



**DG-BG1100U**  
**ADSL2/2+ Combo Broadband Router**  
**User Manual**

V1.1  
2011-07-25

As our products undergo continuous development the specifications are subject to change without prior notice

## COPYRIGHT

Copyright ©2011 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

## Trademarks:

DIGISOL™ is a trademark of Smartlink Network Systems Ltd. All other trademarks are the property of the respective manufacturers.

## Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

## Index

1. Safety Precautions.....	5
2.....	6
2.1 Application.....	8
2.2 Environment.....	8
2.3 System Requirements.....	8
2.4 LED Status.....	8
2.4.1 Front Panel.....	9
2.4.2 Rear panel.....	9
3. Hardware Installation.....	10
3.1 ADSL Connection of Router.....	10
3.2 USB Installation.....	11
4. Web Configuration Management.....	12
4.1 Logging In to the Router.....	12
4.2 Quick Setup – PPPoE Configuration.....	13
4.3 DSL Router Device Information.....	18
4.3.1 Summary of Device information.....	19
4.3.2 WAN Interface Information.....	19
4.3.3 Statistics.....	20
4.3.3.1 ADSL BER Test.....	22
4.3.4 Route Table Information.....	24
4.3.5 ARP Table Information.....	24
4.3.6 DHCP IP Lease Information.....	24
4.4 Advanced Setup.....	25
4.4.1 WAN Configuration.....	25
4.4.1.1 Adding a PPPoE PVC.....	26
4.4.1.2 Adding a PPPoA PVC.....	31
4.4.1.3 Adding an MER PVC.....	34
4.4.1.4 Adding an IPoA PVC.....	39
4.4.1.5 Adding a Bridge PVC.....	43
4.4.2 LAN Configuration.....	46
4.4.2.1 Defining the Private IP Address for the DSL Router.....	47
4.4.2.2 Enabling IGMP Snooping.....	47
4.4.2.3 Configuring the DHCP Server.....	48
4.4.2.4 Reserve IP Address.....	48
4.4.3 NAT.....	48
4.4.3.1 Virtual Servers.....	49
4.4.3.2 Port Triggering.....	51
4.4.3.3 DMZ Host.....	52

4.4.4 Security.....	53
4.4.4.1 Outgoing IP Filtering Setup.....	54
4.4.4.2 Incoming IP Filtering Setup.....	58
4.4.4.3 Parental Control.....	61
4.4.5 Quality of Service.....	62
4.4.5.1 Enabling QoS.....	62
4.4.5.2 QoS - Queue Configuration.....	63
4.4.5.3 QoS - QoS Classification.....	64
4.4.6 Routing.....	66
4.4.6.1 Routing – Default Gateway.....	66
4.4.6.2 Static Routes.....	67
4.4.7 DNS.....	68
4.4.7.1 DNS Server.....	68
4.4.7.2 Dynamic Domain Name Service (DDNS).....	69
4.4.8 DSL.....	71
4.5 Diagnostics.....	72
4.6 Management.....	73
4.6.1 Setting.....	73
4.6.2 System Log.....	74
4.6.3 SNMP Agent.....	75
4.6.3.1 SNMP Protocol.....	75
4.6.3.2 Configuration.....	75
4.6.4 Internet Time.....	76
4.6.5 Access Control.....	77
4.6.6 Update Software.....	79
4.6.7 Save/Reboot.....	79
5. Q&A.....	80

## 1. Safety Precautions

- Use volume labels to mark the type of power.
- Use the power adapter which 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 exists or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is too 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 so. Because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

## 2.

1. Safety Precautions.....	5
2.....	6
2.1 Application.....	8
2.2 Environment.....	8
2.3 System Requirements.....	8
2.4 LED Status.....	8
2.4.1 Front Panel.....	9
2.4.2 Rear panel.....	9
3. Hardware Installation.....	10
3.1 ADSL Connection of Router.....	10
3.2 USB Installation.....	11
4. Web Configuration Management.....	12
4.1 Logging In to the Router.....	12
4.2 Quick Setup – PPPoE Configuration.....	13
4.3 DSL Router Device Information.....	18
4.3.1 Summary of Device information.....	19
4.3.2 WAN Interface Information.....	19
4.3.3 Statistics.....	20
4.3.3.1 ADSL BER Test.....	22
4.3.4 Route Table Information.....	24
4.3.5 ARP Table Information.....	24
4.3.6 DHCP IP Lease Information.....	24
4.4 Advanced Setup.....	25
4.4.1 WAN Configuration.....	25
4.4.1.1 Adding a PPPoE PVC.....	26
4.4.1.2 Adding a PPPoA PVC.....	31
4.4.1.3 Adding an MER PVC.....	34
4.4.1.4 Adding an IPoA PVC.....	39
4.4.1.5 Adding a Bridge PVC.....	43
4.4.2 LAN Configuration.....	46
4.4.2.1 Defining the Private IP Address for the DSL Router.....	47
4.4.2.2 Enabling IGMP Snooping.....	47
4.4.2.3 Configuring the DHCP Server.....	48
4.4.2.4 Reserve IP Address.....	48

4.4.3 NAT.....	48
4.4.3.1 Virtual Servers.....	49
4.4.3.2 Port Triggering.....	51
4.4.3.3 DMZ Host.....	52
4.4.4 Security.....	53
4.4.4.1 Outgoing IP Filtering Setup.....	54
4.4.4.2 Incoming IP Filtering Setup.....	58
4.4.4.3 Parental Control.....	61
4.4.5 Quality of Service.....	62
4.4.5.1 Enabling QoS.....	62
4.4.5.2 QoS - Queue Configuration.....	63
4.4.5.3 QoS - QoS Classification.....	64
4.4.6 Routing.....	66
4.4.6.1 Routing – Default Gateway.....	66
4.4.6.2 Static Routes.....	67
4.4.7 DNS.....	68
4.4.7.1 DNS Server.....	68
4.4.7.2 Dynamic Domain Name Service (DDNS).....	69
4.4.8 DSL.....	71
4.5 Diagnostics.....	72
4.6 Management.....	73
4.6.1 Setting.....	73
4.6.2 System Log.....	74
.....	75
4.6.3 SNMP Agent.....	75
4.6.3.1 SNMP Protocol.....	75
4.6.3.2 Configuration.....	75
4.6.4 Internet Time.....	76
4.6.5 Access Control.....	77
4.6.6 Update Software.....	79
4.6.7 Save/Reboot.....	79
5. Q&A.....	80

## Article I.

The Router is a highly ADSL2+ integrated access device and can support ADSL link downstream up to 24 Mbps and upstream up to 1 Mbps, which is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet. The Router combines high-speed ADSL Internet connection. It is usually preferred to provide high access performance applications for the individual users, the SOHO, the small enterprise and so on.

The router is easy to install and use. The Router can be connected to an Ethernet LAN or a computer via standard Ethernet ports. The ADSL connection is made by using ordinary telephone line with standard connectors. Multiple workstations can be connected to the Internet by using a single wide area network (WAN) interface and a

single global IP address. The advanced security enhancements, packet filtering and port redirection is able to protect your network from potentially devastating intrusions by malicious agents.

