping
- Standard Mode
- Blocking Mode

Disable DHCP Server

Enable DHCP Server

Start IP Address:   
 End IP Address:   
 Subnet Mask:   
 Leased Time (hour):

Static IP Lease List: Please click on Save/Reboot button to make the new configuration effective. (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="button" value="Add Entries"/>	<input type="button" value="Remove Entries"/>	

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 *Disable 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* in 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.
- ▶ Click *Add Entries* button to add IP address excluded in the IP pool.

**DHCP Static IP Lease**

Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address:

IP Address:

**Figure 26: LAN DHCP Static IP Lease Configuration**

- ▶ Enter the MAC address and static IP address which a dedicated PC uses this fixed IP address already. This IP address will be excluded from the IP pool. Click Apply/Save to save configuration.
- ▶ Check to *Enable DHCP Server Relay* and then input the IP address of DHCP server.
- ▶ The device can handle second IP address and subnet of LAN interface. You may check this feature to configure the second IP address and subnet for LAN port to meet your LAN environment.
- ▶ Click *Save* to save the configuration

## Ethernet Mode

The Ethernet Mode feature provides to configure the connection speed of each Ethernet port of switch. Besides, the connection status will be shown too.

Port No.	Speed	Status
1	auto	Disconnected
2	auto	100Mbps Full Duplex
3	auto	Disconnected
4	auto	Disconnected

**Figure 27: Ethernet Mode Configuration**

Global settings:

- ▶ Select the LAN port connection speed of each Ethernet port of switch from the list, AUTO, 100Full, 100Half, 10Full or 10Half. 100Full means 100Mbps full duplex and 100Half means 100Mbps half duplex.
- ▶ 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, and DMZ 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	Remote Host	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	-------------	--------

**Figure 28: 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:

Custom Server:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote ip
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

**Figure 29: 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.
- ▶ Enter the *Remote IP address* to allow the specified IP packet coming through virtual server only.
- ▶ 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 30: 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 *Server IP Address* located in the LAN to provide the service to remote party
- ▶ 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 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:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

**Figure 31: Add A Rule Of Port Triggering**

**DMZ**

A DMZ (De-Militarized Zone) host is a computer on your network that can be accessed from the Internet. The de-militarized 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 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:

**Figure 32: Add A Rule Of Port Triggering**

**Global Setting**



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

## Security

The Security feature provides two more setting pages including 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
<input type="button" value="Add"/> <input type="button" value="Remove"/>						

**Figure 33: 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 34: 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
<div style="display: flex; justify-content: center; gap: 10px;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>							

**Figure 35: 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
- pppoe\_0\_0\_38\_1/ppp\_0\_0\_38\_1

**Figure 36: 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*

**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 37: 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

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

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Save/Apply
------------

**Figure 38: 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*.

## Quality of Service

---

The Quality of Service feature provides a method to prioritize the packet and arrange a better efficiency of bandwidth. In other words, some traffic such as voice or video has handled as higher priority than others such as data to get near real time response.

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

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

Enable QoS

Select Default DSCP Mark

Apply/Save

**Figure 39: Quality of Service Configuration**

### Global Setting

- ▶ Check Enable QoS (Quality of Service)
- ▶ Select "Default DSCP Mark" from the list if the egress packets that do not match any classification rules.
- ▶ Click Save/Apply

## Queue Configuration

You could configure a maximum 16 QoS queues to provide different service levels.

QoS Queue Configuration -- A maximum 24 entries can be configured.

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

Interfacename	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1		
wireless	WMM Voice Priority	2	2		
wireless	WMM Video Priority	3	3		
wireless	WMM Video Priority	4	4		
wireless	WMM Best Effort	5	5		
wireless	WMM Background	6	6		
wireless	WMM Background	7	7		
wireless	WMM Best Effort	8	8		

**Figure 40: Quality of Service Queue Configuration**

Click *Add* to add a class of Quality of Service.

The screen allows to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be user by the classifier to place ingress packets appropriately. Note: lower integer values for precedence imply higher priority for this queue relative to others.

