GAN5.PT156A-B

User Manual

Ver 1.0

Contents

GAN5.PT156A-B

ii

1 Safety Precautions

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

2 Overview

The DSL Router is a highly ADSL2+ Integrated Access Device and can support ADSL link with downstream up to 24 Mbps and upstream up to 1 Mbps. It is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or 802.11g/802.11b/802.11n wireless network. The Router combines high-speed ADSL Internet connection, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

The Router is easy to install and use. The Modem connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet by a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

Network and Router management is done through the web-based management interface that can be accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

2.1 Application

- Home gateway
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

2.2 Features

- User-friendly GUI for web configuration

2

GAN5.PT156A-B

- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPOE sessions
- Support SNMP v2, RIP v1 & RIP v2, NAT
- WLAN with high-speed data transfer rates of up to 300 Mbps, compatible with IEEE 802.11b/g/n, 2.4GHz compliant equipment
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Virtual private network (VPN): IPSec
- Secure socket layer virtual private network (SSL VPN)
- Universal plug-and-play
- File server for network attached storage (NAS) devices
- Print server
- Web filtering
- Management and control
  - Web-based management (WBM)
  - Simple network management protocol (SNMP)
  - Command line interface (CLI)
  - TR-069 WAN management protocol
  - TR-064-LAN-side DSL CPE configuration
- Remote update
- 3G Mobile WAN connection
- System statistics and monitoring

3

- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.
- Port Control Protocol

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

GAN5.PT156A-B

3 Hardware Description and Hardware Installation

3.1 Hardware Description

3.1.1 Front Panel

Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on and the device operates normally.
		Blink	The software is upgrading.
		Off	The device is powered off.
	Red	On	The device is initiating.
		Blink	The software is upgrading.
DSL	Green	On	DSL link has established.
		Blink	The DSL line is training.
		Off	Device is powered off.
Internet	Green	On	Internet is synchronized successfully in the route mode.
		Blink	Internet data is being transmitted.
		Off	Ethernet interface is disconnected.
	Red	On	Authentication has failed.
LAN 1/2/3/4	Green	On	The Ethernet interface is connected.
		Blink	Data is being transmitted through the Ethernet interface.
		Off	The Ethernet interface is disconnected.
USB	Green	On	The connection of 3G or USB flash disk has

| Indicator	Color	Status	Description
			established.
		Blink	Data is being transmitted.
		Off	No signal is detected.
WLAN	Green	On	WLAN is enabled.
		Blink	Data is being transmitted through the wireless interface.
		Off	WLAN is disabled.
WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
		Blink	Negotiation is in progress under Wi-Fi Protected Setup.
		Off	Wi-Fi Protected Setup is disabled.

3.1.2 Rear Panel
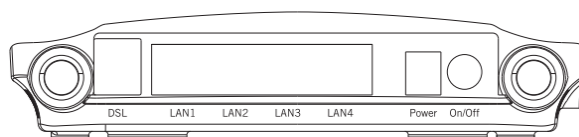
Figure 2 Rear Panel
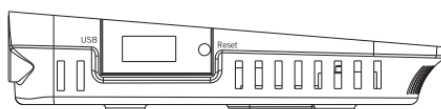
Figure 3 Side Panel

The following table describes the interfaces or the buttons on the rear panel.

Interface	Description
DSL	RJ-11 port: Connect the router to DSL connector or splitter through telephone cable.
LAN 4~1	RJ-45 port, for connecting the router to a PC or another network device.

6

GAN5.PT156A-B

Interface	Description
Reset	Press the button for at least 1 second and then release it. System restores the factory default settings.
USB	For connecting the 3G network adapter or other USB storage devices.
Power	Power interface, for connecting the power adapter.
On/Off	Power switch.
WLAN	WLAN switch, for enabling or disabling the WLAN function.
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the wireless router starts to accept the negotiation of PBC mode.

⚠ **Warning:**

Do not press the Reset button unless you want to clear the current settings. The Reset button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the Reset button gently for 1 second with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.

The power specification is 12V, 1A. If the power adapter does not match the specification, it may damage the device.

3.2 Hardware Installation

3.2.1 Choosing the Best Location for Wireless Operation

Many environmental factors may affect the effective wireless function of the DSL Router. If this is the first time that you set up a wireless network device, read the following information:

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting. Designed to go up to 100 meters indoors and up to 300 meters outdoors, wireless LAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal range. Typical ranges vary depending on types of materials and background RF noise in your home or business.

3.2.2 Connecting the Device

Please follow the steps below to connect the device.

Step1 Connect the **Line** port of the DSL router with a telephone cable.

Step2 Connect the LAN port of the DSL router to the network card of the PC via an Ethernet cable.

Step3 Plug one end of the power adapter to the wall outlet and connect the other end to the Power port of the DSL Router.

The followig figure displays the connection of the DSL router, PC, and telephones.
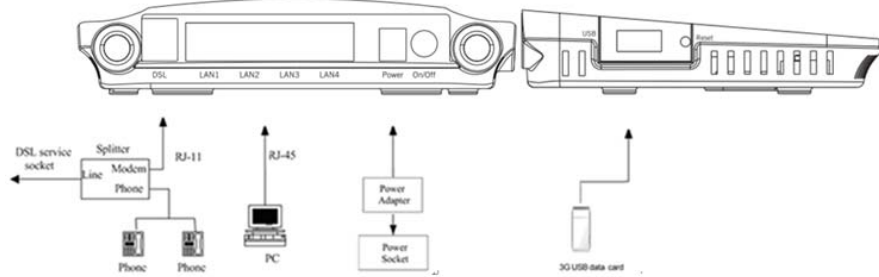
Figure 4 Connecting the DSL router

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows XP.
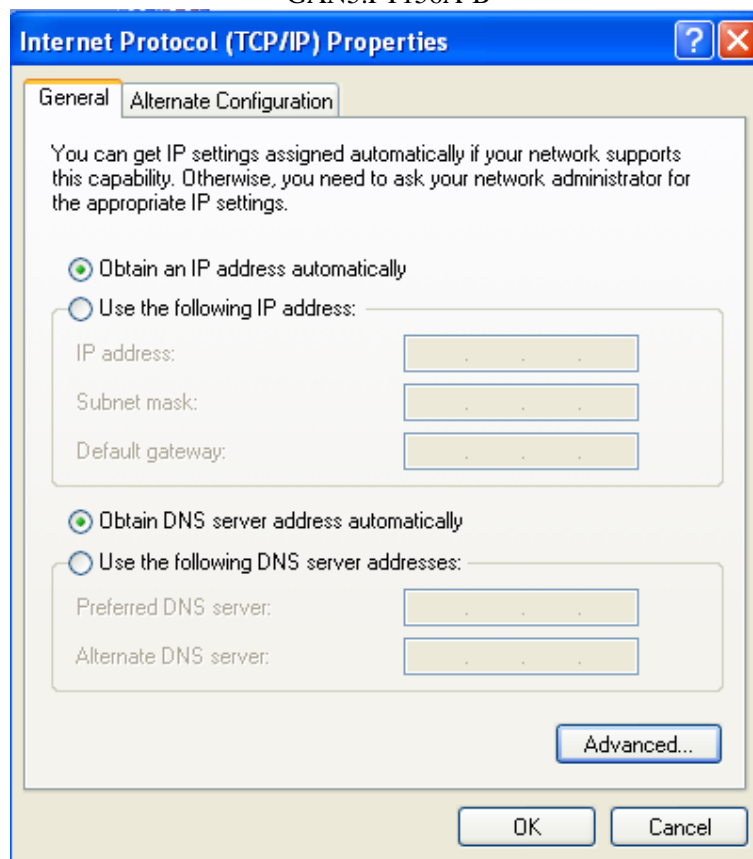
Figure 5 IP and DNS configuration

TCP/IP configuration steps for Windows XP are as follows:

Step1   Choose **Start** > **Control Panel** > **Network Connections**.

Step2   Right-click the Ethernet connection icon and choose **Properties**.

Step3   On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.

Step4   The **Internet Protocol (TCP/IP) Properties** window appears.

10

Step5 Select the **Obtain an IP address automatically** radio button.

Step6 Select the **Obtain DNS server address automatically** radio button.

Step7 Click **OK** to save the settings.

4.2 Logging In to the DSL Router

To log in to the DSL router, do as follows:

Step1 Open a Web browser on your computer.

Step2 Enter *http://192.168.1.1/main.html* in the address bar. The login page appears.

Step3 Enter the user name and the password. The default username and password of the super user are **1234** and **1234**. It is recommended to change these default values after logging in to the DSL router for the first time.

Step4 Click **OK** to log in to the Web page. Otherwise, please click **CANCEL** to exit the login page.

Figure 6 Login page

After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

5 Web-Based Management

This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters in a user-friendly GUI.

5.1 Device Information

Choose **Device Info**, and the submenus of **Device Info** are shown as below:

Figure 7 Submenus of device info

5.1.1 Summary

Choose **Device Info > Summary**, and the following page appears.

Device Info

Board ID:	96328ang
Build Timestamp:	120515_1251
Model Name:	R5000UNv2
Serial Number:	001ee363281e
Software Version:	TE020D005
Bootloader (CFE) Version:	1.0.37-106.5
DSL PHY and Driver Version:	A2pD035g.d23k
Wireless Driver Version:	5.100.138.2001.cpe4.

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	fe80::46d:36ff:fe9e:9261
Global LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Fri Oct 1 00:07:59 2010

This page displays the device information such as the board ID, software version, and the information of your WAN connection such as the upstream rate and the LAN IPv4 address.

5.1.2 WAN

Choose **Device Info > WAN** and the following page appears.

WAN Info

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address	IPv6 Address	Connected Time

This page displays the information of the WAN interface, such as the connection status, IPv4 address, and connected time.

5.1.3 Statistics

5.1.4 LAN

Choose **Device Info > Statistics > LAN** and the following page appears.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	1428	12	0	0
eth1	0	0	0	0	1428	12	0	0
eth2	0	0	0	0	1428	12	0	0
eth3	82643	631	0	0	445420	915	0	0
wlan	0	0	0	0	0	0	0	0

Reset Statistics

In this page, you can view the statistical information about the recevied and transmitted data packets of the Ethernet and wireless interfaces.

Click **Reset Statistics** to restore the values to zero and recount them.

5.1.5 WAN Service

Choose **Device Info > Statistics > WAN Service** and the following page appears.