You can access the web-based management interface to realize network and router management by 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
- Shared broadband internet access
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

## 2.2 Environment

- Operating temperature: 0°C~40 °C (32°F~104°F)
- Storage temperature: -10 °C ~55 °C (14°F~131°F)
- Operating humidity: 10%~95%, non-condensing
- Storage humidity: 5%~95%, non-condensing
- Power adapter input: 100 V—240 V AC, 50/60 Hz

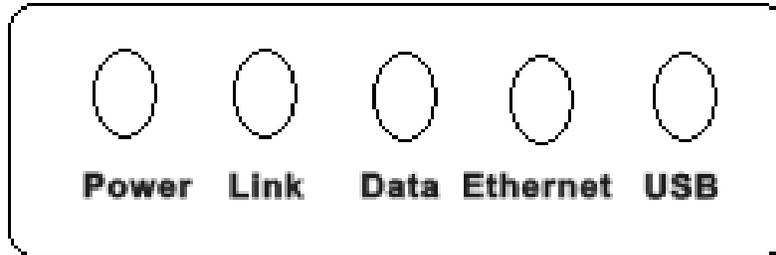
## 2.3 System Requirements

- Pentium 233 MHz or above
- Memory: 64 MB or above
- 10M Base-T Ethernet or above
- Windows 9x, Windows 2000, Windows XP, Windows ME, Windows NT or above
- Ethernet network interface card

## 2.4 LED Status

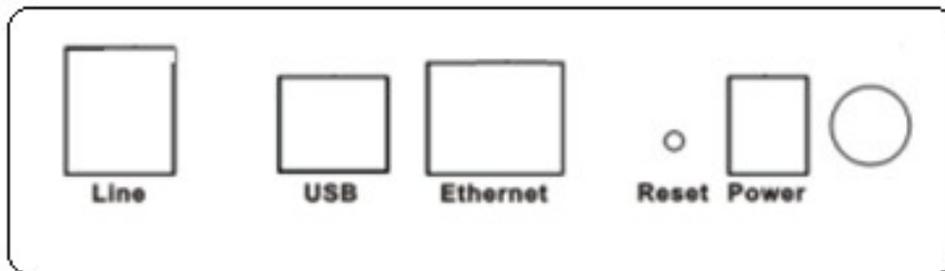
**Note:** *The figures in this document are for reference only.*

**2.4.1 Front Panel**



LED	Status	Description
Power	Off	Power is off.
	On	Power is on and the device operates normally.
Link	Off	No signal is detected.
	Blink	DSL line training is in progress.
	On	DSL line connection is up.
Data	Blink	Traffic is in progress.
Ethernet	Off	No Ethernet signal is detected.
	Blink	User data is going through Ethernet port.
	On	Ethernet interface is ready to work.
USB	Off	No signal is detected.
	Blink	User data is going through USB port.
	On	USB interface is ready to work.

**2.4.2 Rear panel**



Interface	Description
Line	RJ-11 port: Connect the router to ADSL connector or splitter through telephone line.
USB	USB device interface for connecting to PC or other network devices.

Interface	Description
Ethernet	RJ-45 port, for connecting the router to a PC or other network devices through Ethernet cable.
Reset	To restore the factory default, keep the device powered on, push a needle into the hole for about 1 second, and then release.
Power	Power interface, for connecting the power adapter.
	Power switch, on the side of power interface.

### 3. Hardware Installation

The router contains one Ethernet LAN, and a Line (WAN) interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The router should not be located where it is exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

#### 3.1 ADSL Connection of Router

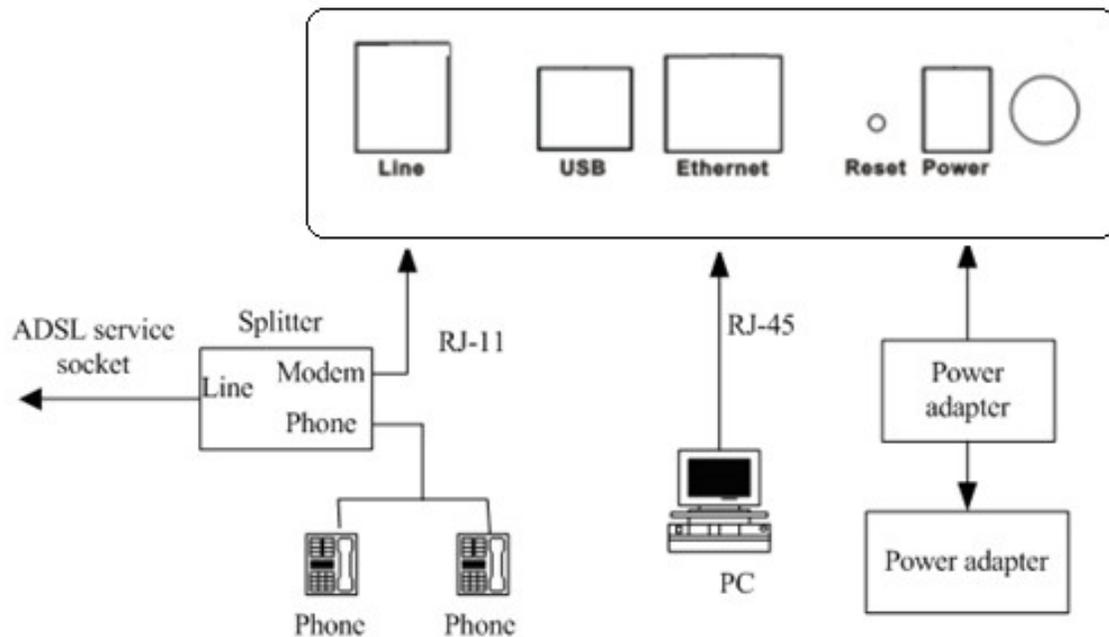
1. Connect the Line port of the router and the Modem port of the splitter with a telephone cable; connect the phone to the phone port of the splitter through a cable; and connect the incoming line to the Line port of the splitter.

The splitter has three ports:

- LINE: Connect to a wall phone jack (RJ-11 jack)
- Modem: Connect to the Line interface of the router
- PHONE: Connect to a telephone set

2. Connect the Ethernet port of the router to the network card of the PC through an Ethernet line.

3. Plug the power adapter to the wall outlet and then connect the other end of it to the Power port of the router.



### 3.2 USB Installation

To connect the DSL router to the USB port of PC, perform the following:

- Connect the USB cable to the USB port on the DSL router. The cable has two different connectors; you may have to try both connectors and the connector is keyed so try different orientations.
- Connect the other end of the USB cable into the USB port of PC.
- For USB installation on Windows XP, once the PC powers up, a message appears in the system tray indicating that new hardware is found.



Then, the **Found New Hardware Wizard** dialog box pops up. Select **Install the software automatically (Recommended)** and insert the Driver CD-ROM. Click Next. The system searches CD-ROM for the best USB driver. Then you can install the USB driver according to the instructions.

## 4. Web Configuration Management

### 4.1 Logging In to the Router

**Step 1** Open the Internet Explorer or Netscape Web browser and enter `http://192.168.1.1` (default IP address).

**Step 2** Connect the router. Enter the user name and password.

- The default user name and password of the super user are admin and admin.
- The default user name and password of the common user are user and user.



After logging in the router as a super user, you can query, configure, and modify all configurations of the router. You can also diagnose the router system.

## 4.2 Quick Setup – PPPoE Configuration

After finishing logging, the Quick Setup page appears shown as the following figure, if you do not configure the PVC of WAN connection.

*Note: This section describes the procedure for adding PVC 0/35 (PPPoE mode). If you want to configure the WAN connection in another mode, refer to 3.4.1 WAN Configuration.*

**Step 1** In this page, you can modify VPI/VCI, and QoS.

**DIGISOL™** **DG-BG1100U** **ADSL**  
Broadband Router

**Device Info**  
**Quick Setup**  
**Advanced Setup**  
**Diagnostics**  
**Management**

**Quick Setup**

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

**ATM PVC Configuration**

The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.

VPI: [0-255]

VCI: [32-65535]

**Enable Quality Of Service**

Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

Next

**Step 2** Click Next and select the type of network protocol and encapsulation that your ISP instructs you to use.

**Connection Type**

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

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

**Encapsulation Mode** 

**Step 3** After proper configuration, click Next, and the following page appears.

**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:

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode

In this page, you can modify the PPP user name, PPP password, authentication method and so on.

- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **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:** A full cone 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.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time.
- **PPP IP extension:** If this function is enabled, the WAN IP address obtained by the router through built-in dial-up can be directly assigned to the PC being attached to the router (at this time, the router connects to only one PC).
- **Use Static IP Address:** If this function is disabled, the router obtains an IP address assigned by uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the router uses this IP address as the WAN IP address.
- **Retry PPP password on authentication error:** If this function is enabled, DSL will retry PPP password on authentication while authenticating with right password failure.
- **Enable PPP Debug Mode:** The PPP Debug Mode enables connection debugging facilities. If this function is enabled, pppd will log the contents of all control packets sent or received in a readable form. The packets are logged through syslog with facility daemon and level debug.

**Step 4** After entering the PPP user name and password, click Next and the following page appears. In this page, you can modify the service name, and enable or disable the IGMP multicast and WAN service.

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name

Back Next

- **IGMP Multicast:** IGMP proxy. For example, if you wish that the PPPoE mode supports IPTV, enable this function.
- **WAN Service:** Enable it, unless you do not want to active the PVC.