Queue Configuration Status:

Queue:

Queue Precedence:

**Figure 41: Add a QoS Queue**

### Global Setting

- ▶ Select Enable or Disable for *Queue Configuration Status*
- ▶ Select the *queue* attaching to a specific network *Interface*
- ▶ Select the *Queue Precedence* (1, 2, 3), lower integer values for precedence imply higher priority for this queue relative to others.
- ▶ Click *Save/Apply* to save it.

## QoS Classification

You need to define one or more *classes* of data traffic and set the priority for each of classes. A maximum 32 entries can be configured.

Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

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

MARK				TRAFFIC CLASSIFICATION RULES													
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Order	Enable/Disable	Remove	Edit

**Figure 42: Quality of Service Classification Setup**

Click *Add* to add a class of Quality of Service.

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

Click *Edit* to edit the entry.

Traffic Class Name:

Rule Order:

Rule Status:

**Assign ATM Priority and/or DSCP Mark for the class**  
 If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the corresponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

**Specify Traffic Classification Rules**  
 Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

**SET-1**

Physical LAN Port:

Protocol:

Differentiated Services Code Point (DSCP) Check:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

**SET-2**

802.1p Priority:

**Figure 43: Add a Quality of Service Classification**

The screen creates a traffic class rule to classify the traffic, assign queue priority which defines the precedence and type of service. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

#### Global Setting

- ▶ Enter the *Traffic Class Name*
- ▶ Select the *Rule Order* and *Rule Status* (enable or disable) from the list
- ▶ Select the *Assign Classification Queue* from the list.
- ▶ Select the *Assign Differentiated Services Code Point (DSCP) Mark* from the list.
- ▶ Select the *802.1p mark level* from the list if 802.1q is enabled.
- ▶ Select the *Physical LAN port*
- ▶ Select the *Protocol of packet*
- ▶ Select the *Differentiated Service Code Point (DSCP) Check* from the list.
- ▶ Select the *IP address*, *Vendor Class ID* (DHCP option 60), or *User class ID* (DHCP option 77) and enter the associated value.
- ▶ Enter *Source Subnet Mask* and *UDP/TCP Source Port* (single port or port range)
- ▶ Enter *Destination IP address* and *Destination Subnet mask*
- ▶ Enter *Source MAC address*, *Source MAC Mask*, *Destination MAC address* and *Destination MAC mask*.
- ▶ Select *802.1p priority* from the list.
- ▶ Click *Apply* to add this QoS class

## 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 and Static Route.

### 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

Save/Apply

**Figure 44: 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
<input type="button" value="Add"/> <input type="button" value="Remove"/>				

**Figure 45: Static Route Configuration**

Click Add to add the static route path.

Destination Network Address:

Subnet Mask:

Use Gateway IP Address

Use Interface

**Figure 46: 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



## Policy Routing

Policy Routing Setting -- A maximum 8 entries can be configured.

Policy Name	Source Interface	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Gateway Address	Gateway Interface	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>									

**Figure 47: Policy Routing Configuration**

Click Add to add the static route path.

### Routing -- Policy Route Add

Enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.  
Note: If selected "MER" as WAN interface, gateway IP address must be configured.

Policy Name:

Source Interface:

Protocol:

Source IP Address:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

Gateway IP Address:

Gateway Interface:

**Figure 48: Add Policy Route Configuration**

### Global Setting

- ▶ Enter the *Policy Name*
- ▶ Select the *Source Interface* (LAN1 to 4 and Wireless) from the list
- ▶ Select the *Protocol* (TCP/UDP, TCP, IP and ICMP) from the list
- ▶ Enter the *Source IP Address* and *Source Subnet Mask*
- ▶ Enter the *Source Port Number* (single port or port range)
- ▶ Enter the *Destination IP Address* and *Destination Subnet Mask*
- ▶ Enter the *Destination Port Number* (single port or port range)
- ▶ Enter the *Gateway IP Address* and select the *associated Gateway WAN Interface* from the list.
- ▶ Click *Save* to save the configuration

## RIP

Global RIP Mode  Disabled  Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	<input type="checkbox"/>
ppp_0_0_35_1	0/0/35	2	Passive	<input type="checkbox"/>

**Figure 49: RIP Configuration**

### Global Setting

- ▶ Check to enable or disable *Global RIP mode*
- ▶ 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

The RIP can not be configured if the WAN interface has NAT enabled.