Statistics -- WAN

Interface	Description	Connected Time	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

Reset Statistics

In this page, you can view the statistical information about the recevied and transmitted data packets of the WAN interface.

Click **Reset Statistics** to restore the values to zero and recount them.

5.1.6 xTM

Choose **Device Info > Statistics > xTM** and the following page appears.

14

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors

Reset

In this page, you can view the statistical information about the recevied and transmitted data packets at the xTM interfaces.

Click the **Reset** button to restore the values to zero and recount them.

5.1.7 xDSL

Choose **Device Info > Statistics** > **xDSL** and the following page appears.

15

Statistics -- xDSL

Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test   Reset Statistics

In this page, you can view the statistical information about the recevied and transmitted data packets of the xDSL interfaces.

Click **xDSL BER Test** to test the xDSL Bit Error Rate.

Click **Reset Statistics** to restore the values to zero and recount them.

xDSL BER Test

Click **xDSL BER Test** to perform a bit error rate (BER) test on the DSL line. The test page is as follows:

ADSL BER Test – Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): 20

Start Close

The **Tested Time (sec)** can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360. Select a time in the drop-down list and click **Start**. The following pages appear.

ADSL BER Test – Running

The xDSL BER test is in progress. The connection speed is 0 Kbps. The test will run for seconds.

Click "Stop" to terminate the test.

Stop Close

When the ADSL BER test completes, the following page appears.

ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x000000001B69B580
Total Error Bits:	0x0000000000000000
Error Ratio:	0.00e+00

Close

Note:
If the BER reaches e-5, you cannot access the Internet.

5.1.8 Route

Choose **Device Info > Route** and the following page appears.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate

D - dynamic (redirect), M - modified (redirect).

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

In this page, you can view the route table information.

5.1.9 ARP

Choose **Device Info > ARP** and the following page appears.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.26	Complete	00:22:b0:68:de:69	br0

In this page, you can view the MAC address and IP address information of the device connected to the router.

5.1.10   DHCP

Choose **Device Info > DHCP** and the following page appears.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

In this page, you can view the host name, the IP address assigned by the DHCP server, the MAC address this is corresponding to the IP address, and the DHCP lease time.

5.2 Advanced Setup

Choose **Advanced Setup** and the submenus of **Advanced Setup** are shown as below:

Advanced Setup

Layer2 Interface

WAN Service

3G Wan Service

LAN

NAT

Security

Parental Control

Quality of Service

Routing

DNS

DSL

UPnP

DNS Proxy

Print Server

Storage Service

DLNA

Interface Grouping

IP Tunnel

PCP

Multicast

Packet Acceleration

Figure 8 Submenus of advance setup

5.2.1 Layer2 Interface

ATM Interface

Choose **Advanced Setup** > **Layer2 Interface > ATM Interface** , and the following page appears.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove

Add   Remove

In this page, you can add or remove the DSL ATM Interfaces.

Click the **Add** button to display the following page.

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

VPI: [0-255]   0

VCI: [32-65535] 35

Select DSL Latency
☑ Path0
☐ Path1

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

Select Connection Mode
⦿ Default Mode – Single service over one connection
◯ VLAN MUX Mode – Multiple Vlan service over one connection

Encapsulation Mode: LLC/SNAP-BRIDGING ▾

Service Category: UBR Without PCR ▾

Select IP QoS Scheduler Algorithm
⦿ Strict Priority
     Precedence of the default queue: 8 (lowest)
◯ Weighted Fair Queuing
     Weight Value of the default queue: [1-63]   1
     MPAAL Group Precedence: 8 ▾

Back   Apply/Save

In this page, you can set the VPI and VCI values, and select the DSL latency, link type (EoA is for PPPoE, IPoE, and Bridge.), connection mode, encapsulation mode, service category, and IP QoS scheduler algorithm.

- **VPI (Virtual Path Identifier)**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

21

- **VCI (Virtual Channel Identifier)**: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Select DSL Latency**: You may select **Path0** and **Path1**.
- **Select DSL Link Type**: You may select **EoA** (it is for PPPoE, IPoE, and Bridge), **PPPoA**, or **IPoA**.
- **Select Connection Mode:** You may select the **Default Mode** or the V**LAN MUX Mode**.
- **Encapsulation Mode**: You may select **LLC/SNAP-BRIDGING** or **VC/MUX** in the drop-down list.
- **Service Category:** you may select **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR** or **Realtime VBR** in the drop-down lsit.
- **Select IP QoS Scheduler Algorithm:** You may select **Strict Priority** and **Weighted Fair Queuing**.

Note:

QoS cannot be set for CBR and Realtime VBR.

After finishing setting, click the **Apply/Save** button to make the settings take effect. See the following figure:

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐

Add   Remove

If you want to remove this Interface, please select the **Remove** check box that is corresponding to the selected interface and then click the **Remove** button.

5.2.2 WAN Service

Choose **Advance Setup > WAN Service,** and the following page appears.

GAN5.PT156A-B

Wide Area Network (WAN) Service Setup

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

Round Dial Interval (seconds)[15-43200] [15] [Save]

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0	PVC:8/32	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp1	PVC:8/36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up

[Add] [Remove]

In this page, you are allowed to add, remove, or edit a WAN service.

Adding a PPPoE WAN Service

This section describes the steps for adding the pppoe_0_0_35 (PPPoE mode) service.

Step1   In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.)

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm0/(0_0_35) ▼

[Back] [Next]

23

GAN5.PT156A-B

Step2   In this page, you can select a ATM Interface for the WAN service. After selecting the ATM interface, click **Next** to display the following page.

WAN Service Configuration

Select WAN service type:
- ⦿ PPP over Ethernet (PPPoE)
- ◯ IP over Ethernet
- ◯ Bridging

Enter Service Description: PVC:0/35

[Back] [Next]

Step3   In this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. If you want IPv6 to support this service. Click **Next** to display the following page.

WAN Service Configuration

Select WAN service type:

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

MTU[576-1500]: 1492

MRU[576-1500]: 1492

☑ Enable IPv4 for this service

☑ Enable Firewall

☑ Enable NAT

☐ Enable Fullcone NAT

☐ Dial on demand (with idle timeout timer)

☐ PPP IP extension

☐ Use Static IPv4 Address

☐ Enable IPv6 for this service

☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

☐ Enable IGMP Multicast Proxy

Back Next

Step4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:**. NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

25

● **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPOE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup. If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.

● **PPP IP extension:** If you want to configure DMZ Host, you should enable it first.

● **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.

● **Enable IGMP Multicast Proxy:**if you want PPPoE mode to support IPTV, enable it.

Step5 After setting the parameters, click **Next** to display the following page.

Routing -- Default Gateway

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0	-> <-	ppp2 ppp1 ppp3g0

Back Next

Step6 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

26

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

○ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces		Available WAN Interfaces
	-> <-	ppp2 ppp0 ppp1 ppp3g0

◉ **Use the following Static DNS IP address:**

Primary DNS server: 80.58.61.250
Secondary DNS server: 80.58.61.254

Back   Next

Step7   In this page, you may obtain the DNS server addresses from the selected WAN interface or manually enter the static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must manually enter the static DNS server addresses. Click **Next**, and the following page appears.

WAN Setup - Summary

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

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

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

Back   Apply/Save

Step8   In this page, it displays the information about the PPPoE settngs. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

27

GAN5.PT156A-B

Wide Area Network (WAN) Service Setup

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

Round Dial Interval (seconds)[15-43200] [15] [Save]

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0	PVC:8/32	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp1	PVC:8/36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp2	PVC:0/35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up

[Add] [Remove]

Adding a MER (IPoE) WAN service

This section describes the steps for adding the ipoe_0_0_36 (MER mode) service.

Step1   In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM configuration for this WAN service.)

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0	PVC:8/32	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp1	PVC:8/36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp2	PVC:0/35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up

GAN5.PT156A-B
WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm3/ (0_0_36) ▼

Back   Next

Step2   Select an ATM Interface, for example, atm1/(0_0_36), and then click
Next to display the following page.

WAN Service Configuration

Select WAN service type:
○ PPP over Ethernet (PPPoE)
⦿ IP over Ethernet
○ Bridging

Enter Service Description: PVC:0/36

Back   Next

29

Step3 In this page, select the WAN service type to be IP over Ethernet, enter the service description, and enable IPv6 for this service. After finishing setting, click **Next** to display the following page.

WAN IP Settings

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

☑ Enable IPv4 for this service
◉ Obtain an IP address automatically

Option 60 Vendor ID: [   ]
Option 61 IAID: [   ] (8 hexadecimal digits)
Option 61 DUID: [   ] (hexadecimal digit)
Option 125: ◉ Disable   ○ Enable
○ Use the following Static IP address:
WAN IP Address: [   ]
WAN Subnet Mask: [   ]
WAN gateway IP Address: [   ]

☐ Enable IPv6 for this service

[Back] [Next]

Step4 In this page, you may themodify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP. If you eable IPv6 for this WAN service, you should also enter the next-hop IPV6 address. Click **Next** and the following page appears.

Note:

*If selecting **Obtain an IP address automatically**, DHCP will be enabled for PVC in MER mode.*

*If selecting **Use the following Static IP address**, please enter the WAN IP address, subnet mask and gateway IP address.*

GAN5.PT156A-B

Network Address Translation Settings

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

☑ Enable NAT

☐ Enable Fullcone NAT

☑ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast

☐ Enable MLD Multicast Proxy

[Back] [Next]

Step5 In this page, you can set the network address translation settings,for example, enabling NAT, enabling firewall,.enabling IGMP multicast, and enabling MLD multicast proxy. After finishing setting, click **Next** and the following page appears.

Routing ·· Default Gateway

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

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0	atm3 ppp1 ppp2 ppp3g0

-> <-

IPv6: Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface [ipoe_0_0_36/atm3 ▾]

[Back] [Next]

Step6 In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

31

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

○ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server
Interfaces

Available WAN Interfaces

atm3
ppp0
ppp1
ppp2
ppp3g0

->
<-

◉ **Use the following Static DNS IP address:**

Primary DNS server: 80.58.61.250

Secondary DNS server: 80.58.61.254

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

◉ Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: ipoe_0_0_36/atm3 ▼

Back   Next

Step7   In this page, you may obtain the DNS server addresses from the selected WAN interface or manually enter static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must enter the static DNS server addresses. After finishi+ng setting, click **Next** to display the following page.

