PLANET
Networking & Communication

User's Manual

G.SHDSL Bridge/Router

► **GRT-101 / GRT-401 / GRT-402**

www.PLANET.com.tw

Copyright

Federal Communication Commission Interference Statement

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

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance, for example, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

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 manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste; they should be collected separately.

Revision

User's Manual for PLANET G.SHDSL Bridge/Router

Model: GRT-101/GRT-401/GRT-402

Rev: 5.0 (July 2013)

Part No. EM-GRTV5

Table of Contents

Chapter 1 . Overview

Next-Generation G.SHDSL Bridge / Router

Based on digital subscriber line (DSL) technology, PLANET's new DSL product, the GRT series, provides an affordable, flexible, and efficient Internet access solution for SOHO (small office / home office) customers, while reducing deployment and operation costs from service providers. Using existing telephone lines, the GRT series concentrates on all traffic onto a single high-speed trunk for Internet activities or shares a corporate intranet. Through the simple-yet-powerful management user interface of the GRT series, network administrators can complete a managed network deployment simply in seconds.

High-speed Symmetric Data Transmission

With bandwidth of up to 5.7Mbps, the GRT-101 / 401 outperforms both T1's at 1.544 Mbps and E1's at 2.048 Mbps. The GRT-402's bandwidth reaches up to 11.4Mbps. By using a standard RJ-45 or phone wire as a connection medium, the installation and equipment costs of the GRT series are dramatically less than that of T1, E1, and Frame Relay. Using integrated bridging and routing support, two GRT series can be connected as a LAN-to-LAN network connection at the distance up to 7.7km (4.8 miles) via regular phone wire.

Built-in PPPoE Feature

The GRT series built-in PPPoE feature enables both the users and the service providers to make use of the existing PPP/PAP/CHAP based authentication and accounting infrastructure. The built-in PPPoE feature saves time by eliminating the need to install software.

High-speed Internet Access

G.SHDSL is the best solution to quickly provide cost-effective, high-speed network service for enterprises and SME users or SOHO users who need high-speed symmetrical Internet connections. By utilizing the existing telephony infrastructure, network installation is simple and straightforward. With up to 5.7 Mbps full duplex speed IP telephony, website hosting and various broadband services can be easily provisioned.

1.1 Product Features

➢ ■ **Internet Access Features**

- Efficient IP routing and transparent learning bridge to support broadband Internet services
- NAT/PAT feature lets user both conserve valuable IP address space and reduce IP address management, meanwhile, also protects certain attack from outer network or internal workstations.
- Full ATM protocol stack implementation over SHDSL / SHDSL.bis
- PPPoA and PPPoE support user authentication with PAP/CHAP/MS-CHAP
- DMZ host/Multi-DMZ/Multi-NAT enables multiple workstations on the LAN to access the Internet for the cost of IP address

➢ **Advanced Internet Functions**

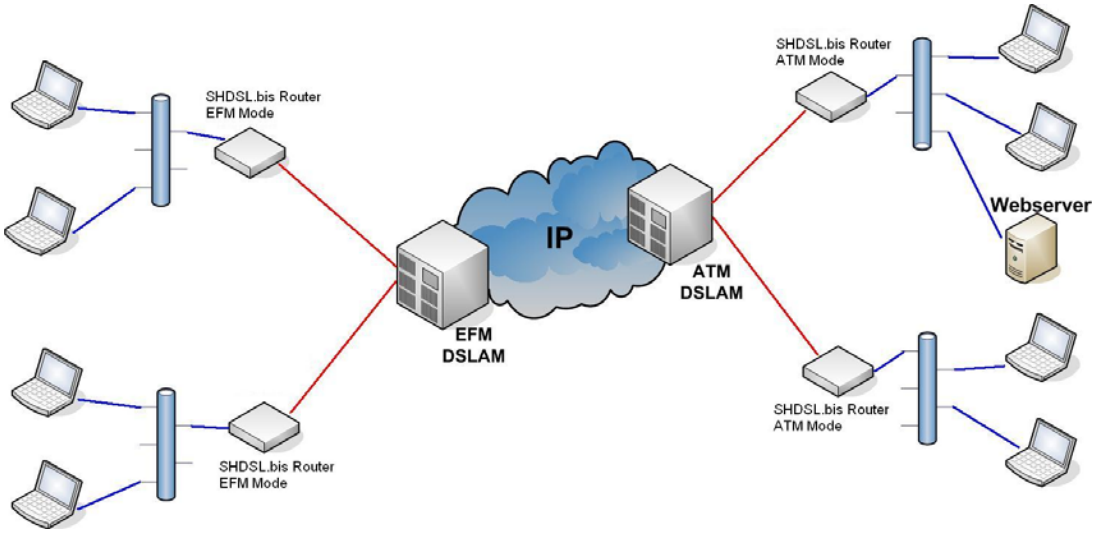
- Easy configuration and management with password control for various application environments
- SNMP management with SNMPv1/SNMPv2 agent and MIB II
- Console and remote (Telnet or HTTP) administration allow user or service providers to locally or remotely diagnose network problems in details
- Symmetrical data rate from 192kbps to 5.7Mbps (GRT-101/GRT-401)
- Symmetrical data rate from 384kbps to 11.4Mbps (GRT-402)
- Virtual LANs (VLANs) offer significant benefit in terms of efficient use of bandwidth, flexibility, performance and security
- VPN pass-through for safeguarded connections