**Step 5** Click next and the following page appears. In this page, you can set the IP Address and Subnet Mask of DSL Router for LAN interface. Usually, you can use the default configurations.

#### Device Setup

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

IP Address:   
 Subnet Mask:

- Disable DHCP Server  
 Enable DHCP Server

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

Configure the second IP Address and Subnet Mask for LAN interface

**Step 6** Click Next and ensure that the below settings match the settings provided by your ISP. See the following figure.

#### WAN Setup - Summary

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

<b>PORT / VPI / VCI:</b>	0 / 0 / 35
<b>Connection Type:</b>	PPPoE
<b>Service Name:</b>	pppoe_0_0_35_1
<b>Service Category:</b>	UBR
<b>IP Address:</b>	Automatically Assigned
<b>Service State:</b>	Enabled
<b>NAT:</b>	Enabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.  
 NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

**Step 7** Click Save/Reboot to save your configurations. The setting for PPPoE is complete.

*Note: After the Quick Setup is completed, you can add the new WAN configuration in Advanced Setup. Select Advanced Setup > WAN, the following figure appears, you can click Add to add WAN configuration.*

### 4.3 DSL Router Device Information

Choose Device Info, the following page appears. Choose items to view the relative information.

#### 4.3.1 Summary of Device information

This page contains the following information:

- LAN IP Address: the management IP address.
- Default Gateway: In the bridging mode there is no gateway. In other modes, it is the address of the uplink equipment, for example, PPPoE/PPPoA.

- DNS Server: In the PPPoE/PPPoA mode, it is obtained from the uplink equipment. In the bridging mode, there is no DNS Server address and you can manually enter the information.

<b>Device Info</b>
Summary
<b>WAN</b>
Statistics
Route
ARP
DHCP
Quick Setup
Advanced Setup
Diagnostics
Management

**Device Info**

Board ID:	DG-BG1100U
Software Version:	DG_110701
Bootloader (CFE) Version:	before 1.0.37-5.12

This information reflects the current status of your DSL connection.

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

### 4.3.2 WAN Interface Information

Click **WAN** and the following page appears. The **WAN Info** page displays the status and the connect or disconnect button, depending on the selected connection mode. This page contains the following informations for each WAN connection:

**WAN Info**

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

### 4.3.3 Statistics

This page contains the following four parts:

- Statistics of LAN
- Statistics of WAN
- Statistics of ATM
- Statistics of ADSL

#### Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	411199	3162	0	0	1494185	3209	0	0
USB	0	0	0	0	0	0	0	0

Reset Statistics

Figure 1 Statistics of LAN

#### Statistics -- WAN

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

Reset Statistics

Figure 2 Statistics of WAN

#### ATM Interface Statistics

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

#### AAL5 Interface Statistics

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

#### AAL5 VCC Statistics

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

Reset Statistics

Figure 3 Statistics of ATM

## Statistics -- ADSL

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

ADSL BER Test

Reset Statistics

Figure 4 Statistics of ADSL

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

#### 4.3.3.1 ADSL BER Test

In the ADSL **Statistics** page, click **ADSL BER Test** to perform a bit error rate (BER) test on the DSL line. The test page is as follows:

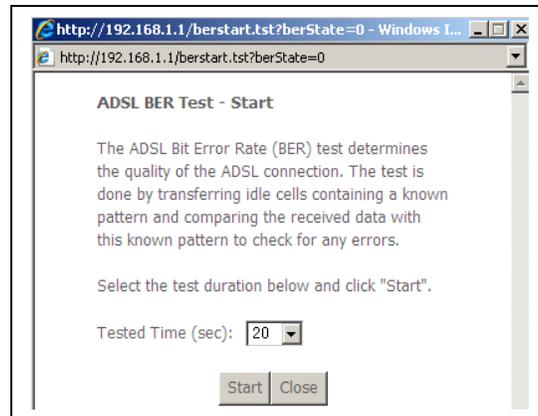


Figure 5 ADSL BER test

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

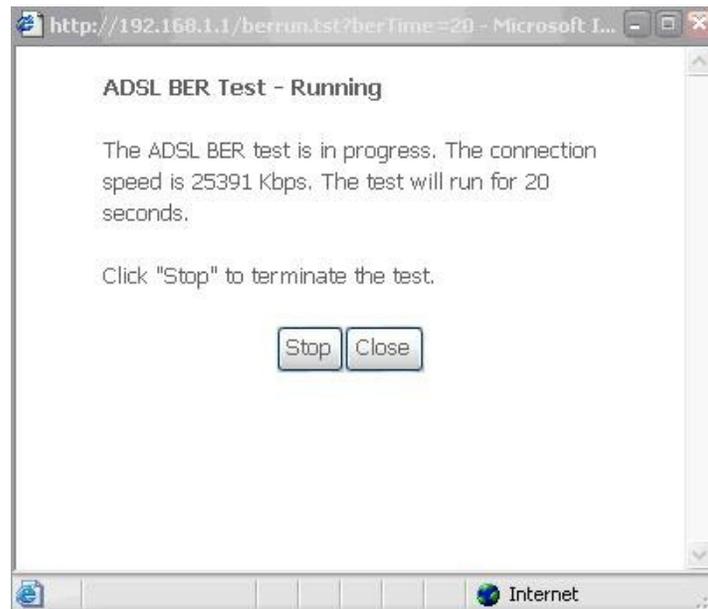


Figure 6 ADSL BER test – running

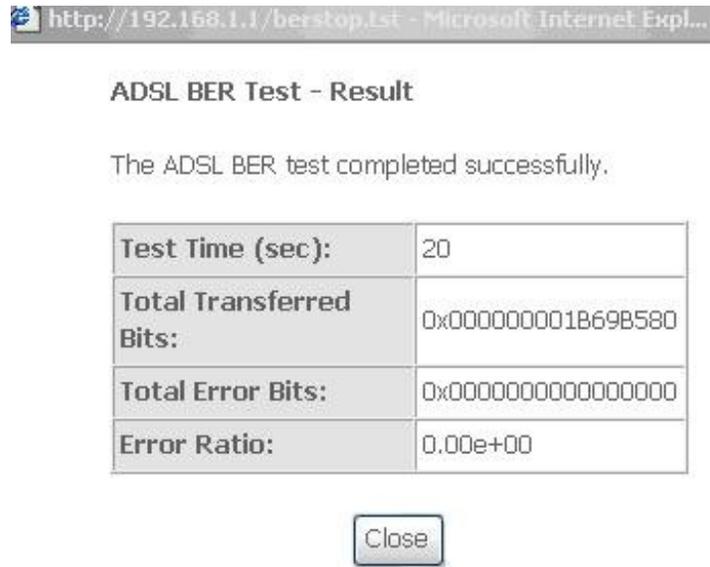


Figure 7 ADSL BER test result

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

**4.3.4 Route Table Information**

Click **Route** and the following page appears. You can view the following information of each route in the route table:

**Device Info -- Route**

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

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

### 4.3.5 ARP Table Information

Click **ARP** and the following page appears. You can query the MAC and IP address information of the equipment attached to the modem and the information includes the following:

#### Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.25	Complete	00:1D:0F:19:91:C1	br0

### 4.3.6 DHCP IP Lease Information

Click **DHCP** and the following page appears. You can query the IP address assignment for MAC address at the LAN side of the DSL router and obtain the IP Address from the DHCP server through Ethernet and wireless in the DSL router.

The information of each lease item includes the following:

**Expires In:** Time that the device leases the IP Address for the MAC Address

#### Device Info -- DHCP Leases

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

## 4.4 Advanced Setup

### 4.4.1 WAN Configuration

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

Device Info

Quick Setup

Advanced Setup

WAN

LAN

HiAT

Security

Quality of Service

Routing

DNS

DSL

Diagnostics

Management

**Wide Area Network (WAN) Setup**

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

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

Add Remove Save/Reboot

- To modify the parameters of existing PVC, click **Edit**.
- To add an ATM PVC, click **Add**.
- To delete PVC, select the **Remove** check box in the table and click **Remove**.
- Click **Save/Reboot** to apply the changes and reboot the router.

*Note: After PVC is deleted or modified, the system must be rebooted. Otherwise, the modification does not take effect.*

Click **Add**. The configure page displayed contains the following information:

**ATM PVC Configuration**

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

VPI: [0-255]

VCI: [32-65535]

VLAN Mux - Enable Multiple Protocols Over a Single PVC

Service Category: UBR Without PCR

**Enable Quality Of Service**

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

Enable Quality Of Service

Back Next

This page is the same as the **Quick Setup** page. The procedure for adding PVC is described as follows.