WAN Setup - Summary

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

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

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

Back   Apply/Save

Step8 In this page, it displays the information about the IPoE settngs.Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

Wide Area Network (WAN) Service Setup

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

Round Dial Interval (seconds)[15-43200] 15   Save

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0	PVC:8/32	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp1	PVC:8/36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp2	PVC:0/35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up
atm3	PVC:0/36	IPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	

Add   Remove

Adding a PPPoA WAN service

This section describes the steps for adding the pppoa_0_0_37 (PPPoA mode) service.

Step1 Choose **Advanced Setup** > **Layer2 Interface** > **ATM Interface** to dsipaly the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for PPPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

ATM PVC Configuration

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

VPI: [0-255]   0

VCI: [32-65535]   37

Select DSL Latency
☑ Path0
☐ Path1

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

Encapsulation Mode: VC/MUX

Service Category: UBR Without PCR

Select IP QoS Scheduler Algorithm
◉ Strict Priority
    Precedence of the default queue: 8 (lowest)
○ Weighted Fair Queuing
    Weight Value of the default queue: [1-63]   1
    MPAAL Group Precedence: 8

Back   Apply/Save

Step2   Select the DSL link type to be **PPPoA**, and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to apply the setings, and the following page appears.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	32	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm1	8	36	Path0	UBRWPCR	EoA	DefaultMode	Disabled				☐
atm2	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm3	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm4	0	37	Path0	UBR	PPPoA	DefaultMode	Enabled	SP	1	8	☐

Add   Remove

Step3   Choose **WAN Service** and click **Add** to display the following page.

34

GAN5.PT156A-B

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm4/(0_0_37) ▼

Back Next

Step4   Select the proper interface for the WAN service, and then click **Next** to display the following page.

WAN Service Configuration

Enter Service Description: PVC:0/37

Back Next

Step5   In this page, you may modify the service description. Click **Next** to display the following page.

PPP Username and Password

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

PPP Username:	
PPP Password:	
Authentication Method:	AUTO
MTU[576-1500]:	1492
MRU[576-1500]:	1492

☑ Enable IPv4 for this service

☑ Enable Firewall

☑ Enable NAT

☐ Enable Fullcone NAT

☐ Dial on demand (with idle timeout timer)

☐ PPP IP extension

☐ Use Static IPv4 Address

☐ Enable IPv6 for this service

☐ Enable PPP Debug Mode

Multicast Proxy

☐ Enable IGMP Multicast Proxy

Back Next

Step6   In this page, you can enter the PPP username and PPP password provided by your ISP. Select the authentication method according to your requirement. After finishing setting, click **Next** to display the following page.

Routing -- Default Gateway

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

Selected Default
Gateway Interfaces

Available Routed WAN
Interfaces

ppp0		pppoa4 atm3 ppp1 ppp2 ppp3g0
	-> <-	

Back Next

Step7   In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

○ **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces   Available WAN Interfaces

```
                                    pppoe4
                                    atm3
                                    ppp0
                          [ -> ]    ppp1
                                    ppp2
                          [ <- ]    ppp3g0
```

⊙ **Use the following Static DNS IP address:**

Primary DNS server: `80.58.61.250`
Secondary DNS server: `80.58.61.254`

[Back] [Next]

Step8   In this page, you can obtain the DNS server addresses from the selected WAN interface or manually enter the static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must enter the static DNS server addresses. After finishing setting, click **Next** to display the following page.

WAN Setup - Summary

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

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

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

[Back] [Apply/Save]

Step9   In this page, it displays the information about the PPPoA settngs.Click **Apply/Save** to apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

37

Wide Area Network (WAN) Service Setup

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

Round Dial Interval (seconds)[15-43200] [15] [Save]

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0	PVC:8/32	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp1	PVC:8/36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp2	PVC:0/35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up
pppoa4	PVC:0/37	PPPoA	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up
atm3	PVC:0/36	IPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	

[Add] [Remove]

Adding an IPoA WAN service

This section describes the steps for adding the ipoa_0_0_38 (IPoA mode).

Step1   Choose **Advanced Setup > Layer2 Interface > ATM Interface** to dsipaly the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for IPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

ATM PVC Configuration

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

VPI: [0-255]   [0]

VCI: [32-65535]   [38]

Select DSL Latency
☑ Path0
☐ Path1

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

Encapsulation Mode: [LLC/SNAP-ROUTING ▾]

Service Category: [UBR Without PCR ▾]

Select IP QoS Scheduler Algorithm
◉ Strict Priority
    Precedence of the default queue: 8 (lowest)
○ Weighted Fair Queuing
    Weight Value of the default queue: [1-63]   [1]
    MPAAL Group Precedence: [8 ▾]

[Back] [Apply/Save]

Step2   Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After

finishing setting, click the **Apply/Save** button to display the following page.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	32	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm1	8	36	Path0	UBRWPCR	EoA	DefaultMode	Disabled				☐
atm2	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm3	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP	1	8	☐
atm4	0	37	Path0	UBR	PPPoA	DefaultMode	Enabled	SP	1	8	☐
ipoa0	0	38	Path0	UBR	IPoA	DefaultMode	Enabled	SP	1	8	☐

[Add] [Remove]

Step3 Choose **WAN Service** and click **Add** to display the following page.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

[ipoa0/(0_0_38) ▼]

[Back] [Next]

Step4 Select the proper interface for the WAN service ,and then click **Next** to display the following page.

WAN Service Configuration

Enter Service Description: PVC:0/38

[Back] [Next]

Step5 In this page, you may modify the service description. Click **Next** to display the following page.

WAN IP Settings

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

WAN IP Address: 0.0.0.0

WAN Subnet Mask: 0.0.0.0

[Back] [Next]

Step6 In this page, enter the WAN IP address and the WAN subnet mask provided by your ISP and then click **Next** to display the following page.

Network Address Translation Settings

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

☑ Enable NAT

☐ Enable Fullcone NAT

☑ Enable Firewall

IGMP Multicast

☐ Enable IGMP Multicast

[Back] [Next]

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

If you do not want to enable NAT, and wish the user of modem to access the Internet normally, you need to add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, please enable the NAT function.

Step7 After finishing setting, click **Next** to display the following page.

40

Routing -- Default Gateway

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

Selected Default
Gateway Interfaces

ppp0

Available Routed WAN
Interfaces

ipoa0
ata3
ppp1
ppp2
pppoa4
ppp3g0

->

<-

Back Next

Step8   In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

○ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

Available WAN Interfaces

ipoa0
ata3
ppp0
ppp1
ppp2
pppoa4
ppp3g0

->

<-

⊙ Use the following Static DNS IP address:

Primary DNS server: 80.58.61.250

Secondary DNS server: 80.58.61.254

Back Next

Step9   In this page, you should use a static DNS IP address for IPoA mode. Select the proper DNS server interface and enter the primary DNS server and the secondary DNS server. Click **Next** to display the following page.

41

GAN5.PT156A-B

WAN Setup - Summary

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

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

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

Back   Apply/Save

Step10 In this page, it displays the information about the IPoA settngs. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

Wide Area Network (WAN) Service Setup

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

Round Dial Interval (seconds)[15-43200] 15   Save

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0	PVC:8/32	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp1	PVC:8/36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp2	PVC:0/35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up
pppoa4	PVC:0/37	PPPoA	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up
atm3	PVC:0/36	IPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	
ipoa0	PVC:0/38	IPoA	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	

Add   Remove

Adding a Bridge WAN service

This section describes the steps for adding the br_0_0_39 (Bridge mode) service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.) Click the **Add** button to display the following page.

42

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm5/ (0_0_39)

Back   Next

Step2   Select the proper ATM Interface, for example atm3/(0_0_39) and then
click **Next** to display the following page.

WAN Service Configuration

Select WAN service type:
○ PPP over Ethernet (PPPoE)
○ IP over Ethernet
◉ Bridging

Enter Service Description: PVC:0/39

Back   Next

43

Step3   In this page, you can select the WAN service type, modify the service description. After finishing setting, click **Next** to display the following page.

WAN Setup - Summary

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

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

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

Back   Apply/Save

Step4   In this page, it displays the information about the bridge settngs. Click **Apply/Save** to save and apply the settings, and then the following page appears. You can modify the settings by clicking the **Back** button if necessary.

Wide Area Network (WAN) Service Setup

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

Round Dial Interval (seconds)[15-43200] 15   Save

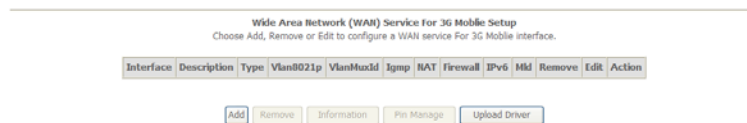| Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
ppp0	PVC:8/32	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp1	PVC:8/36	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	Up
ppp2	PVC:0/35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up
pppoa4	PVC:0/37	PPPoA	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	Up
atm3	PVC:0/36	IPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Enabled	Disabled	☐	edit	
ipoa0	PVC:0/38	IPoA	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	☐	edit	
atm5	PVC:0/39	Bridge	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	☐	edit	

Add   Remove

Figure 9 Completing the settings of bridge WAN service

5.2.3 3G WAN Service

Choose **Advanced Setup > 3G WAN Service** , and the following page appears.

modem status: NO USB CARD

Wide Area Network (WAN) Service for 3G Mobile Setup
Choose Add, Remove or Edit to configure a WAN service For 3G Mobile interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit	Action

Add   Remove   Information   Pin Manage   Upload Driver

This page is used to configure 3G connection. If you want to access the Internet through 3G connection, a 3G network card is required. Connect the 3G network card to the USB interface of the Router.

- **Information**: Click it to display the information of the 3G network card.
- **Pin Manage**: Click it to configure the 3G PIN.
- **Upload Driver**: For a un-support USB dongle, click it to upload the new driver for supporting the USB. The driver is a text file.

Click **Add** in the **WAN Service for 3G Mobile Setup** to display the following page.

45

3G USB mobile modem setup

☑ Enable USB Modem

User Name: [   ]

Password: [   ]

Authentication Method: [AUTO   ▼]

APN: [internet   ]

Dial Number: [*99#   ]

Idle time(in sec.): [0   ]

Net Select: [Auto   ▼]

☐ Dial on demand

Dial Delay(in sec.): [10   ]

Default WAN Connection Select: [DSL   ▼]

WAN backup mechanism: ⊙ DSL   ○ IP connectivity

[Apply/Save]   [Auto Setting]

In this page, you are allowed to configure the settings of the 3G USB modem.