## DNS

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

### DNS Server

You could configure to get the IP address of DNS server automatically or set the IP address of DNS server manually.

#### 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

Primary DNS server:

Secondary DNS server:

**Figure 50: DNS Server Configuration**

### Global Setting

- ▶ Check to *Enable Automatic Assign DNS* or enter IP address of *Primary DNS server/Secondary DNS server* manually.
- ▶ Click *Save/Apply* 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.



**Figure 51: 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

Hostname

Interface

**DynDNS Settings**

Username

Password

**Figure 52: 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*
- ▶ 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 53: 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.

## Interface Grouping

The page provides Interface Grouping configuration. In default, the LAN1 to LAN4 and wireless grouped together as a single Ethernet environment. Interface grouping supports multiple LAN ports to PVC and bridging groups. Only bridged-WAN interface will show on this page. Each bridging group will perform as an independent network.

### Interface Group -- A maximum 16 entries can be configured

Interface Group 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

Group Name	Remove	Edit	Interfaces
Default			LAN1
			LAN2
			LAN3
			LAN4
			Wireless(SSID1)

**Figure 54: Interface Grouping Configuration**

Click *Add* to add a new Interface group setting. Check *Remove* and click *Save/Apply* button to remove the specified entry. Click *Edit* button to edit current settings.

To create (add) a new interface group:

Group Name:

Grouped Interfaces

Available Interfaces

LAN1  
LAN2  
LAN3  
LAN4

->  
<-

Automatically Add Clients  
With the following DHCP  
Vendor IDs

Save/Apply

**Figure 55: Create New Interface Group Configuration**

#### Global Setting

- ▶ Enter the *Group Name*.
- ▶ Select the *Interfaces* from the available interface list and add it to the grouped interface list using the arrow buttons to create required mapping of the ports. The selected 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. If a vendor ID is configured for a specified client device, please reboot the client device attached to the modem to allow it to obtain an appropriate IP address.
- ▶ Click *Save/Apply* to save the configuration.

## IPSec

The page provides IPSec VPN configuration to establish a VPN tunnel.

### IPSec Tunnel Mode Connections

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

Enable	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	
<input type="checkbox"/>	new connection	0.0.0.0	192.168.4.1	192.168.4.100	<input type="button" value="Edit"/> <input type="button" value="Remove"/>

**Figure 56: IPSec VPN Configuration**

Check the *Enable* box to enable this IPSec tunnel.

Click *Add New Connection* to create a IPSec VPN profile. Click *Edit* button to edit the current settings, click *Remove* button to remove the IPSec VPN profile.

### IPSec Settings

IPSec Connection Name	<input type="text" value="new connection"/>
Remote IPSec Gateway Address	<input type="text" value="0.0.0.0"/>
Tunnel access from local IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Tunnel access from remote IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Key Exchange Method	<input type="text" value="Auto(IKE)"/>
Authentication Method	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key	<input type="text" value="key"/>
Perfect Forward Secrecy	<input type="text" value="Disable"/>
Advanced IKE Settings	<input type="button" value="Show Advanced Settings"/>
	<input type="button" value="Save / Apply"/>

**Figure 57: IPSec VPN Settings**

### Global Setting

- ▶ Enter *IPSec Connection Name*
- ▶ Enter the *IP address of remote IPSec Gateway*
- ▶ Select *Tunnel access from local IP address*: subnet or single IP address
- ▶ Enter the local *IP address of VPN tunnel*
- ▶ Enter the local *IP subnet mask*
- ▶ Select the *Key exchange method*: IKE or Manual

- ▶ Select the *Authentication Method*: Pre-shared Key or Certificate (X.509)
- ▶ Enter the *Pre-shared key* if chooses Pre-shared key as the authentication method
- ▶ Select to enable or disable the *Perfect Forward Secrecy*.
- ▶ Click Show Advanced Settings for more settings.