#### 4.4.1.1 Adding a PPPoE PVC

This section describes the procedure for adding PVC 8/35 (PPPoE mode). In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. In this page, you can modify VPI/VCI, service categories, and QoS.

##### ATM PVC Configuration

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

VPI: [0-255]

VCI: [32-65535]

Service Category:

##### Enable Quality Of Service

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

Enable Quality Of Service

- **VPI:** Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI:** Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category:** UBR without PCR/UBR with PCR/CBR/Non Realtime VBR/Realtime VBR.
- **Enable Quality Of Service:** Enable or disable QoS.

In this example, PVC 8/35 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required. After proper modifications, click **Next** and the following page appears. In this page, you can modify the Internet connection type and encapsulation type.

**Connection Type**

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

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

**Encapsulation Mode**

LLC/SNAP-BRIDGING

Back Next

Change the connection type of PVC 8/35 to **PPP over Ethernet (PPPoE)** and set the **Encapsulation Mode** to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

**Connection Type**

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

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

**Encapsulation Mode**

LLC/SNAP-BRIDGING

Back Next

Click Next and the following page appears.

### 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:

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode

In this page, you can modify the PPP user name, PPP password, authentication method and so on.

- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **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:** A full cone 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.
- **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 router does not detect the flow of the user continuously, the router automatically stops the PPPoE connection. Once it detects the flow (like access to a webpage), the router restarts the PPPoE dialup.

If this function is disabled, the router performs PPPoE dial-up all the time. The PPPoE connection does not stop, unless the router is powered off and DSLAM or uplink equipment is abnormal.

- **PPP IP extension:** If this function is enabled, the WAN IP address obtained by the router through built-in dial-up can be directly assigned to the PC being attached to

the router (at this time, the router connects to only one PC). From the aspect of the PC user, the PC dials up to obtain an IP address. But actually, the dial-up is done by the router.

If this function is disabled, the router itself obtains the WAN IP address.

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

If this function is enabled, the router uses this IP address as the WAN IP address.

- **Retry PPP password on authentication error:** If this function is enabled, DSL will retry PPP password on authentication while authenticating with right password failure.
- **Enable PPP Debug Mode:** The PPP Debug Mode enables connection debugging facilities. If this function is enabled, pppd will log the contents of all control packets sent or received in a readable form. The packets are logged through syslog with facility daemon and level debug.

After entering the PPP user name and password, click Next and the following page appears.

In this page, you can modify the service name, and enable or disable the IGMP multicast and WAN service.

#### Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name

- **IGMP Multicast:** IGMP proxy. For example, if you wish that the PPPoE mode supports IPTV, enable this function.
- **WAN Service:** Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears.

This page shows all the configuration. You can view the default values of network address translation (NAT) enable and Firewall enable.

### WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_8_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.



*Note: You need to reboot the router to activate this WAN interface and further configure services in this interface.*

### 4.4.1.2 Adding a PPPoA PVC

This section describes the procedure for adding PVC 8/35 (PPPoA mode).

Device Info

Quick Setup

Advanced Setup

**WAN**

LAN

IPAT

Security

Quality of Service

Routing

DNS

DSL

Diagnostics

Management

**Wide Area Network (WAN) Setup**

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

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

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

In this page, you can modify VPI/VCI, service categories, and QoS.

**ATM PVC Configuration**

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

VPI: [0-255] VCI: [32-65535] Service Category: **Enable Quality Of Service**

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

Enable Quality Of Service  

**VPI:** Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.

**VCI:** Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).

**Service Category:** UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

**Enable Quality Of Service:** Enable or disable QoS.

In this example, PVC 8/35 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the **Internet Connection Type** and **Encapsulation Type**.

**Connection Type**

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

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

**Encapsulation Mode**

Click **Next** and the following page appears.

#### PPP Username and Password

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

PPP Username:

PPP Password:

Authentication Method:

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode

In this page, you can modify the PPP user name, PPP password, authentication method and so on.

- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:** A full cone 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.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time.
- **PPP IP extension:** If this function is enabled, the WAN IP address obtained by the router through built-in dial-up can be directly assigned to the PC being attached to the router (at this time, the router connects to only one PC).

- **Use Static IP Address:** If this function is disabled, the router obtains an IP address assigned by an uplink equipment such as BAS, through PPPoA dial-up. If this function is enabled, the router uses this IP address as the WAN IP address.
- **Retry PPP password on authentication error:** If this function is enabled, DSL will retry PPP password on authentication while authenticating with right password failure.
- **Enable PPP Debug Mode:** The PPP Debug Mode enables connection debugging facilities. If this function is enabled, pppd will log the contents of all control packets sent or received in a readable form. The packets are logged through syslog with facility daemon and level debug.

After entering the PPP user name and password, click **Next** and the following page appears.

In this page, you can modify the service name, and enable or disable the IGMP multicast and WAN service.

#### Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name

#### IGMP

#### Multicast:

IGMP proxy. For example, if you wish that the PPPoA mode supports

IPTV, enable this function.

**WAN Service:** Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears.

This page shows all the configuration. You can view the default values of NAT enable and Firewall enable.

#### WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_8_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

To save the settings, click **Save**. To make any modifications, click **Back**.

**Note:** You need to reboot the router to activate this WAN interface and further configure services in this interface.

### 4.4.1.3 Adding an MER PVC

This section describes the procedure for adding PVC 8/35 (MER mode).

Device Info

Quick Setup

Advanced Setup

**WAN**

LAN

NAT

Security

Quality of Service

Routing

DNS

DSL

Diagnostics

Management

**Wide Area Network (WAN) Setup**

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

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

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

In this page, you can modify VPI/VCI, service categories and QoS.

#### ATM PVC Configuration

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

VPI: [0-255]

VCI: [32-65535]

Service Category:

#### Enable Quality Of Service

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

Enable Quality Of Service

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

**VCI:** Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

**Enable Quality Of Service:** Enable or disable QoS.

In this example, PVC 8/35 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the Internet **Connection Type** and **Encapsulation Mode**.

#### Connection Type

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

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

#### Encapsulation Mode

LLC/SNAP-BRIDGING ▾

Back Next

Change the connection type of PVC 8/35 to **MAC Encapsulation Routing (MER)** and set the **Encapsulation Mode** to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

#### Connection Type

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

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

#### Encapsulation Mode

LLC/SNAP-BRIDGING ▼

Back Next

Click **Next** and the following page appears.

In this page, you can modify the WAN IP address, default gateway, and DNS server settings.

#### WAN IP Settings

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

Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

- Obtain an IP address automatically
- Use the following IP address:

WAN IP Address:

WAN Subnet Mask:

- Obtain default gateway automatically
- Use the following default gateway:

Use IP Address:

Use WAN Interface: mer\_0\_8\_35/ ▼

- Obtain DNS server addresses automatically
- Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

Back Next

**Obtain an IP address automatically:** The router obtains a WAN IP address automatically and at this time it enables DHCP client functions. The WAN IP address is obtained from the uplink equipment like BAS and the uplink equipment is required to enable the DHCP server functions.

**Use the following IP address:** If you want to manually enter the WAN IP address, select this check box and enter the information in the field.

**WAN IP Address:** Enter the IP address of the WAN interface provided by your ISP.

**WAN Subnet Mask:** Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

**Obtain Default Gateway automatically:** Obtain the IP address of the default gateway assigned by the uplink equipment such as BAS.

**Use the following Default Gateway:** If you want to manually enter the IP address of the default gateway, select this check box and enter the information in the fields.

**Use IP Address:** Enter the gateway of the WAN interface provided by your ISP.

**Use WAN Interface:** As to BAS equipment, it is the IP address of the downlink interface.

**Obtain DNS server address automatically:** To obtain the IP address of the DNS server assigned by the uplink equipment such as BAS.

**Use the following DNS server addresses:** If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.

**Primary DNS server:** Enter the IP address of the primary DNS server.

**Secondary DNS server:** Enter the IP address of the secondary DNS server provided by your ISP.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the service name, and enable or disable the NAT, firewall, IGMP multicast, and WAN service.

#### 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

#### Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

**Enable NAT:** Select it to enable the NAT functions of the router. If you do not want to enable NAT and wish the router user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.