● **Enable USB Modem:** If you want to access the Internet through the 3G network card, you must enable the USB modem.

● **User Name:** Username provided by your 3G ISP.

● **Password:** Password provided by your 3G ISP.

● **Authentication Method:** Select a proper authentication method in the drop-down list. You can select Auto, PAP, CHAP, or MSCHAP.

● **APN:** APN (Access Point Name) is used to identify the service type. Enter the APN provided by your 3G ISP.

● **Dial Number:** Enter the dial number provided by your 3G ISP.

● **Idle time (in sec.):** If no traffic for the preset time, the 3G will disconnect automatically.

● **Dial on demand**: Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the 3G

connection. Once it detects the flow (like access to a webpage), the modem restarts the 3G dialup.

- **Dial Delay (in sec.)**: The 3G delays dial after the DSL is disconnected.
- **Default WAN Connection Select**: You can select DSL or 3G from the drop-down list.
- **WAN back mechanism**: The 3G connection is backup for the DSL connection.
    - **DSL**: If the DSL is disconnected, the 3G starts to dial.
    - **IP connectivity**: If the system fails to ping the specified IP address, the 3G starts to dial.

After finishing setting, click the **Apply/Save** button to save the settings.

You may also click the **auto setting** button to automatically configure the 3G connection.

After clicking the **Apply/Save** button, the following page appears.

modem status: NO USB CARD

Wide Area Network (WAN) Service For 3G Mobile Setup
Choose Add, Remove or Edit to configure a WAN service For 3G Mobile interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit	Action
ppp3g0	mobile	mobile	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	--	edit	Dial

Add   Remove   Information   Pin Manage   Upload Driver

If the 3G network card is installed, you may click the button on the **Action** column to establish or disconnect the 3G connection.

Note:

When there is no DSL WAN connection, insert the 3G network card, and then system will perform dial-up automatically. If the DSL WAN connection and the 3G connection coexist, the DSL WAN connection takes priority over the 3G connection. When the DSL WAN connection starts to perform dial-up, the 3G connection will be disconnected. If the DSL WAN connection has established, you may manually to perform 3G dial-up, and then the DSL WAN connection will be disconnected.

5.2.4 LAN Configuration

Choose **Advanced Setup > LAN**, and the following page appears.

47

Local Area Network (LAN) Setup

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

IP Address: `192.168.1.1`

Subnet Mask: `255.255.255.0`

☑ Enable IGMP Snooping

☐ Enable STP

○ Disable DHCP Server
◉ Enable DHCP Server

Start IP Address: `192.168.1.33`

End IP Address: `192.168.1.199`

Primary DNS server: `80.58.61.250`

Secondary DNS server: `80.58.61.254`

Leased Time (hour): `24`

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

| Edit Multi LAN | Edit DHCP Option | DHCP Advance setup |

| MAC Address | IP Address | Remove |

| Add Entries | Remove Entries |

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

IP Address: `192.168.249.1`

Subnet Mask: `255.255.255.252`

Apply/Save

In this page, you can configure an IP address for the DSL router, enable IGMP snooping, enable or disable the DHCP server, edit the DHCP option, configure the DHCP advanced setup and set the binding between a MAC address and an IP address.

Configuring the Private IP Address for the DSL Router

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

In this page, you can modify the IP address of the device. The preset IP address is 192.168.1.1.

Enabling IGMP Snooping

IGMP snooping enables the router to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the router listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

☐ Enable IGMP Snooping

In this page, you can enable the IGMP snooping.

Enable STP

☐ Enable STP

In this page, you can enable STP.

Configuring the DHCP Server

○ Disable DHCP Server
◉ Enable DHCP Server

Start IP Address:	192.168.1.33
End IP Address:	192.168.1.199
Primary DNS server:	80.58.61.250
Secondary DNS server:	80.58.61.254
Leased Time (hour):	24

Figure 10 Setting the DHCP server

If you enable the DHCP sever, the clients will automatically acquire the IP address from the DHCP server. If the DHCP server is disabled, you need to manually set the start IP address, end IP address and the lease time for the clients in the LAN.

Editing the DHCP Option

Click the **Edit DHCP Option** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option Setup** page.

DHCP OPtion Setup

This page allows you to configurate the DHCP OPTION. These options will be sent to DHCP client.

You can define at most 30 options.

State	Code	Value	Pool	Edit/Remove

<div align="right">Add   Edit   Remove   Return</div>

In this page, you can add, edit or delete the DHCP options, and these options will be sent to the DHCP client.

Edit Multi LAN

Click the **Edit Multi LAN** button in the **Local Area Network (LAN) Setup** page to display the **LAN IP Interface and DHCP Option 60 setup** page.

LAN IP Interfase and DHCP Option 60 setup

This page allow you to setup LAN IP Interfase and DHCP Option 60, the dhcp server will assign one ip address based on you setting to dhcp client.

LAN IP Interfase and DHCP Option 60 tables:

LAN Interface	LAN IP Address	Subnet Mask	DHCP State	Vendor Id	IP Routers	Start IP	End IP	Primary DNS	Secondary DNS	Edit
Second LAN	0.0.0.0	255.255.255.0	Disable		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	○
Third LAN	0.0.0.0	255.255.255.0	Disable		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	○

<div align="center">Add   Edit   Remove   Return</div>

In this page, you can configure LAN IP Interface and DHCP Option 60. The DHCP server will assign one IP address based on you setting to DHCP client.
Click **Add** to display the following page.

GAN5.PT156A-B

LAN IP Address:	
Subnet Mask:	
DHCP State:	Enable
Vendor Id:	
VendorId Match Mode:	Exact
IP Routers:	
Start IP Address:	
End IP Address:	
Primary DNS server:	
Secondary DNS server:	
Leased Time (seconds):	

Apply   Cancel

● **DHCP State**: you can enable or disable DHCP State.

VendorId Match Mode: you can choose the following items from drop-down list.

```
Exact
Exact
Prefix
Suffix
Substring
```

DHCP Advance Setup

Click the **DHCP Advance Setup** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Advance Setup** page.

51

DHCP Advance Setup

This page allows you to enable or disable dhcp for every lan interface.

State	Interface
☑	eth0
☑	eth1
☑	eth2
☑	eth3
☑	wl0
☑	wl0.1
☑	wl0.2
☑	wl0.3

In this page, you can enable or disable DHCP for each LAN interface.

Configuring the DHCP Static IP Lease List

The lease list of static IP address can reserve the static IP addresses for the hosts with the specific MAC addresses. When a host whose MAC address is in the lease list of static IP address requests the DHCP server for an IP address, the DHCP server assigns the reserved IP address to the host.

MAC Address	IP Address	Remove

Add Entries	Remove Entries
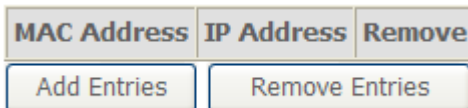
Figure 11 DHCP static lease list

Click the **Add Entries** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Static IP Lease** page.

DHCP Static IP Lease

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

MAC Address:

IP Address:

Apply/Save

Figure 12 Adding an entry of DHCP static IP lease list

In this page, enter the MAC address of the LAN host and the static IP address that is reserved for the host, and then click the **Apply/Save** button to apply the settings.

Configuring the Second IP Address and Subnet Mask for a LAN Interface

In the **Local Area Network (LAN) Setup** page, you are allowed to set the second IP address and the subnet mask for a LAN interface.

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

IP Address:

Subnet Mask:

Figure 13 Setting the second IP address and subnet mask

After enabling **Configure the second IP Address and Subnet Mask for LAN interface**, enter an IP address and a subnet mask for the LAN interface.

After finishing setting, click the **Apply/Save** button to apply the settings.

IPv6 Autoconfig

Click **Advanced Setup > LAN >IPv6 Autoconfig**, and the following page appears.

IPv6 LAN Auto Configuration

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

Static LAN IPv6 Address Configuration

ULA Interface Address (prefix length is required): [_____] should start with 'fd'

IPv6 LAN Applications

☑ Enable DHCPv6 Server
⊙ Stateless
○ Stateful

Start Interface ID: [0:0:0:33]
End Interface ID: [0:0:0:254]
Leased Time (hour): [12]

☑ Enable RADVD

☐ Enable ULA Prefix Advertisement
Prefix: [_____] should start with 'fd'
Preferred Life Time (hour): [-1]
Valid Life Time (hour): [-1]

Site Prefix Configuration
⊙ Delegated Site Prefix from WAN
○ Static Site Prefix
Site Prefix: [2002::]
Site Prefix Length: [48]

☐ Enable MLD Snooping

[Save/Apply]

Figure 14 IPv6 auto configuration

In this page, you can set an IP address for the DSL IPv6 router, enable the DHCPv6 server, enable RADVD and enable the MLD snooping function.

● **Enable DHCPv6 Server:** WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.

● **Enable RADVD:** The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.

● **Enable MLD Snooping**: Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes

54

mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

After finishing setting, click the **Save/Apply** button to apply the settings.

5.2.5 NAT

Note:
The NAT information is not displayed in the bridge mode.

Virtual Servers

Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

Choose **Advanced Setup > NAT > Virtual Servers**, and the following page appears.
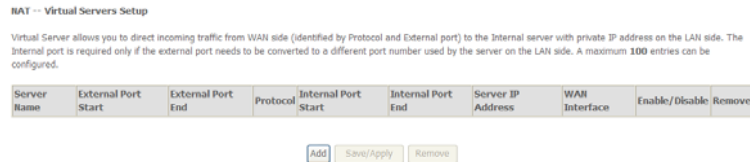
Figure 15 Virtual server setup

In this page, you are allowed to add, or remove a virtual server entry.

To add a virtual server, do as follows:

Click the **Add** button to display the following page.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End".However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
Remaining number of entries that can be configured:100

Use Interface   ipoe_0_0_36/atm3
Service Name:
⊙ Select a Service: Select One
○ Custom Service:

Server IP Address: 192.168.1.