Advanced IKE Settings

Hide Advanced 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

**Figure 58: IPsec VPN Advanced Settings**

- ▶ There are two phases in advanced settings. There are five parameters in phase 1 and four parameters in phase 2.
- ▶ Select *Mode* from the list in phase 1: Main or Aggressive
- ▶ Select *Encryption Algorithm* from the list in phase 1 and 2: DES, 3DES, AES-128, AES-192, AES-255
- ▶ Select *Integrity Algorithm* in phase 1 and 2: MD5 or SHA1
- ▶ Set *Diffie-Hellman Group* in phase 1 and 2 for Key Exchange
- ▶ Enter the *Key life time* in phase 1 and 2 to change the key again.
- ▶ Click *Save/Apply* to save the configuration

## Certificate

The page provides the Certificate configuration. There are two sub-menu (Local and Trusted CA) are provided. “Local” means local certificates and “Trusted CA” means trusted certificate Authority certificates. Local Certificates preserve the identity of the modem. CA certificates are used by the device to verify certificates from the other hosts.

### Local Certificates

Local certificates are used by peers to verify your identity.

#### Local Certificates

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

Name	In Use	Subject	Type	Action
<input type="button" value="Create Certificate Request"/> <input type="button" value="Import Certificate"/>				

**Figure 59: Local Certificate Configuration**

Click *Create Certificate Request* to generate a certificate.  
 Check *Import Certificate* to get a certificate from file.

**Create New Certificate Request:**

Create new certificate request

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

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

**Figure 60: Create New Certificate Request**

**Global Setting**

- ▶ Enter *Certificate Name*, *Common Name*, *Organization Name*, and *State/Province Name*.
- ▶ Select *Country/Region Name* from the list.
- ▶ Click *Apply* to create new certificate request. The generated certificate will be shown as below.

**Certificate signing request**  
 Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	Test
Type	request
Subject	CN=Test/O=Xavi/ST=CA/C=US
Signing Request	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBdzCB4QIBADA4MQU0wCwYDVQQDEwRUZXRhbnR1eXN0b290wCwYDVQQKEwRYYXZpMQswCQYD VQQIEwJDTQTELMakGA1UEBhMCVWVmgZ8wDQYJKoZIhvcNAQEBBQADgV0AMIGJAoGB AM6Fw8Bm5zka8bkTfYjTZVNL8WOKxBDcVuoAaccelelnHoZo7zY4SDdp+urDyfo UV/TriMwpb6Up1TlQJ3YO2d44e9jY/JCQrxkkti5pgdo+pkCWdBtUuVdsZt0DH5B Z7W26hqe7buCbB91h3sKi6uA98yRVWtWNmeK5/TAKzBhAgMBAAGgADANBgkqhkiG 9w0BAQQAFAA0BgQAEg/ tTNx5rb33FqKrRrZKH6KJ5i rqv3TgkHJDagV+9qzNgKo gV5hPkaAos0EuTPbGCvOmj 1P7J oKA5WmumoWYA9ucakdndfdj3k48pIoQGfKfu0 Eg1HNbTW7Ah1A7TKiGeL+gt103rUJjvzkl0RGS+9qoeLKT4fkPuTDAYGA= -----END CERTIFICATE REQUEST-----                     </pre>

**Figure 61: Generated Certificate**

The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into modem. Click "Load Signed Certificate" button to load the certificate and then a new certificate is created.



### Import Certificate:

Import certificate  
 Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate: 

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

Private Key: 

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

**Figure 62: Import Certificate**

#### Global Setting

- ▶ Enter *Certificate Name*
- ▶ Enter the *Certificate* and *Private Key*
- ▶ Click *Apply*

### Trusted CA Certificate

CA (Certificate Authority) is used by you to verify peer's certificate. It can be imported only.

#### Trusted CA (Certificate Authority) Certificates

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

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

**Figure 63: Trusted CA (Certificate Authority) Certificates Configuration**

Click Import Certificate to set certificate.

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

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

Certificate:

**Figure 64: Import CA Certificate**

Global Setting

- ▶ Enter *Certificate Name*.
- ▶ Enter the *Certificate*.
- ▶ Click *Apply*.