**Enable Fullcone NAT:** A full cone 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.

**Enable Firewall:** Enable or disable IP filtering.

**IGMP Multicast:** IGMP proxy. For example, if you wish that the MER mode supports IPTV, enable this function.

**WAN Service:** Enable it, unless you do not want to active the PVC.

Click Next and the following page appears. This page shows all the configuration.

#### WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	MER
Service Name:	mer_0_8_35
Service Category:	UBR
IP Address:	21.21.21.12
Service State:	Enabled
NAT:	Enabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

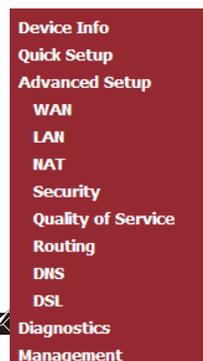
Back Save

To save the settings, click Save. To make any modifications, click Back.

*Note: You need to reboot the router to activate this WAN interface and further configure services in this interface.*

### 4.4.1.4 Adding an IPoA PVC

This section describes the procedure for adding PVC 8/35 (IPoA mode).



#### Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.

Choose Save/Reboot to apply the changes and reboot the system.

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

Add Remove Save/Reboot

Click **Add** and the following page appears.  
In this page, you can modify VPI/VCI, service categories, and QoS.

**ATM PVC Configuration**

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

VPI: [0-255] VCI: [32-65535] Service Category: **Enable Quality Of Service**

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

Enable Quality Of Service  

**VPI:** Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.

**VCI:** Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

**Enable Quality Of Service:** Enable or disable QoS.

In this example, PVC 8/35 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the Internet connection type and encapsulation type.

**Connection Type**

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

 PPP over ATM (PPPoA) PPP over Ethernet (PPPoE) MAC Encapsulation Routing (MER) IP over ATM (IPoA) Bridging**Encapsulation Mode**

Change the connection type of PVC 8/35 to **IP over ATM (IPoA)** and set the **Encapsulation Mode** to **LLC/SNAP-ROUTING** (according to the uplink equipment).

#### Connection Type

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

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

#### Encapsulation Mode

LLC/SNAP-ROUTING ▼

Back Next

Click **Next** and the following page appears.

In this page, you can modify the WAN IP, default gateway, and DNS server settings.

#### WAN IP Settings

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

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.

WAN IP Address:

WAN Subnet Mask:

Use the following default gateway:

Use IP Address:

Use WAN Interface:

Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

Back Next

**WAN IP Address:** Enter the IP address of the WAN interface provided by your ISP.

**WAN Subnet Mask:** Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

**Use the following Default Gateway:** If you want to manually enter the IP address of the default gateway, select this check box and enter the information in the fields.

**Use IP Address:** Enter the gateway of the WAN interface provided by your ISP.

**Use WAN Interface:** As to BAS equipment, it is the IP address of the downlink interface.

**Use the following DNS server addresses:** If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.

**Primary DNS server:** Enter the IP address of the primary DNS server.

**Secondary DNS server:** Enter the IP address of the secondary DNS server provided by your ISP.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the service name, and enable or disable the NAT, firewall, IGMP multicast, and WAN service.

#### 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

#### Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

**Enable NAT:** Select it to enable the NAT functions of the router. If you do not want to enable NAT and wish the router user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.

**Enable Fullcone NAT:** A full cone 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.

**Enable Firewall:** Enable or disable IP filtering.

**IGMP Multicast:** IGMP proxy. For example, if you wish that the IPoA mode supports IPTV, enable this function.

**WAN Service:** Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears. This page shows all the configuration.

#### WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_8_35
Service Category:	UBR
IP Address:	21.21.21.12
Service State:	Enabled
NAT:	Enabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.



To save the settings, click **Save**. To make any modifications, click **Back**.

*Note: You need to reboot to the router to activate this WAN interface and further configure services in this interface.*

#### 4.4.1.5 Adding a Bridge PVC

This section describes the procedure for adding PVC 8/35 (Bridge mode).

Device Info

Quick Setup

Advanced Setup

**WAN**

LAN

NAT

Security

Quality of Service

Routing

DIS

DSL

Diagnostics

Management

#### Wide Area Network (WAN) Setup

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

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

Click **Add** and the following page appears.  
In this page, you can modify VPI/VCI, service categories, and QoS.

#### ATM PVC Configuration

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

VPI: [0-255]

VCI: [32-65535]

Service Category:

#### Enable Quality Of Service

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

Enable Quality Of Service

**VPI (Virtual Path Identifier):** Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.

**VCI (Virtual Channel Identifier):** Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).

**Service Category:** UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

**Enable Quality Of Service:** Enable or disable QoS.

In this example, PVC 8/35 is to be modified and the default values of service category and QoS remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears.

In this page, you can modify the Internet connection type and encapsulation type.

#### Connection Type

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

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

Click **Next** and the following page appears. In this page, you can modify the service name.

Unselect the check box below to disable this WAN service

Enable Bridge Service:

Service Name:

**WAN Service:** Enable it, unless you do not want to active the PVC.  
Click Next and the following page appears. This page shows all the configuration.

#### WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	Bridge
Service Name:	br_0_8_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

To save the settings, click **Save**. To make any modifications, click **Back**.

*Note: You need to reboot the router to activate this WAN interface and further configure services in this interface.*

### **4.4.2 LAN Configuration**

You can use the LAN configuration to define an IP address for the DSL Router and configure the DHCP server.

**Local Area Network (LAN) Setup**

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

IP Address:   
Subnet Mask:

- Enable IGMP Snooping  
 Standard Mode  
 Blocking Mode

- Disable DHCP Server  
 Enable DHCP Server

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

**Reserve IP Address**

Choose "Edit Reserved IP Address List" to configure Reserved IP Address List.

NOTE1: You can max reserve 10 ip address and special mac.

NOTE2: When you added a new reserve ip. You must reboot system to active it.

[Edit Reserved IP Address List](#)

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

[Save](#) [Save/Reboot](#)

#### 4.4.2.1 Defining the Private IP Address for the DSL Router

In this page, you can change the IP address of the device. The preset IP address is 192.168.1.1. This is the private IP address of the DSL Router, under which the device can be reached in the local network. It can be freely assigned from the block of available addresses. The IP address under which the Router can be reached from outside is assigned by the ISP.

- If you want to assign a different IP address to the DSL Router, enter it in the field next to IP address.
- Adjust the subnet mask if necessary.

It is recommended to use an address from a block that is reserved for private use. The address block is 192.168.1.1~192.168.255.254.

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

*Note: New settings can only be made after the DSL Router is rebooted. If necessary, reconfigure the IP address on your PC (including the one that is statically assigned) so that it matches the new configuration.*

#### 4.4.2.2 Enabling IGMP Snooping

Internet Group Management Protocol

IGMP is an Internet protocol that enables an Internet computer to inform neighboring routers that it is a member of a multicast group. With multicasting, a computer can send content on the Internet to several other computers that have registered an interest in the content of the first computer. Multicasting can, for example, be used for multimedia programs for media streaming to recipients that have set up multicast group membership.

<input type="checkbox"/>	Enable IGMP Snooping
<input checked="" type="radio"/>	Standard Mode
<input type="radio"/>	Blocking Mode

*Note: If IGMP snooping function is enabled, the DSL Router capability improves.*

#### 4.4.2.3 Configuring the DHCP Server

The DSL Router has a DHCP server for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the DSL Router.

Disable DHCP Server  
 Enable DHCP Server

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

**Note:**

- If the DHCP server for the DSL Router is activated, you can configure the network setting on the PC so that the option 'Obtain an IP address automatically' is set up.
- If you deactivate the DHCP server, you need to assign a static IP address for the PCs that use the network settings.
- If the DHCP server is active, you can define a lease time. The lease time determines the period for which the PCs retain the IP addresses assigned to them without changing them.
- Define the range of IP addresses that the Router should use to automatically assign IP addresses to the PCs. Define the first issued IP address and the last issued IP address.
- Enable DHCP Server Relay: This function allows you to relay DHCP and BOOTP requests from a subnet with no DHCP server on it to one or more DHCP servers on other subnets.

#### 4.4.2.4 Reserve IP Address

If you want to reserve one specific IP address for a certain PC by MAC address, edit the reserved IP Address List.

##### Reserve IP Address

Choose "Edit Reserved IP Address List" to configure Reserved IP Address List.