Status:

[Apply/Save]

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

[Save/Apply]

Figure 16 Adding an entry of virtual server

- **Use interface**: Select an interface that you want to configure.
- **Select a Service**: Select a proper service in the drop-down list.
- **Custom Service**: Enter a new service name to establish a user service type.
- **Server IP Address**: Assign an IP address to virtual server.
- **Status:** Enable or Disable this entry.
- **External Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **External Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Protocol**: You may select TCP/UDP, TCP, or UDP in the drop-down list.
- **Internal Port Start**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Internal Port End**: When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

After finishing setting, click **Save/Apply** to save and apply the settings.

Port Triggering

Some applications need some ports to be opened in the firewall for the remote access. When an application initializes a TCP/UDP to connect to a remote user, port triggering dynamically opens the open ports of the firewall.

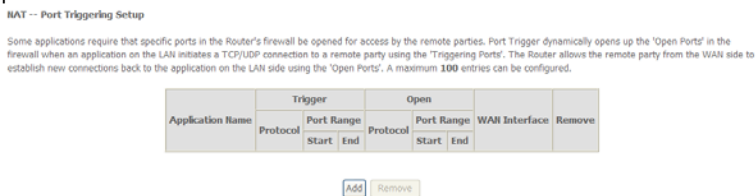Choose **Advanced Settings > NAT > Port Triggering**, and the following page appears.

Figure 17 Port triggering setup

In this page, you may add or delete an entry of port triggering.
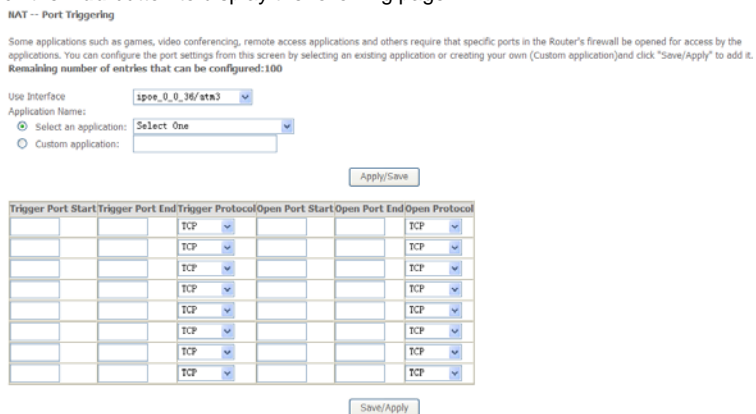
Click the **Add** button to display the following page.

Figure 18 Adding an entry of port triggering

- **Use interface**: Select an interface that you want to configure.
- **Select an application:** Select a proper application in the drop-down list.
- **Custom application:** Manually define an application.

- **Trigger port Start:** The start port number that LAN uses to trigger the open port.
- **Trigger port End:** The end port number that LAN uses to trigger the open port.
- **Trigger Protocol:** Select the application protocol. You may select TCP/UDP, TCP, or UDP.
- **Open Port Start:** The start port number that is opened to WAN.
- **Open Port End:** The end port number that is opened to WAN.
- **Open Protocol:** Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

After finishing setting, click **Save/Apply** to apply the settings.

Note:
You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

DMZ Host

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. Set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by firewall.

Choose **Advanced Setup > NAT > DMZ host** to display the following page.

NAT -- DMZ Host

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

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

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

DMZ Host IP Address: [   ]

Apply/Save

Figure 19 DMZ host

In this page, enter the IP address of the DMZ host.

After finishing the settings, click the **Apply/Save** button to apply the settings.

If you want to clear the DMZ function of the host, please delete the IP address of the host in the field of **DMZ Host IP Address**, and then click the **Apply/Save** button.

5.2.6 Security

By default, the firewall is enabled. The firewall is used to block the file transmission between the Internet and your PC. It serves as a safety guard and permits only the authorized files to be sent to the LAN.

Note:
If the DSL router is configured to be bridge mode, IP filtering is disabled and the IP filtering interface does not appear.

Firewall

Choose **Security** > **Firewall** and the following page appears.

Click **Modify Firewall** or **Remove Firewall** to modify or remove the firewall. And click **Modify Rule** or **Remove Rule** to modify or remove the rule.

Click **Add Firewall**, and the following page appears.

- **name**: The name of the firewall.
- **interface**: You can select **a proper interface** from the drop-down list.
- **type**: You can select **In** or **Out** from the drop-down list.
- **defaultaction**: You can select **Permit** or **Drop** from the drop-down list.

MAC Filtering Setup

In some cases, you may want to manage Layer2 MAC address to block or permit a computer within the home network. When you enable MAC filter rules, the DSL router serves as a firewall that works at layer 2.

Note:

*MAC filtering is only effective on ATM PVCs configured in bridge mode. If the ATM PVCs are configured in other routing modes (such as PPPoE mode), the **MAC Filtering Setup** page does not appear.*

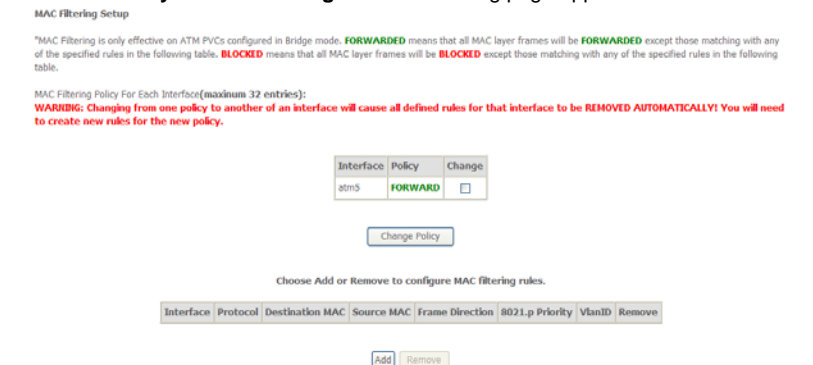Choose **Security** > **MAC Filtering** and the following page appears.

Figure 20 MAC filtering setup

In this page, you can add or remove the MAC filtering rule. You may change the MAC filtering policy from **FORWARDED** to **BLOCKED** by clicking the **Change Policy** button.

Click the **Add** button to display the following page.

Add MAC Filter

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

Protocol Type: [▼]
Destination MAC Address: [   ]
Source MAC Address: [   ]

Frame Direction: [LAN<=>WAN ▼]
802.1p Priority: [▼]
Tag VLAN ID [0-4094]: [   ]

WAN Interfaces (Configured in Bridge mode only)

[br_0_0_39/atm5 ▼]

[Apply/Save]

Figure 21 Adding a MAC filter

- **Protocol Type**: Select the proper protocol type.
- **Destination MAC Address**: Enter the destination MAC address.
- **Source MAC Address**: Enter the source MAC address.
- **Frame Direction**: The direction of transmission frame.
- **WAN Interface (Configured in bridge mode only)**: Select the proper WAN interface in the drop-down list.

After finishing setting, click **Apply/Save** to save and apply the filtering rule.

5.2.7 Parental Control

Time Restriction

Choose **Advanced Setup** > **Parental Control** > **Time Restriction**, and the following page appears.

Access Time Restriction -- A maximum 16 entries can be configured.

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

[Add] [Remove]

Click the **Add** button to display the following page.

Access Time Restriction

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

User Name

⦿ Browser's MAC Address 00:22:b0:68:de:69
○ Other MAC Address
(xx:xx:xx:xx:xx:xx)

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

Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)

[Apply/Save]

This page is used to control the time restriction to a special LAN device that connects to the DSL router. In this page, se the user name and configure the time settings.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.2.8 Quality of Service

Enabling QoS

Choose **Advance Setup > Quality of Service** and the following page appears.

QoS -- Queue Management Configuration

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

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

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

☐ Enable QoS

[Apply/Save]

Select **Enable QoS** to enable QoS and configure the default DSCP mark.

QoS -- Queue Management Configuration

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

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

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

☑ Enable QoS

Select Default DSCP Mark No Change (-1) ▾

Apply/Save

In this page, enable the QoS function and select the default DSCP mark. After finishing setting, click **Apply/Save** to save and apply the settings.

Note:

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

Queue Configuration

Choose **Advanced Setup** > **Quality of Service** > **QoS Queue**, and the following page appears.

63

GAN5.PT156A-B

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	33	atm0	SP	8		Path0		☑	
High Pri Queue	34	atm0	SP	1		Path0		☑	☐
Default Queue	35	atm2	SP	8		Path0		☑	
High Pri Queue	36	atm2	SP	1		Path0		☑	☐
Default Queue	37	atm3	SP	8		Path0		☑	
High Pri Queue	38	atm3	SP	1		Path0		☑	☐
Default Queue	39	atm4	SP	8		Path0		☑	
High Pri Queue	40	atm4	SP	1		Path0		☑	☐
Default Queue	41	ipoa0	SP	8		Path0		☑	
High Pri Queue	42	ipoa0	SP	1		Path0		☑	☐
Default Queue	43	atm5	SP	8		Path0		☑	
High Pri Queue	44	atm5	SP	1		Path0		☑	☐

[Add] [Enable] [Remove]

In this page, you can enable, add or remove a QoS rule.

Note:

The lower integer value for precedence indicates the higher priority.

Click the **Add** button to display the following page.

QoS Queue Configuration

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

Name: [   ]

Enable: Disable ▾

Interface: ▾

[Apply/Save]

- **Name:** Enter the name of QoS queue.
- **Enable:** Enable or disable the QoS queue.
- **Interface:** Select the proper interface for the QoS queue.

After finishing setting, click **Apply/Save** to save and apply the settings.

QoS Classification

Choose **Advanced Setup** > **Quality of Service** > **QoS Classification** and the following page appears.

QoS Classification Setup -- A maximum 32 entries can be configured.

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

													CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	TOS Check	802.1P Check	Queue Key	DSCP Mark	TOS Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Frame size	Enable	Remove
pvc1	1	LAN	IP				81.47.224.0/22							34		0					☑	☐
tr069	2	LAN	IP				80.58.63.192/26							34		0					☑	☐

[Add] [Enable] [Remove]

In this page, you can enable, add or remove a QoS classification rule.
Click the **Add** button to display the following page.

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. 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 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order: Last

Rule Status: Enable

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

Class Interface: LAN

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Frame size rage for Bridged interface(FROME:TO):

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID [0-4094]:

Apply/Save

In this page, enter the traffic name, select the rule order and the rule status, and specify the classification criteria and the classification results.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.9 Routing

Default Gateway

Choose **Advanced Setup** > **Routing** > **Default Gateway**, and the following page appears.