# 7 Wireless Setup

The Wireless Setup web page menu comprises:

**Basic**

**Security**

**MAC Filter**

**Wireless Bridge**

**Advanced**

**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).

### 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
- Disable Wireless When DSL Line is Down
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise

SSID:

BSSID:

Max Clients:

**Figure 65: Wireless Setting – Basic**

### Global Setting

- ▶ Check to enable *Wireless feature*
- ▶ Check to *disable Wireless feature when DSL line is down*
- ▶ Check to enable *Hide Access Point* to hide from active scan of wireless client
- ▶ Check to isolate the wireless clients that each wireless client can not communicate others by the device directly.
- ▶ Check to disable WMM (WiFi Multi-Media) feature. WMM takes the audio, voice, and video data stream as prioritized packet to support better performance for such applications.
- ▶ Enter the *wireless network name (SSID)*

- ▶ The *BSSID* is the MAC address of the device
- ▶ Input to set the maximum wireless clients the device wants to provide service.
- ▶ Click *Save/Apply* 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 may setup configuration manually

#### Manual Setup AP

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

Select SSID:

Network Authentication:

WEP Encryption:

**Figure 66: 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:

WEP Encryption:

Encryption Strength:

Current Network Key:

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

**Figure 67: Wireless Setting – OPEN and WEP Security**

- ▶ 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

Save/Apply

**Figure 68: Wireless Setting – 802.1x Security**

- ▶ 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

Save/Apply

**Figure 69: Wireless Setting – WPA Security**

- ▶ 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:	<input type="text"/> <a href="#">Click here to display</a>
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP
WEP Encryption:	Disabled

**Figure 70: Wireless Setting – WPA-PSK Security**

- ▶ 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

**Figure 71: Wireless Setting – WPA2 Security**

- ▶ 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:	<input type="text"/> <a href="#">Click here to display</a>
WPA Group Rekey Interval:	0
WPA Encryption:	AES
WEP Encryption:	Disabled

**Figure 72: Wireless Setting – WPA2-PSK Security**

- ▶ 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

**Figure 73: Wireless Setting – Mixed WPA2/WPA Security**

- ▶ 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:	<input type="text"/> <a href="#">Click here to display</a>
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

**Figure 74: Wireless Setting – Mixed WPA2/WPA-PSK Security**

- ▶ 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

Add Remove

**Figure 75: 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:

Save/Apply

**Figure 76: 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).

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Refresh Save/Apply

**Figure 77: 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 (set *Bridge Restrict* is Disabled) or just the specified MAC addresses of remote wireless bridge devices (set *Bridge Restrict* is Enable or Enable (scan)).
- ▶ Click Refresh to get the updated information
- ▶ Click *Save/Apply* to save the configuration

## Advanced

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

Band:	2.4GHz	
Channel:	11	Current: 11
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	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
54g™ Mode:	54g Auto	
54g™ Protection:	Auto	
Preamble Type:	long	
Transmit Power:	100%	

**Figure 78: Wireless Setting – Advanced**

## Global Setting

- ▶ Enable *AP Isolation* if you do not want AP to be able to communicate with each other.
- ▶ Set the *Wireless 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.

## 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.

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

Refresh

**Figure 79: 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.

Test the connection to your local network

Test your LAN1 Connection:	FAIL	<a href="#">Help</a>
Test your LAN2 Connection:	PASS	<a href="#">Help</a>
Test your LAN3 Connection:	FAIL	<a href="#">Help</a>
Test your LAN4 Connection:	FAIL	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	FAIL	<a href="#">Help</a>

Test the connection to your Internet service provider

Test PPP server connection:	FAIL	<a href="#">Help</a>
Test authentication with ISP:	FAIL	<a href="#">Help</a>
Test the assigned IP address:	FAIL	<a href="#">Help</a>
Ping default gateway:	FAIL	<a href="#">Help</a>
Ping primary Domain Name Server:	PASS	<a href="#">Help</a>

**Figure 80: Diagnostic Result**

Global Setting:

- ▶ 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**

**SNMP Agent**

**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.

Backup Settings

**Figure 81: 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:

Update Settings

**Figure 82: 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 DSL router settings to the factory defaults.

Restore Default Settings

**Figure 83: 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.

View System Log

Configure System Log

**Figure 84: 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:

Display Level:

Mode:

Save/Apply

**Figure 85: 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.

## SNMP Agent

---

This page allows you to use a management application to retrieve statistics and status from the SNMP agent in the device.

### SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent  Disable  Enable

Read Community:	<input type="text" value="public"/>
Set Community:	<input type="text" value="private"/>
System Name:	<input type="text" value="Sysname"/>
System Location:	<input type="text" value="unknown"/>
System Contact:	<input type="text" value="unknown"/>
Trap Manager IP:	<input type="text" value="0.0.0.0"/>

**Figure 86: Management Configuration – SNMP Agent**

## Global Setting

- ▶ Check to enable or disable *SNMP Agent*
- ▶ Enter the name of *Read Community* and *Set Community*
- ▶ Enter the name of *System Location* and *System Contact*
- ▶ Enter the IP address of *Trap Manager IP*
- ▶ 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:

ACS URL:

ACS User Name:

ACS Password:

Display SOAP messages on serial console  Disable  Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

**Figure 87: 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*
- ▶ Select to *Enable* or *Disable* to send the TR-069 SOAP messages to serial console port. This is usually used for trouble shooting purpose.
- ▶ Check to enable *Connection Request Authentication*
- ▶ 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

Save/Apply

**Figure 88: Internet Time Configuration**

### Global Setting

- ▶ Check to enable *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	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
ICMP	Enable	<input checked="" type="checkbox"/> Enable
SNMP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable

Save/Apply

**Figure 89: 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)
- SNMP
- SSH
- TELNET
- TFTP

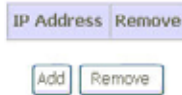
▶ Click *Save/Apply* to save the configuration.

### 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



**Figure 90: 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:   
Subnet Mask:

**Figure 91: Management Configuration – Access Control: Add IP Address**

Global Setting:

- ▶ Add the IP Address and Subnet Mask which are 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 settings and statistics, as well as update 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 92: Management Configuration – Access Control: Password**

Global Setting:

- ▶ Select the level of *Username*; *admin*, *support* or *user*
- ▶ 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 93: 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.

Save/Reboot

Or discard changes and reboot the router.

Reboot

**Figure 94: 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 Network Settings

To surf Internet through the device, you need to configure the network settings of your PC correctly. This appendix provides the guide for a reference.

## Configuring Ethernet (LAN) Card

---

### Before you begin

By default, the device automatically assigns the required Internet settings to your PCs. You need to check your PCs to get the information automatically. If you need to set the information manually, please make sure you get enough information from service provider and configure the network settings of PC correctly.

If you have connected your LAN PCs via Ethernet to the device, please follow the instructions to configure the network settings in Windows XP (for example). The instructions for different Windows system are very similar, please refer its manual separately.

### Windows XP PCs

Click the *Start* button, and then click *Control Panel*, and then click the *Network connection icon*. In the *LAN* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Make sure that the check box of *Internet Protocol TCP/IP* is checked and click *Properties*. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Obtain an IP address automatically and also click the radio button labeled Obtain DNS server address automatically. The PC will send inquiry packet to the device to get an IP address, gateway IP address, DNS IP address and son on automatically.

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

### Assigning static IP addresses to your PCs

If you are professional in networking and subscribe to public IP addresses from service provider, you need to assign the public IP address and associated information to the PCs manually. For example, you may provide public WEB server in your LAN environment, you need to assign public IP address in the WEB server. Basically, you need the information from your service provider.

1. The IP address and subnet mask of each your PC.
2. The gateway IP address for PC to send packets to.
3. The DNS server IP address.

With above information, you are ready to configure your PCs.

Click the *Start* button, and then click *Control Panel*, and then click the *Network connection icon*. In the *LAN* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Make sure that the check box of *Internet Protocol TCP/IP* is checked and click *Properties*. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button to enter the LAN IP address, subnet and gateway IP address manually. Besides, click the radio button to enter DNS IP address manually.