NOTE1: You can max reserve 10 ip address and special mac.

NOTE2: When you added a new reserve ip. You must reboot system to active it.

[Edit Reserved IP Address List](#)

#### 4.4.3 NAT

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

Click **Advanced Setup > NAT**, and the following page appears. This part contains Virtual Servers, Port Triggering, and DMZ Host. Choose the item to do relative configurations.

**NAT**

**Virtual Servers** 8

**Port Triggering** 4 (Toll Free)

**DMZ Host**





- **Select a Service:** Select a proper service in the drop-down list.
- **Custom Server:** Enter a new service name to establish a user service type.
- **Server IP Address:** Assign an IP address to virtual server.
- **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.

Step 2. After finishing setting, click Save/Apply to save and apply the settings.

#### 4.4.3.2 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 ports of the firewall.

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

**NAT -- Port Triggering Setup**

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

Add Remove

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

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

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it. **Remaining number of entries that can be configured:32**

Application Name:

Select an application: Select One

Custom application:

Save/Apply

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

Save/Apply

- **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.*

#### 4.4.3.3 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 DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

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

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

DMZ Host IP Address:

Save/Apply

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

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

### 4.4.4 Security

Security is an important function of DSL. It protects resources of a private network from users from other networks, and prevents unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet (that is, the local network to which you are connected) must pass through the security checks, which checks each message and blocks those that do not meet the specific security criteria.

There are two basic types of security techniques:

- **IP packet filtering:** The system checks each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but is difficult to configure.
- **Parental Control:** The system checks each frame entering or leaving the network from layer 2. It accepts and rejects frames according to user-defined rules.

Choose **Security > IP Filtering** and the following page appears. By default, the firewall is enabled. The firewall is used to block document transmissions between the Internet and your PC. It serves as a safety guard and permits only authorized documents to be sent to the LAN.

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

If no PVC of Bridge mode is configured, MAC filtering is disabled and the MAC Filtering interface does not appear.

Device Info  
Quick Setup  
Advanced Setup  
WAN  
LAN  
NAT  
Security  
IP Filtering  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
Diagnostics  
Management

**Outgoing IP Filtering Setup**

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

#### 4.4.4.1 Outgoing IP Filtering Setup

When setup of outgoing IP filtering rules is enabled on the router, various security functions for the local network are enabled at the same time. You can protect the network against hacker attacks and block access of individual PC to selected services or Internet websites.

Choose **Security > IP Filtering > Outgoing** and the following page appears.

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

##### Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
-------------	----------	-----------------------	-------------	----------------------	------------	------------	--------

Click **Add** and the page for defining the IP filtering rule appears.

In this page, you can create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All specified conditions in the filtering rule must be complied with the rule to take effect.

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

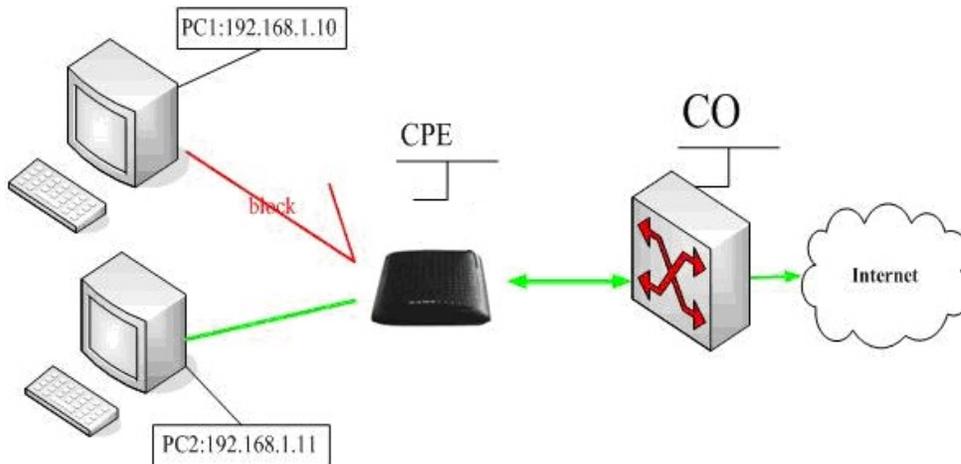
**Add IP Filter -- Outgoing**

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

Filter Name:	<input type="text" value="123"/>
Protocol:	<input type="text"/>
Source IP address:	<input type="text"/>
Source Subnet Mask:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address:	<input type="text"/>
Destination Subnet Mask:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>
DSCP Mark:	<input type="text"/>

- **Filter Name:** Enter the name of outgoing filter rule.
- **Protocol:** Select one from TCP/UDP, TCP, UDP, and ICMP protocols.
- **Source IP address:** Enter an IP address. After you set the IP address, outgoing packets (protocol selected packets) are blocked.
- **Source port:** UPD/TCP source port or a range of ports.
- **Destination IP address:** IP address of the destination (default: null).
- **Destination port:** UPD/TCP destination port or a range of ports.
- **DSCP Mark:** Marking DSCP that outgoing packets.

The following is an example of configuring the outgoing IP filtering.



The topology is as follows:

### Request

- I need to block PC1 whose IP address is 192.168.1.10. All outgoing UDP/TCP packet from that PC1 (192.168.1.10) is not allowed.
- Allow all outgoing traffic packet from PC2 (192.168.1.11).

### Configuration

Step 1 By default, all outgoing IP traffic from LAN is allowed. Hence, all outgoing IP packets from PC2 are allowed. The detailed configuration steps are as follows:

### Add IP Filter -- Outgoing

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

Filter Name:	<input type="text" value="filter1"/>
Protocol:	<input type="text" value="TCP/UDP"/>
Source IP address:	<input type="text" value="192.168.1.10"/>
Source Subnet Mask:	<input type="text" value="255.255.255.0"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address:	<input type="text"/>
Destination Subnet Mask:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>
DSCP Mark:	<input type="text"/>

Step 2 Click **Save/Apply** and the following page appears:

### Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
filter1	TCP/UDP	192.168.1.10 / 255.255.255.0					<input type="checkbox"/>

#### 4.4.4.2 Incoming IP Filtering Setup

The incoming IP filter is used to block and permit IP packet transmission from internet. By default incoming IP filter block all incoming packet from Internet. When incoming IP filtering rules setup being enable on the router, you can permit remote individual PC to access various local network service.

Choose **Security > IP Filtering > Incoming** and the following page appears.

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

##### Incoming IP Filtering Setup

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

Choose Add or Remove to configure incoming IP filters.

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

Click **Add** and the page for defining the IP filtering rule appears.

In this page, you can create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All specified conditions in the filter rule must be complied with the rule to take effect. Click **Save/Apply** to save and activate the filter.

You must select at least one WAN interface to apply this rule.

##### Add IP Filter -- Incoming

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

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

DSCP Mark:

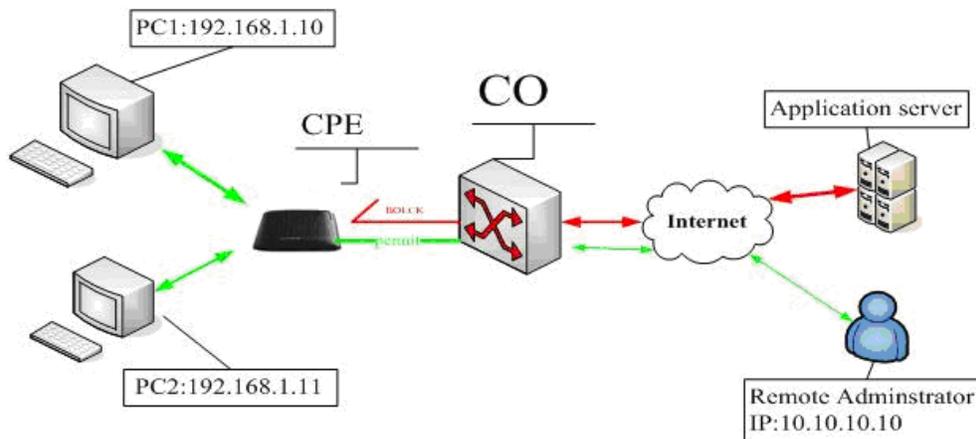
##### WAN Interfaces (Configured in Routing mode and with firewall enabled only)

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

- Select All
- pppoa\_0\_0\_100\_1/ppp\_0\_0\_100\_1

- **Filter Name:** Enter the name of incoming filter rule.
- **Protocol:** Select one from TCP/UDP, TCP, UDP, and ICMP protocols.
- **Source IP address:** Enter an IP address. After you set the IP address, the incoming packets (protocol selected packets) are allowed.
- **Source port:** UDP/TCP source port or a range of ports.
- **Destination IP address:** destination IP (default: null).
- **Destination port:** UDP/TCP destination port or a range of ports.
- **DSCP Mark:** Marking DSCP that outgoing packets.
- **WAN interfaces:** You can select WAN interfaces and PVC.