66

Routing -- Default Gateway

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

Selected Default Gateway Interfaces

ppp0

Available Routed WAN Interfaces

atm3
ipoa0
ppp1
ppp2
pppoa4

->
<-

TODO: IPV6 ********** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface ipoe_0_0_36/atm3

Apply/Save

In this page, you can modify the default gateway settings.

Select a proper WAN interface in the drop-down list of **Selected WAN Interface** as the system default gateway.

After finishing setting, click **Apply/Save** to save and apply the settings.

Static Route

Choose **Advanced Setup** > **Routing** > **Static Route** and the following page appears.

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

IP Version	DstIP/ PrefixLength	Gateway	Interface	Metric	Remove

Add   Remove

In this page, you can add or remove a static routing rule.

Click the **Add** button to display the following page.

Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

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

Metric:

Apply/Save

- **IP Version:** Select the IP version.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

After finishing setting, click **Apply/Save** to save and apply the settings.

RIP

Choose **Advanced Setup > Routing > RIP** and the following page appears.

Routing -- RIP Configuration

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm3	2	Passive	☐
ipoa0	2	Passive	☐
atm5	2	Passive	☐
ppp0	2	Passive	☐
ppp1	2	Passive	☐
ppp2	2	Passive	☐
pppoe4	2	Passive	☐

Apply/Save

In this page, if you want to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.10   DNS

DNS Server

Choose **Advanced Setup > DNS > DNS Server** and the following page appears.

68

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

○ DSelect DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces   Available WAN Interfaces

atm3
ppp0
ppp1
ppp2
pppoe4

⊙ Use the following Static DNS IP address:
Primary DNS server: 80.58.61.250
Secondary DNS server: 80.58.61.254

TODO: IPV6 ********** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

⊙ Obtain IPv6 DNS info from a WAN interface:
WAN Interface selected: ipoe_0_0_36/atm3

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

Apply/Save

In this page, you can select a DNS server interface from the available interfaces, manually enter the DNS server addresses, or obtain the DNS address from a WAN interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

Dynamic DNS

Choose **Advanced Setup > DNS > Dynamic DNS** and the following page appears.

Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Add   Remove

In this page, you are allowed to modify the DDNS settings.

Click the **Add** button to display the following page.

Add Dynamic DNS

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

D-DNS provider   DynDNS.org ▾

Hostname   [   ]
Interface   pppoe_0_1_1/ppp0.1 ▾

DynDNS Settings
Username   [   ]
Password   [   ]

                                    Apply/Save

- **D-DNS provider:** Select a proper DDNS server in the drop-down list.
- **Hostname:** It is the domain name and it can be modified.
- **Interface:** The interface that the packets pass through on the DSL router.
- **Username:** Enter the username for accessing the DDNS management interface.
- **Password:** Enter the password for accessing the DDNS management interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.11 DSL

Choose **Advanced Setup** > **DSL** and the following page appears. In this page, you can view the DSL settings. Usually, you can keep this factory default setting. The modem negotiates the modulation mode with the DSLAM. If you select **VDSL2 Enabled** check box, you can set the VDSL2 parameters on the right area.

GAN5.PT156A-B

DSL Settings

Select the modulation below.
- ☑ T1.413 Enabled
- ☑ ADSL2+ Enabled
- ☑ AnnexM Enabled

Select the phone line pair below.
- ◉ Inner pair
- ○ Outer pair

Capability
- ☑ Bitswap Enable
- ☐ SRA Enable

[Apply/Save] [Advanced Settings]

In this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.12 UPnP

Choose **Advanced Setup > UPnP** and the following page appears.

UPnP Configuration

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

- ☑ Enable UPnP

[Apply/Save]

In this page, you can enable or disable the UPnP function.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.13 DNS Proxy

Choose **Advanced Setup > DNS Proxy** and the following page appears.

DNS Proxy Configuration

☑ Enable DNS Proxy

Host name of the Broadband Router: dsl_route

Domain name of the LAN network: Home

Apply/Save

In this page, you can enable or disable the DNS proxy function.

After enabling the DNS proxy function, enter the host name of the broadband router and the domain name of the LAN network, and then click **Apply/Save** to save and apply the settings.

5.2.14 Print Server

Choose **Advanced Setup > Printer Server** and the following page appears.

Print Server settings

This page allows you to enable / disable printer support.

☐ Enable on-board print server.

Apply/Save

In this page, you can enable or disable the printer server.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.15   Storage Service

Storage Device

Choose **Advanced Setup > Storage Service > Storage Device** and the following page appears.

Figure 22 Storage Service

This page is used to display the information of the storage device that connects to the DSL router.

Server Configuration

Choose **Advanced Setup > Storage Service > Server Config** and the following page appears.

Figure 23 Server Configuration

Enable file sharing service, and then enter the workgroup name that is configured for file sharing server.

Click **Apply/ Save** to save and apply the settings.

User Configuration

Choose **Advanced Setup > Storage Service > User Config** and the following page appears.

GAN5.PT156A-B

File Share User Setup

Choose Add,Remove or Edit to Configure File Share User and Password

Active	User Name	Remove	Edit
Yes	root	☐	edit

Add   Remove

Figure 24

Click Add and the following page appears.

File Share Username and Password Add

☐ Active
User Name: _____
Password: _____
Retype to Confirm: _____

Apply/Save   Cancle

Enter the user name and password that is configured for file sharing server and then click **Apply / Save** to save and apply the settings.

Share Configuration

Choose **Advanced Setup > Storage Service > Share Config** and the following page appears.

File Share Configuration

Choose Add, Remove or Edit to configure a file share configuration.

Share Name	Share Directory	Share Description	Remove	Edit

Add   Remove

Click **Add** and the following page displays.

File Sharing - Share Configuration Add

Share Name:

Share Directory:

Share Descriptioin:

Apply/Save   Cancle

- **Share Name**: Name of the sharing directory created in workgroup that you have configured.
- **Share Directory**: The USB path where the share name created is placed.

Click **Apply / Save** to save and apply the settings.

5.2.16   DLNA

Choose **Advanced Setup > DLNA** and the following page appears.

GAN5.PT156A-B

Digital Media Server settings

This page allows you to enable / disable digital media server support.

☑ Enable on-board digital media server.

Interface `Default` ▾

Media Library Path `/mnt/usb1_1`

Apply/Save

This page allows you to enable/disable digital media server support. In this page, enter the media library path to run digital media server.

5.2.17 Interface Grouping

Choose **Advanced Setup > Interface Grouping** and the following page appears.

Interface Grouping -- A maximum 16 entries can be configured

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

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0	ENET1	
		ppp1	ENET2	
		ppp2	ENET3	
		atm3	ENET4	
		atm5	wlan0	
			wl0_Guest1	
			wl0_Guest2	
			wl0_Guest3	

Add Remove

Interface grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with the appropriate LAN and WAN interfaces using the **Add**

76

button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the default group. Only the default group has IP interface.

Click the **Add** button to display the following page.

Interface grouping Configuration

To create a new interface group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

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

3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

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

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

Group Name: _____

WAN Interface used in the grouping `ipoe_0_0_36/atm3`

Grouped LAN Interfaces

Available LAN Interfaces

```
ENET1
ENET2
ENET3
ENET4
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3
```

-> <-

Automatically Add Clients With the following DHCP Vendor IDs

_____
_____
_____
_____
_____

Apply/Save

77

In this page, please follow the on-screen configuration steps to configure the parameters of the interface grouping.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.18 IP Tunnel

5.2.18.1   IPv6 in IPv4

Choose **Advanced Setup > IP Tunnel** > **IPv6inIPv4** and the following page appears. The default value is IPv6 in IPv4 information.

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove

Add Remove

Click **Add** and the following page is displayed. In this page, you can add a new tunnel.

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name	
Mechanism:	6RD
Associated WAN Interface:	
Associated LAN Interface:	LAN/br0
⊙ Manual ○ Automatic	

IPv4 Mask Length:	
6rd Prefix with Prefix Length:	
Border Relay IPv4 Address:	

Apply/Save

5.2.18.2   IPv4 in IPv6

Choose **Advanced Setup > IP Tunnel** > **IPv4inIPv6** and the following page appears.

78

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	Remote IPv6 Address	Remove

Add Remove

Click **Add** and the following page appears. In this page, you can add a new tunnel.

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name

Mechanism: DS-Lite

Associated WAN Interface:

Associated LAN Interface: LAN/br0

⦿ Manual ◯ Automatic

Remote IPv6 Address:

Apply/Save

5.2.19   PCP

Choose **Advanced Setup > PCP** and the following page appears.

Port Control Protocol (PCP) Configuration -- draft-ietf-pcp-base-22

Associated WAN Interface:

Map Option Configuration   :   Add New Map

Server Name	Protocol Type	Internal Port	External IP Address	External Port	Lifetime	State	Edit

Peer Option Configuration   :   Add New Peer

Server Name	Protocol Type	Internal Port	External IP Address	External Port	Lifetime	Remote Port	Remote IP Address	State	Edit

Map Opcode

Choose **Advanced Setup > PCP** > **Map Opcode** and the following page appears.

Port Control Protocol -- Map Opcode part

Associated WAN Interface:	[dropdown]
PCP Server Name(IPv4/IPv6):	[ ]
Lifetime(seconds):	[ ]
Protocol:	TCP ▾
Internal Port[0-65535]:	[ ]
Suggested External Port[0-65535]:	[ ]
Suggested External IP Address(IPv4/IPv6):	[ ]

Port Control Protocol -- Option part

☐ Third Party: [ ]
☐ Prefer Failure:

[Apply/Save]

- **PCP Server Name (IPv4/IPv6):** The server side of the PCP protocol via which PCP clients request and manage explicit mappings.
- **Lifetime (seconds):** Requested Lifetime.
- **Internal Port [0-65535]:** Internal port for the mapping. The value 0 indicates "all ports".
- **Suggested External Port [0-65535]:** Suggested external port for the mapping. This is useful for refreshing a mapping, especially after the PCP server loses state. If the PCP client does not know the external port, or does not have a preference, it MUST use 0.
- **Suggested External IP Address (IPv4/IPv6):** Suggested external IPv4 or IPv6 address. This is useful for refreshing a mapping, especially after the PCP server loses state. If the PCP client does not know the external address, or does not have a preference, it MUST use the address-family-specific all-zeroes address.
- **Third Party:** It is an Internal Host when a PCP client wants to control a mapping other than itself.