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

## **Configuring Wireless LAN card**

---

If your PC is connected to the device through wireless link, you need to configure the network setting of wireless LAN card in stead of LAN card. The steps to configure the network settings of wireless LAN card are the same procedure described in previous section, Configuring Ethernet LAN card section.

### **Wireless card and drivers**

You need to install the wireless card and drivers correctly. Please check the information of installation and security of wireless card provided by the wireless card vendor or notebook vendor.

### **Configuring wireless device**

The following steps provide a basic guide line to configure the wireless card to establish a wireless connection to the device.

To configure wireless card to establish a connection to the device:

1. Make sure the wireless access card is installed.
2. Make sure the wireless driver is installed.
3. Scan the available wireless AP (Access Point) and find the SSID of the device
4. Connect to the AP
5. Enter the security code (WPA, WEP or others) if necessary

Then you have a connection to the device through wireless link.

## Appendix B - Troubleshooting

During the installing or using the device, you may encounter problem, this appendix provides the solution and instructions to solve the issues. In case, the problem can not be solved, please contact Customer Support for further support.

### Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
<b>LEDs</b>	
<i>Power LED does not illuminate after product is turned on.</i>	Verify that you are using the power adapter provided with the device and that it is securely connected to the device and a wall socket/power strip.
<i>LAN LED does not illuminate after Ethernet cable is attached to your PC.</i>	Verify that the Ethernet cable is securely connected to your LAN switch or PC and to the device. Make sure the PC and/or hub is turned on.
<b>Internet Access</b>	
<i>Cannot access the Internet</i>	Use the ping utility provided by PC's system to check whether your PC can communicate with the device. Command: ping device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.  If you assigned a private IP address to your PC, (not a public address), please check the IP addresses of gateway and DNS server in your PC network settings. Those IP addresses should be given by service provider. Otherwise, configure the PC to receive the IP, gateway IP and DNS IP automatically.
<i>Cannot surf web pages on the Internet.</i>	Verify that the DNS server IP address in the PCs is correct for your ISP. If you configured that the DNS server be assigned automatically from a server, then verify with your ISP that the address configured on the device is correct.
<b>Device's Web pages</b>	
<i>Forgot my user ID or password.</i>	The default setting of username and password is "admin". If you failed to access the device by enter this. You can reset the device to the default configuration by pressing the Reset Default button on the front or rear panel of the device. Then, type the default Username (admin) and password (admin). <b>WARNING:</b> Reset Default means the device returns all settings to their default values.

Problem	Troubleshooting Suggestion
<i>Cannot access the web pages</i>	<p>Verify the Ethernet connection by using ping utility. Command: ping device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.</p> <p>Verify that you are using latest Internet Explorer or Netscape Navigator or other browsers.</p> <p>Verify that subnet mask: the PC's IP address should be defined as being on the same subnet as the IP address of the LAN port on the device.</p>
<i>Changes/settings to the web pages are not being saved.</i>	Be sure to save the configuration after any changes.

## IP Utilities for diagnostic

### Ping

Ping is a simple command and easy way to check remote PC or device on your network and the Internet. Besides, this is a command supported in most of IP-based network operation system like Windows, Linux and so on. To use it, you must know the IP address of the PC or device which you like to send a message to. If the remote PC or device gets this message, the PC or device will send back a message in reply. If you saw the reply, you know the communication link to remote PC or device is OK. In Windows system, you can execute a ping command from the Start menu by clicking the Start button, and then clicking Run and then enter below statement in the open box: (the 192.168.1.1 is an IP address which you like to check the device is on line or not.)

```
ping 192.168.1.1
```

Click OK.

If the communication link is OK, you will see the message and a Command Prompt window is displayed as an example:

```

C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128

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

```

If not, you will receive the message Request timed out.

You could also use this ping tool to verify the Internet connection by entering an external address, such as [www.yahoo.com](http://www.yahoo.com). If you do not know the IP address of a particular Internet location, you can use the nslookup command as described in the following section.

Please be noted that some of PCs or devices may reject to reply message requesting by ping command. At that time, you won't get message in reply, but message timeout.