The following is an example of configuring the incoming IP filtering:



### Request

- I need to permit a PC whose IP address is 10.10.10.10. All Incoming TCP/UDP packet traffic from that PC (10.10.10.10) is allowed.
- Block all IP traffic from other PCs.

## Configuration

**Step 1** By default, all incoming IP traffic from Internet is blocked. Hence, all incoming IP packets from other PCS except PC (10.10.10.10) are blocked.

**Step 2** The detailed configuration steps are as follows:

### Add IP Filter -- Incoming

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

Filter Name:	<input type="text" value="Incoming"/>
Protocol:	<input type="text" value="TCP/UDP"/>
Source IP address:	<input type="text" value="10.10.10.10"/>
Source Subnet Mask:	<input type="text" value="255.255.0.0"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address:	<input type="text"/>
Destination Subnet Mask:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>
DSCP Mark:	<input type="text"/>

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

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

- Select All
- pppoe\_0\_8\_35\_1/ppp\_0\_8\_35\_1

**Step 3** Click Save/Apply and the following page appears:

### Incoming IP Filtering Setup

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

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
Incoming	ALL	TCP/UDP	10.10.10.10 / 255.255.0.0					<input type="checkbox"/>

### 4.4.4.3 Parental Control

If you allow your children to access to the Internet in the specific time, add the schedule with the LAN MAC address of the device. Choose **Security > Parental Control** and the following page appears.

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

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>											

Click **Add** and the following page appears

#### Time of Day Restriction

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

User Name

Browser's MAC Address

Other MAC Address

(xx:xx:xx:xx:xx:xx)

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

In this page, you can add time of day restriction to a specific LAN device connected to the Router. Enter the user name, select days of week and the blocking time, and click **Save/Apply**. The following page appears

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

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
one	00:1d:0f:19:91:c1	x							00:00	23:59	<input type="checkbox"/>

### 4.4.5 Quality of Service

Many communication and multimedia applications require large, high speed bandwidths to transfer data between the local network and the Internet. However, for many applications there is often only one Internet connection available with limited capacity. QoS divides this capacity between the different applications and provides undelayed and continuous data transfer where data packets with higher priority are given preference. Click **Quality of Service** and the following page appears. Under **Quality of Service**, there are two network share modes: **Queue Config** and **QoS Classification**.

#### 4.4.5.1 Enabling QoS

In this page, you can configure QoS queue management. By default, the system enables QoS and sets a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.

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 'Save/Apply' 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:

Select **Enable QoS** to enable QoS and set the default DSCP mark. Click **Save/Apply** to active QoS.

#### 4.4.5.2 QoS - Queue Configuration

The queuing in packet QoS becomes effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging, not under control of the packet QoS.

Click **Queue Config** and the following page appears. In this page, you can configure QoS Queue. A maximum of 24 entries can be configured.

QoS Queue Configuration can allocate three queues. Each of the queues can be configured for a precedence value. The queue entry configured is used by the classifier to place ingress packets appropriately.

QoS Queue Configuration -- A maximum 16 entries can be configured.

Interfacename	Description	Precedence	Queue Key	Enable	Remove
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> <span>Add</span> <span>Remove</span> <span>Save/Reboot</span> </div>					

*Note: Lower integer values for precedence indicate higher priority for this queue relative to others.*

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

##### QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Save/Apply' to save and activate the filter.

Queue Configuration Status:

Queue:

Queue Precedence:

Save/Apply

**Queue Configuration Status:** Set to enable or disable a QoS queue.

**Queue:** Select a specific network interface. The router automatically allocates selected network interface to the queue.

**Queue Precedence:** Select an integer value for queue precedence. After you select an integer value, the queue entry appropriately places to ingress packets. Lower integer values for precedence imply higher priority for this queue relative to others.

### 4.4.5.3 QoS - QoS Classification

Some applications require specific bandwidth to ensure their data be forwarded in time. QoS classification can create 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. After QoS classification, QoS divides capacity between different applications and provides undelayed and continuous data transfer where data packet with higher priority is given preference.

Click **QoS Classification** and the following page appears. In this page, you can configure network traffic classes.

#### Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

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

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

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

#### 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 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

#### Assign ATM Priority and/or DSCP Mark for the class

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

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

#### Specify Traffic Classification Rules

Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

##### SET-1

Protocol:

Differentiated Services Code Point (DSCP) Check:

IP Address

Source Subnet Mask:

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

Destination IP Address:

Destination Subnet Mask:

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

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

##### SET-2

802.1p Priority:

☎ 1800-209-3444 (Toll Free)

✉ helpdesk@digisol.com

🕒 sales@digisol.com

🌐 www.digisol.com

- **Traffic Class Name:** Enter a name of the class.
- **Rule Order:** Select order for queue.
- **Rule Status:** Enable or disable this traffic class rule.
- **Assign Classification Queue:** Select a classification queue.
- **Assign Differentiated Service Code Point (DSCP) Mark:** Select a mark service that modifies the original packet IP header if all rules defined within the classification class are matched. (CS - Mark IP Precedence, AF - Assured Forwarding, EF - Expedited Forwarding)
- **Mark 802.1p if 802.1q is enabled:** Select an 802.1p priority number that serves as the 802.1p value.

There are two sets of classification rules. Set-1 is based on different fields within TCP/UDP/IP layer plus physical LAN port; Set-2 is based on MAC layer IEEE 802.1p priority field.

802.1p priority: The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one.

## 4.4.6 Routing

### 4.4.6.1 Routing – Default Gateway

In this page, you can modify the Default Gateway settings.

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

*Note: After changing the **Automatic Assigned Default Gateway** from unselected to selected, you must reboot the router to obtain the automatic assigned default gateway.*

If you want to use a default gateway, select the **Enable Automatic Assigned Default Gateway** check box to show the following page:

#### Routing -- Default Gateway

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

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

Enable Automatic Assigned Default Gateway

Save/Apply

Use Default Gateway: Select the **Enable automatic Assigned Default Gateway** box.  
Custom DSL router Default Gateway

- Enable Automatic Assigned Default Gateway
- Use Default Gateway IP Address
- Use Interface: interface that the packets pass through on the router

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

#### 4.4.6.2 Static Routes

Networking devices forward packets using route information that is either manually configured or dynamically learned using a routing protocol. Static routes are manually configured and define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Static routes can be redistributed into dynamic routing protocols but routes generated by dynamic routing protocols cannot be redistributed into the static routing table. No algorithm exists to prevent the configuration of routing loops that use static routes.

Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases.

##### Routing -- Static Route Add

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

Destination Network Address:	<input type="text" value="10.11.102.4"/>
Subnet Mask:	<input type="text" value="255.255.0.0"/>
<input checked="" type="checkbox"/> Use Gateway IP Address	<input type="text" value="192.168.1.2"/>
<input checked="" type="checkbox"/> Use Interface	<input type="text" value="pppoe_0_8_35_1/ppp_0_8_35_1"/>
<input type="button" value="Save/Apply"/>	

#### Adding Static Route

- Step 1** Enter destination network address.
- Step 2** Enter subnet Mask.
- Step 3** Enable **Use Gateway IP Address** and enter IP address.
- Step 4** Select use interface.
- Step 5** Click **Save/Apply** to apply the settings.

#### Remove static route

Select Remove box in the table, and click **Remove** to apply the settings.

### 4.4.7 DNS

*Note: If the connection is Bridge PVC, you can not view the DNS item.*

Click **Advanced Setup > DNS**, and the following page appears. Choose the item to do relative configurations.



#### 4.4.7.1 DNS Server

In this interface, you can modify the DNS server settings.

##### DNS Server Configuration

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

Enable Automatic Assigned DNS

Save

If the **Enable Automatic Assigned DNS** check box is selected, this router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. The interface is below.