- **Prefer Failure:** This Option indicates that if the PCP server is unable to map either the Suggested External Port or Suggested External Address, the PCP server should not create a mapping.

Peer Opcode

Choose **Advanced Setup > PCP** > **Peer Opcode** and the following page appears.

Port Control Protocol -- Peer Opcode part

Associated WAN Interface:	
PCP Server Name(IPv4/IPv6):	
Lifetime(seconds):	
Protocol:	TCP
Internal Port[0-65535]:	
Suggested External Port[0-65535]:	
Suggested External IP Address(IPv4/IPv6):	
Remote Peer Port[0-65535]:	
Remote Peer IP Address(IPv4/IPv6):	

Port Control Protocol -- Option part

☐ Third Party:

Apply/Save

- **PCP Server Name (IPv4/IPv6):** The server side of the PCP protocol via which PCP clients request and manage explicit mappings.
- **Lifetime (seconds):** Requested Lifetime.
- **Internal Port [0-65535]:** Internal port for the mapping.
- **Suggested External Port [0-65535]:** Suggested external port for the mapping. If the PCP client does not know the external port, or does not have a preference, it MUST use 0.
- **Suggested External IP Address (IPv4/IPv6):** Suggested External IP Address for the mapping. If the PCP client does not know the external address, or does not have a preference, it MUST use the address-family-specific all-zeroes address.

81

- **Remote Peer Port [0-65535]:** Remote peer's port for the mapping.
- **Remote Peer IP Address (IPv4/IPv6):** Remote peer's IP address from the perspective of the PCP client, so that the PCP client does not need to concern itself with NAT64 or NAT46. This field allows the PCP client and PCP server to disambiguate multiple connections from the same port on the Internal Host to different servers. An IPv6 address is represented directly, and an IPv4 address is represented using the IPv4-mapped address syntax.
- **Third Party**: It is an Internal Host when a PCP client wants to control a mapping other than itself.

5.2.20   Multicast

Choose **Advanced Setup > Multicast** and the following page appears.

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval (s):	15
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval (s):	125
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Groups:	10
Maximum Multicast Data Sources (for IGMPv3):	10
Maximum Multicast Group Members:	10
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑

Apply/Save

In this page, you can configure the multicast parameters.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.21 Packet Acceleration

Choose **Advanced Setup > Packet Acceleration** and the following page appears.

In this page, you can enable packet flow accelerator.

83

Packet Acceleration

☑ Enable Packet Flow Accelerator

[Apply/Save]

5.3 Wireless

Choose **Wireless** and the submenus of **Wireless** are shown as below:

Wireless
  Basic
  Security
  MAC Filter
  Wireless Bridge
  Advanced
  Station Info
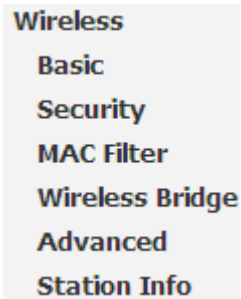
5.3.1 Basic Settings

Choose **Wireless** > **Basic** to display the following page. In this page, the figure in the right area is 2-dimensional code. It includes the wireless SSID and password. You can obtain the wireless SSID and password through scanning this figure.

84

GAN5.PT156A-B

Wireless -- Basic

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

- ☑ Enable Wireless
- ☐ Enable Autogeneration
- ☐ Hide Access Point
- ☐ Clients Isolation
- ☐ Disable WMM Advertise
- ☐ Enable Wireless Multicast Forwarding (WMF)

SSID: WLAN_281E

BSSID: 5e:1e:e3:63:28:13

Country: SPAIN

Max Clients: 16

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
☐	Broadcom2	☐	☐	☐	☐	16	N/A
☐	Broadcom3	☐	☐	☐	☐	16	N/A
☐	Broadcom4	☐	☐	☐	☐	16	N/A

[Apply/Save]

This page allows you to configure the basic features of the wireless LAN interface.

- **Enable Wireless:** Enable or disable the wireless function.
- **Hide Access Point:** if you want to hide any access point for your router, select this option, and then a station cannot obtain the SSID through the passive scanning.
- **Clients Isolation:** When many clients connect to the same access point, they can access each other. If you want to disable the access between the clients that connect to the same access point, you can select this option.
- **Disable WMM Advertise:** After enabling this option, the transmission performance multimedia of the voice and video data can be improved.
- **Enable Wireless Multicast Forwarding (WMF):** After enabling this option, the transmission quality of video service such as IPTV can be improved.
- **SSID**: For the security reason, you should change the default SSID to a unique name.
- **BSSID:** Display the MAC address of the wireless interface.
- **Country**: The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, the channel will adjust according to nations to adapt to each nation's frequency provision.

85

- **Max Clients:** Specify the maximum wireless client stations to be enabled to link with AP. Once the clients exceed the max vlaue, all other clients are refused. The value of maximum clients is 16.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

After finishing setting, click **Apply/Save** to save the basic wireless settings and make the settings take effect.

5.3.2 Security

Choose **Wireless** > **Security** to display the following page.

This page allows you to configure the security features of the wireless LAN interface. In this page, you can configure the network security settings by the Wi-Fi Protected Setup (WPS) method or setting the network authentication mode.

- **WPS Setup**

GAN5.PT156A-B

WPS Setup

Enable **WPS**   Enabled ▼

WPS Version   Version1.0 ▼

Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
⦿ Push-Button
○ Enter STA PIN ○ Use AP PIN   [Add Enrolee]

There are 2 primary methods used in the Wi-Fi Protected Setup:
- PIN entry, a mandatory method of setup for all WPS certified devices.
    – **Enter STA PIN**: If you select it, you need to enter the station PIN from client.
    – **Use AP PIN**: The PIN is generated by AP.
- Push button configuration (PBC), an actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

If you are using the PIN method, you will need a Registrar (access point/wireless router) to initiate the registration between a new device and an active access point/wireless router. (**Note:** *The PBC method may also need a Registrar when used in a special case where the PIN is all zeros*)

In order to use the push-button for WPS authentication, you must ensure that the network card support the function. if it supports, you need not to do any configuration. You can press the WPS button directly to enable the WPS function.

- **Manual Setup AP**

This page provides 9 types of network authentication modes, including Open, Shared, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

87

GAN5.PT156A-B

Manual Setup AP

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

Select SSID: WLAN_281E ▾

Network Authentication: WPA-PSK ▾

                               Open
                               Shared
WPA/WAPI passphrase: 802.1X   k here to display
WPA Group Rekey Interval: WPA
WPA/WAPI Encryption: WPA-PSK
                               WPA2
WEP Encryption: WPA2 -PSK
                               Mixed WPA2/WPA
                               Mixed WPA2/WPA -PSK

                               Apply/Save

- Open Mode

Network Authentication: Open ▾

WEP Encryption: Enabled ▾
Encryption Strength: 64-bit ▾
Current Network Key: 1 ▾
Network Key 1:   D001EE363281E
Network Key 2:   D001EE363281E
Network Key 3:   D001EE363281E
Network Key 4:   D001EE363281E

                               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

                               Apply/Save

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the Open mode.
- **WEP Encryption:** Enable or disable WEP encryption. After enabling this function, you can set the encryption strength, current network key, and network keys.
- **Encryption Strength:** You can set 64-bit or 128-bit key.
- **Current Network Key:** The current key that you use.
- **Network Key1/2/3/4:** Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

88

- Shared Mode

Network Authentication:	Shared
WEP Encryption:	Enabled
Encryption Strength:	64-bit
Current Network Key:	1
Network Key 1:	D001EE363281E
Network Key 2:	D001EE363281E
Network Key 3:	D001EE363281E
Network Key 4:	D001EE363281E

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

Apply/Save

The parameters' description of shared mode, please refer to the **Open Mode**.

- 802.1x

Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled
Encryption Strength:	64-bit
Current Network Key:	2
Network Key 1:	D001EE363281E
Network Key 2:	D001EE363281E
Network Key 3:	D001EE363281E
Network Key 4:	D001EE363281E

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

Apply/Save

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the 802.1X in the drop-down list.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.

89

- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WEP Encryption:** You can only select **Enabled**.
- **Encryption Strength:** You can set 64-bit or 128-bit key.
- **Current Network Key:** The current key that you use.
- **Network Key1/2/3/4:** Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

- WPA Mode

Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	TKIP+AES
WEP Encryption:	Disabled

Apply/Save

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA mode.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA-PSK Mode

GAN5.PT156A-B

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA-PSK mode.
- **WPA/WAPI passphrase:** The key for WPA encryption. Click the **Click here to display** button to display the current key. The default key is 87654321.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA2 Mode

GAN5.PT156A-B

- ● **Select SSID:** Select a SSID for configuring the security settings.
- ● **Network Authentication:** Select the WPA2 mode.
- ● **WPA2 Preauthentication:** Enable or disable pre-authentication.
- ● **Network Re-auth Interval:** Set the network re-auth interval.
- ● **WPA Group Rekey Interval:** Setting the interval for renewing key.
- ● **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- ● **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- ● **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- ● **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA2-PSK

Network Authentication:	WPA2 -PSK
WPA/WAPI passphrase:	●●●●●●●●●●●●●●●●● Click here to display
WPA Group Rekey Interval:	0
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

Apply/Save

The parameters' description of WPA2-PSK mode, please refer to the **WPA-PSK mode**.

- Mixed WPA2/WPA

GAN5.PT156A-B

The parameters' description of Mixed WPA2/WPA mode, please refer to the **WPA2 mode**.

- Mixed WPA2/WPA-PSK

The parameters' description of Mixed WPA2/WPA-PSK mode, please refer to the **WPA-PSK mode**.

5.3.3 MAC Filter

Choose **Wireless > MAC Filter** to display the following page.

Wireless -- MAC Filter

Select SSID: [WLAN_281E ▼]

MAC Restrict Mode: ⦿ Disabled ◯ Allow ◯ Deny

MAC Address	Remove

[Add] [Remove]

This page is used to allow or reject the wireless clients to access the wireless network of the wireless router.

In this page, you can add or remove the MAC filters.

The MAC restrict modes include **Disabled**, **Allow**, and **Deny**.

● **Disabled**: Disable the wireless MAC address filtering function.

● **Allow**: Allow the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.

● **Deny**: Reject the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.

Click the **Add** button to display the following page.

Wireless -- MAC Filter

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

MAC Address: [   ]

[Apply/Save]

94

In this page, enter the MAC address of the wireless client, and then click the **Apply/Save** button to add the MAC address to the MAC address list.