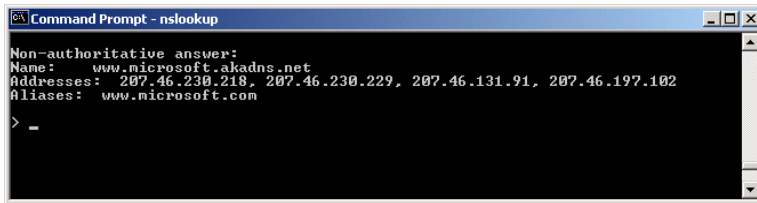
### Nslookup

There is another useful command provided by Windows system. You can use the nslookup command to get the IP address associated with a domain name like [www.yahoo.com](http://www.yahoo.com) or [www.microsoft.com](http://www.microsoft.com). The nslookup command looks up the domain name in on your DNS server located in your service provider. The server then returns the associated IP address. In Windows system, you can execute the nslookup command by clicking the Start button and then clicking Run and then entering below statement in the open box.

Nslookup

Click OK.

A Command Prompt window is prompted. Enter the domain name like [www.yahoo.com](http://www.yahoo.com) or [www.microsoft.com](http://www.microsoft.com). The associated IP address will be shown as below



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

In this case, you see multiple IP addresses associated with that domain name. It is common for Web server. System engineers prepare multiple and redundant servers to handle the heavy traffic and also balance the load in each server.



# Appendix C - Specification

## A1. Hardware Specifications

- Local 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 ADSL Line Interface
  - Compliant with ITU-T G.992.1, G.992.2, G.992.3, G.992.5 and ANSI T1.413 Issue 2
  - Line Impedance: 100  $\Omega$
  - Connection Loops: One (pair wire)
  - Connector: RJ-11
- Indicators
  - POWER – Green LED indicates power and operation. Orange LED indicates failure.
  - ALARM – Red LED indicates DSL link not connected.
  - LAN 1 ~ 4 – Green LED indicates LAN connection.
  - WLAN – Green LED indicates wireless function enabled.
  - DSL – Green LED indicates DSL link connected.
  - INTERNET – Green LED indicates PPP connection. Red indicates PPP failure or device can not get an IP address.
- OAM&P
  - Local: Telnet and Web management
  - Remote: Telnet and Web Management
- Environment
  - Operation Temperature: 0°C ~ 40°C
  - Operation Humidity: 5% ~ 95%
  - Storage Temperature: -20 ~ +85°C
  - Storage Humidity: 5%~95%
- Power
  - DC Adapter: Input 100~240VAC, 50/60Hz; Output 12VDC 1A
- Certificates
  - UL,FCC(TBD)

## A2. Software Specifications

- Bridging
  - ▶ Transparent Bridging and spanning(IEEE 802.1D) with at least 32 MAC addresses
  - ▶ RFC2684 (RFC 1483) Bridged
- 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
- Firewall
  - ▶ Support NAT and DMZ
  - ▶ Stateful Packet Inspection (SPI) with DOS protection - Ping of Death, SYN Flood LAND

- ▶ Protection against IP and MAC address spoofing
- Configuration and Network Management Features
  - ▶ SNMP GETs, SETs and TRAPs for four groups in MIB-II
  - ▶ DHCP client and server for IP management
  - ▶ UPnP Internet Gateway Device (IGD) compliance
  - ▶ WEB for local or remote management
  - ▶ HTTP or TFTP for firmware upgrade and configuration
  - ▶ Support TR-069, TR-098 and with parameters: DeviceInfo, ManagementServer, Time, IPPingDiagnostic, etc

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

## Appendix D - 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 DOCUMENTATION. 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.

## Appendix E - 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](http://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: +55-12-8144-2972

### **EUROPEAN BRANCH OFFICE**

Oehleckerring 6B, 22419 Hamburg, Germany

Tel: +49-40-514400-53 Fax: +49-40-514400-79

### **CHINA SUBSIDIARY**

Room 401, Floor 4, #608 ZhaoJiaBang Road,  
Shanghai, 200031

Tel: +86-21-6431-8800 Fax: +86-21-6431-7885

V1.0XAAR3960