### DNS Server Configuration

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

Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

Save

Click **Save** to save the new configuration.

---

#### Caution:

**You must reboot the router to make the new configuration effective.**

---

## 4.4.7.2 Dynamic Domain Name Service (DDNS)

### Overview

Dynamic DNS allows binding of domain names to hosts with dynamically assigned IP addresses by a Dynamic Host Control Protocol (DHCP) server and updates the name server with the new information about the host or the network. This is particularly useful for broadband users to use Internet services, such as FTP, Hyper Text Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP), on their local hosts connected to the broadband network. Dynamic DNS allows access to such hosts connected to the broadband networks using a domain name to exchange files, send and receive email with highly personalized email addresses, and host a website.

To provide such support for the feature described above, a client is installed in the host that directs Internet traffic to the domain. The client updates the IP address of the host, whenever the host renegotiates the IP address for any reason. The Router reference software allows users to configure the following dynamic DNS servers for DDNS service:

- DynDNS.org: A free DNS service for hosts with dynamic IP addresses.
- TZO: A service provider providing paid dynamic and static DNS services.

To use one of the providers mentioned above requires the users to register with the dynamic DNS service provider the information about the host and the installed client software on the host which can update the service provider with the IP address and the domain name information.

### Configuration

You can configure in the menu to support the DDNS feature in Linux reference software. After the software support is built for a profile, you can choose **Advanced Setup > DNS > Dynamic DNS** and configure the feature in the following page:

#### Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>				

Click **Add** to configure the information of a new host.

#### Add dynamic DDNS

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

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text"/>
Interface	<input type="text" value="pppoe_0_0_35_1/ppp_0_0_35_1"/>
<b>DynDNS Settings</b>	
Username	<input type="text"/>
Password	<input type="text"/>

- **D-DNS provider:** Website of the dynamic DNS provider.
- **Hostname:** It is the domain name and it can be modified.
- **Interface:** The interface that the packets pass through on the modem.
- **Username:** This is the User name needed to access the DDNS management interface.
- **Password:** This is the Password you will be prompted to enter when you access the DDNS management interface.

Select the service provider for the DDNS service, provide the hostname and the interface to use when sending the DDNS updates, and enter the service provider specific registration information. Then, click **Save/Apply** to use the feature.

### 4.4.8 DSL

In this interface, you can view the DSL settings. Normally, you can keep the factory default settings. The router support these modulations: G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM. The router negotiates the modulation mode with the DSLAM.

#### DSL Settings

Select the modulation below.

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

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Save/Apply

Advanced Settings

Click **Advanced Settings**, and the following page appears.

#### DSL Advanced Settings

Select the test mode below.

- Normal
- Reverb
- Medley
- No retrain
- L3

Apply

Tone Selection

## 4.5 Diagnostics

Click Diagnostics, and the following page appears.

Device Info

Quick Setup

Advanced Setup

**Diagnostics**

Management

pppoe\_0\_0\_35\_1 Diagnostics

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

**Test the connection to your local network**

Test your ENET Connection:	PASS	<a href="#">Help</a>
Test your USB Connection:	DOWN	<a href="#">Help</a>

**Test the connection to your DSL service provider**

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

**Test the connection to your Internet service provider**

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

Rerun Diagnostic Tests
Test With OAM F4

Your router is capable of testing your DSL connection. The individual tests are listed above. 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.

## 4.6 Management

### 4.6.1 Setting

#### Settings - Backup

Select the “Backup” to show the following interface. In the interface, you can backup the DSL router configurations.

#### Settings - Update

Select the “Update” to show the following interface. Click the “Browsing...” button to select the correct update configure settings file. Then click the “Update Settings” to update the router settings.

#### Settings - Restore Default

Click **Management > Settings > Restore Default** to restore DSL router to the factory default configuration.

## 4.6.2 System Log

Click **Management > System Log**, and the following page appears. The system log dialog allows you to view the system log and configure the system log options.

### System Log

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

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

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



Click "Configure System Log" to show the following interface. You can enable or disable the system log and then select the log level, display level and mode, and click "Apply" to end your configurations.

### System Log -- Configuration

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

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

Log:  Disable  Enable

Log Level:

Display Level:

Mode:

Both the log level and display level have eight choices. The default log level is "Debugging" and the default display level is "Error". The mode options are "Local", "Remote", and "Both". The default option is "Local". If you select "Remote" or "Both", all events are transmitted to the specified UDP port of the specified log server.

### System Log -- Configuration

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

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

Log:  Disable  Enable

Log Level:

Display Level:

Mode:

Server IP Address:

Server UDP Port:

After operations under “System Log”, click “View System Log” to query the system logs.

*Note: The log and display of the system events are above the set level. If you intend to record all information, you need to set the levels as “Debugging”.*

**System Log**

Date/Time	Facility	Severity	Message
-----------	----------	----------	---------

Click “Refresh” to refresh the system event logs or “Close” to exit from this interface.

### 4.6.3 SNMP Agent

#### 4.6.3.1 SNMP Protocol

The SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

#### 4.6.3.2 Configuration

Choose **Management > SNMP Agent** and the page shown as follows appears.

**SNMP - Configuration**

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

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

SNMP Agent  Disable  Enable

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

Click **Enable** to open SNMP function, enter the information that your ISP has provided to you, and click **Save/Apply**.

#### 4.6.4 Internet Time

Click **Management > Internet Time**, and the following page appears. In this page, the router can synchronize with Internet time servers.

##### Time settings

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

**Automatically synchronize with Internet time servers**

Save/Apply

After enable **Automatically synchronize with Internet time servers**, the interface show below. Enter proper configurations and click Save/Apply.

##### Time settings

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

**Automatically synchronize with Internet time servers**

First NTP time server:

Second NTP time server:

Time zone offset:

Save/Apply

## 4.6.5 Access Control

### Access Control – Services

Select “**Access Control**”-->”**Services**” to show the following interface. In the interface, you can enable/disable the FTP, HTTP, ICMP, SNMP, TELNET and TFTP services. And the LAN side and WAN side show different configurations.

#### Access Control -- Services

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

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

Save/Apply

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

### Access Control – IP Addresses

Choose **Access Control > IP Addresses** and the following page appears.

#### Access Control -- IP Address

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

Access Control Mode:  Disable  Enable

IP Address Remove

Add Remove

In this page, you can add or remove the IP address in the IP access control list. If the **Access Control Mode** is enabled, it indicates that the router permits the access to local management services from the IP addresses contained in the access control list. If the **Access Control Mode** is disabled, the system does not validate IP addresses for the incoming packets.

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

#### Access Control

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

IP Address:

Save/Apply

In this page, enter the IP address of the management station permitted to access the local management services, and then click **Save/Apply**.

#### Access Control – Passwords

Click “Access Control”-->”Passwords” to show the following interface. In the interface, you can modify the accounts passwords.

#### Access Control -- Passwords

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

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

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

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

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

Username:

Old Password:

New Password:

Confirm Password:

Save/Apply

### 4.6.6 Update Software

Click “Update Software” to show the following interface. In this interface, you can update the router software. Click the “Browse...” button to find the right version file and press “Update Software” to do the update.

#### Tools -- Update Software

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

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

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

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

Software File Name:

*Note: Do not turn off your router during firmware updates. When the update is finished, the router reboots automatically. Do not turn off your router before the reboot is over. You must guarantee the update software is right and accurate. It is strictly forbidden to use other software for updates.*

After update software, it is suggested to restore the router to the factory defaults and configure it again.

### 4.6.7 Save/Reboot

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

Click the button below to save and reboot the router.

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

## 5. 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 Link indicator is off?**

**A:** Check the connection between the “Line” port of router and the wall jack.

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

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

(5) **Q: Why does the web configuration page of the router fail to be accessed?**

**A:** Choose **Start > Run** from the desktop, and ping **192.168.1.1** (IP address of the router). If the router cannot be reached, check the type of the network cable, the connection between the 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, keep the device powered on; push a needle into the hole for about 3 seconds, and then release. The default IP address and subnet mask of the router are **192.168.1.1** and **255.255.255.0** respectively.

- User/password of super user: **admin/admin**.
- User/password of common user: **user/user**

This product comes with lifetime warranty. For further details about warranty policy and Product Registration, please visit support section of [www.digisol.com](http://www.digisol.com)