5.3.4 Wireless Bridge

Choose **Wireless > Wireless Bridge** to display the following page.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode:	Access Point
Bridge Restrict:	Enabled
Remote Bridges MAC Address:	

[Refresh] [Apply/Save]

This page allows you to configure the wireless bridge features of the wireless LAN interface.

- **AP mode**: you may select Access Point or Wireless Bridge.
- **Bridge Restrict**: Enable or disable the bridge restrict function.
- **Remote Bridges MAC Address**: Enter the remote bridge MAC address.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.3.5 Advanced Settings

Choose **Wireless** > **Advanced** to display the following page. This page allows you to configure the advanced features of the wireless LAN interface. Usually, you do not need to change the settings in this page.

Wireless -- Advanced

This page allws you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click 'Apply/Save' to configure the advanced wireless options.

Band:	2.4GHz	
Channel:	Auto	Current: 6 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz in Both Bands	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
RX Chain Power Save:	Disable	Power Save status: Full Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress Technology:	Enabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Apply/Save

- **Band:** You can select 2.4GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
- **Auto Channel Timer (min):** Specifies the timer of auto channelling.
- **802.11n/EWC:** Select **disable** 802.11n or **Auto**.
- **Bandwidth:** Select the bandwidth for the network. You can select **20MHz in Both Bands**, **20MHz in 2.4G Band and 40MHz in 5G Band**, or **40MHz in Both Bands.**
- **802.11n Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **802.11n Protection:** The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without "speaking" at the same time.

- **Support 802.11n Client Only:** Only stations that are configured in 802.11n mode can associate.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).   Default (100) is recommended.
- **XPress Technology:** Select Enable or Disable. This is a special accelerating   technology for IEEE802.11g. The defaule is Disabled.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
- **WMM (Wi-Fi Multimedia):** Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
- **WMM No Acknowledgement:** Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which

decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.

● **WMM APSD:** APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

Note:

The advanced wireless setting is only for the advanced user. For the common user, do not change any settings in this page.

5.3.6 Station Info

Choose **Wireless** > **Station Info** to display the following page.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

Refresh

This page shows the authenticated wireless stations and their status.

5.4   Diagnostics

5.4.1 Diagnostics

Click **Diagnostics** > **Diagnostics**, and the following page appears.

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider.

You may diagnose the connection by clicking the **Test** button or clicking the **Test With OAM F4** button. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

98

pppoe_0_8_32 Diagnostics

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

Test the connection to your local network

Test your ENET1 Connection:	FAIL	Help
Test your ENET2 Connection:	FAIL	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

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

Test the connection to your Internet service provider

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

Next Connection

Test   Test With OAM F4

Diagnostic Toolkit

Click **Diagnostics** > **Diagnosis Toolkit**, and the following page appears. Enter
IPv4 address or domain name, and then click **Test**.

Traceroute Test

IPv4 Address or Domain Name: [   ]   Test

5.5 Management

Choose **Management** and the submenus of **Management** are shown as below:

99

GAN5.PT156A-B

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

5.5.1 Settings

Backup

Choose **Management > Settings > Backup** to display the following page.

Settings - Backup

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

Backup Settings

In this page, click the **Backup Settings** button to save your router's settings to your local PC.

Update

Choose **Management > Settings > Update**, and the following page appears.

Tools -- Update Settings

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

Settings File Name: [＿＿＿＿＿] Browse...

Update Settings

In this page, click the **Browse…** button to select the correct new settings file, and then click the **Update Settings** button to update the router's settings.

Restore Default

Choose **Management > Settings > Restore Default** to display the following page.

Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Restore Default Settings

In this page, click the **Restore default settings** button, and then system returns to the default settings.
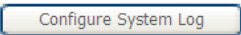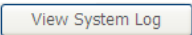
5.5.2 System Log

Choose **Management > System Log** to display the following page.

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

In this page, you are allowed to configure the system log and view the security log.

● **Configuring the System Log**

Click the **Configure System Log** button to display the following page.

System Log -- Configuration

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

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

Log: ⊙ Disable ○ Enable

Log Level: Debugging
Display Level: Error
Mode: Local
                 Local
                 Remote
                 Both

Apply/Save

In this page, you can set 3 types of system log modes, including **Local**, **Remote**, and **Both**.

- **Local:** When selecting **Local**, the events are recorded in the local memory.
- **Remote:** When selecting **Remote**, the events are sent to the specified IP address and UDP port of the remote system log server.
- **Both:** When selecting **Both**, the events are recorded in the local memory or sent to the specified IP address and UDP port of the remote system log server.

After finishing setting, click the **Apply/Save** button to save and apply the settings.
Note:
*If you want to log all the events, you need to select the **Debugging** log level.*

- **View System Log**

Click the **View System Log** button to display system log information.

Click the **Refresh** button to refresh the system log. Click the **Close** button to exit.

5.5.3 TR-69 Client

Choose **Management > TR-069Client** to display the following page.

TR-069 client - Configuration

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

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

Inform	⊙ Disable ○ Enable
Certificate Management:	[View/Edit Certificate]
Inform Interval:	86400
ACS URL:	https://main.acs.telefoni
ACS User Name:	ACS1234
ACS Password:	•••••••
WAN Interface used by TR-069 client:	Any_WAN
Display SOAP messages on serial console	⊙ Disable ○ Enable
☑ Connection Request Authentication	
Connection Request User Name:	ACSCR1234
Connection Request Password:	••••••••
Connection Request Port:	7547
Connection Request URL:	

[Apply/Save] [GetRPCMethods]

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

In this page, you may configure the parameters such as the ACS URL, ACS password, and connection request user name.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.5.4 Internet Time

Choose **Management > Internet Time** to display the following page.

Time settings

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

☐ Automatically synchronize with Internet time servers

Apply/Save

In this page, you may configure the router to synchronize its time with the Internet time servers.

After enabling **Automatically synchronize with Internet time servers**, the following page appears.

Time settings

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

☐ Automatically synchronize with Internet time servers

Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server: `hora.ngn.rima-tde.net`
Second NTP time server: `ntp0.voip.telefonica.de`
Third NTP time server: `None`
Fourth NTP time server: `None`
Fifth NTP time server: `None`

Current Router Time : Fri Oct 1 02:38:04 2010
Time zone offset: (GMT+01:00) Brussels, Copenhagen, Madrid, Paris

☑ Enable manual daylight saving, overwrite automatic rule

		Month	Week	Day	Time
Daylight Saving Dates :	Start	Oct	Last	Sun	2 am
	End	Mar	Last	Sun	3 am

Apply/Save

In this page, set the proper time servers, and then click the **Apply/Save** button to save and apply the settings.

5.5.5 Access Control

Passwords

Choose **Management > Access Control > Passwords**, and the following page appears.

GAN5.PT156A-B

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 15 characters and click 'Apply/Save' to change or create passwords. Note: Password cannot contain a space.

Username:	
New Username:	
Old Password:	
New Password:	
Confirm Password:	

Apply/Save

In the page, you can modify the username and password of different users.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

Services Control

Choose **Management > Access Control > Services Control** and the following page appears.

105

Access Control -- Services

Services access control list (SCL) enable or disable the running services.

Services	LAN	WAN	Port
HTTP	☑ enable	☑ enable	80
TELNET	☑ enable	☑ enable	23
FTP	☑ enable	☑ enable	21
TFTP	☑ enable	☐ enable	69
ICMP	☑ enable	☑ enable	0
SAMBA	☑ enable	☐ enable	445

Apply/Save

In this page, you can enable or disable the different types of services.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.5.6 Update Software

Choose **Management > Update Software**, and the following page appears.

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 Broadband Router will reboot.

Software File Name: [   ] Browse...

Update Software

If you want to upload the software, click the **Browse…** button to choose the new software, and then click the **Update Software** button.

Note:
When software update is in progress, do not shut down the router. After software update completes, the router automatically reboots.

Please make sure that the new software for updating is correct, and do not use other software to update the router.

5.5.7 Reboot

Choose **Management > Reboot** and the following page appears.

Click the button below to reboot the router.

Reboot

In this page, click the **Reboot** button, and then the router reboots.

5.5.8 Logout

Choose the **Logout** to log out of the web configuration page.

6 Q&A

(1) **Q**: Why all the indicators are off?

    A: Check the following:

- The connection between the power adaptor and the power socket.
- The status of the power switch.

(2) **Q**: Why the **Ethernet** indicator is off?

    A: Check the following:

- The connection between the ADSL router and your computer, hub, or switch.
- The running status of your PC, hub, or switch.

(3) **Q**: Why the **ADSL** indicator is off?

    A: Check the connection between the "**ADSL**" port of router and the wall jack.

(4) **Q**: Why Internet access fails while the **ADSL** indicator is on?

    A: Check whether the VPI, VCI, user name, and password are correctly entered.

(5) **Q**: Why I fail to access the web configuration page of the DSL router?

    A: Choose **Start** > **Run** from the desktop, and ping *192.168.1.1* (IP address of the DSL router). If the DSL router is not reachable, check the type of the network cable, the connection between the DSL router and the PC, and the TCP/IP configuration of the PC.

(6) **Q**: How to load the default settings after incorrect configuration?

    A: To restore the factory default settings, turn on the device, and press the reset button for about 1 second, and then release it. The default IP address and the subnet mask of the DSL router are **192.168.1.1** and **255.255.255.0**, respectively.

- User/password of super user: **1234**/**1234**

FCC - PART 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA.　On the bottom of the device of this equipment is a label that contains, among other information, a product identifier in the format US: SGEDL01BR5500UN　and REN: 0.09B for this equipment.

This equipment uses the following USOC jacks: RJ-11 Jacks！

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA.　A compliant telephone cord and modular plug is provided with this product.　It is designed to be connected to a compatible modular jack that is also compliant.　See installation instructions for details.

REN (RINGER EQUIVALENT NUMBERS) STATEMENT　Notice: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

If this equipment US: SGEDL01BR5500UN causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible.　Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment US ID , for repair or warranty information, please contact Shenzhen Gongjin Electronics Co.,Ltd. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs.　Contact the state public utility commission, public service commission or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this US: SGEDL01BR5500UN does not disable your alarm equipment.　If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

FCC STATEMENT

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

The grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. Such modifications could void the user's authority to operate the equipment.

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

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

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

FCC RF Radiation Exposure Statement

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