1.2 Product Specifications

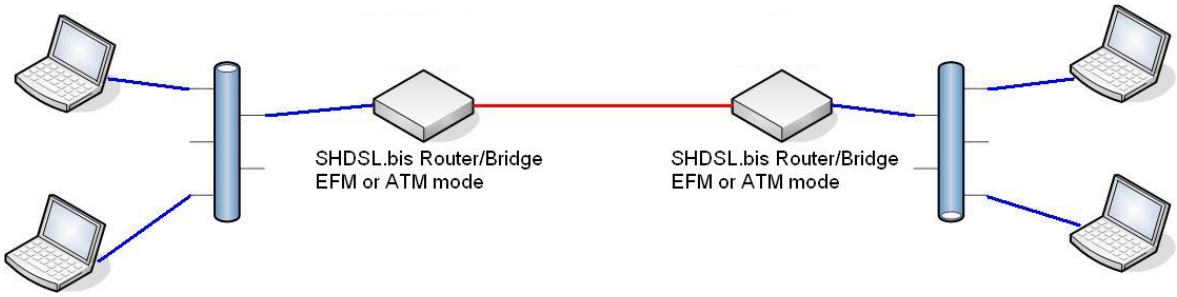
Model	GRT-101	GRT-401	GRT-402
WAN			
Interface	1 x RJ-45		
SHDSL	ITU-T G.991.2 (Annex AF, Annex BG, Annex ABFG) ITU–T G.991.2 rev2 (.bis) ITU-T G.994.1 (G.hs)		
Encoding Scheme	TCPAM-16,TCPAM-32		
EFM Bonding	IEEE 802.3ah PAF		
Data Rate	N x 64Kbps (N=3~89)	N x 64Kbps (N=3~89)	N x 128Kbps (N=3~89)
Impedance	135ohms		
LAN			
Interface	1 x RJ-45	4 x RJ-45	4 x RJ-45
Ethernet	10Base-T, 100Base-TX		
Data Rate	10/100Mbps, Full/Half-Duplex		
Console port			
Interface	RS-232		
LED Indicator			
General	PWR, ALM		
WAN	LNK, ACT		
LAN	1 x LNK/ACT	4 x LNK/ACT	4 x LNK/ACT
Routing			
IP Routing			
Static Routing and RIPv1/RIPv2			
IP masquerading NAT			
DHCP server			
DNS relay and caching			
Natural NAT firewall			
IP precedence (RFC 791)			
Bridging			
IEEE 802.1D transparent learning bridge			
Configuration			
Local console (RS-232) , Telnet, Web (HTTP), Password control			
Network management			
SNMPv1 / SNMPv2 agent MIB II			
ATM			
Up to 8 PVCs UBR/CBR traffic shaping AAL5 OAM F5 loopback ATM Forum UNI 4.0			
AAL5 Encapsulation			
VC multiplexing and SNAP/LLC Ethernet over ATM (RFC 2684/1483) PPP over ATM (RFC 2364) Classical IP over ATM (RFC 1577)			
PPP			

PPP over Ethernet (RFC 2516) **PPP over ATM (RFC 2364)** **User authentication with PAP/CHAP/MS-CHAP**			
Physical/Electrical			
Dimensions (WxDxH)	187 x 145 x 33 mm		
Power	12V DC, 1.0A		
Power consumption	7 watts / 23.8 BTU	8 watts / 27.2 BTU	9 watts / 30.6 BTU
Operating Temp.	0 ~ 45 degrees C		
Storage Temp.	-20 ~ 70 degrees C		
Operating Humidity	0 ~ 95 degrees C (non-condensing)		
Storage Humidity	0 ~ 95 degrees C (non-condensing)		
EMC/EMI			
FCC, CE			

1.3 Applications



Combination with EFM or ATM DSLAM



Point-to-point Connection

Chapter 2 . Installation

2.1 Front Panel LEDs

The LEDs on the front panel indicate the operational status of GRT series.

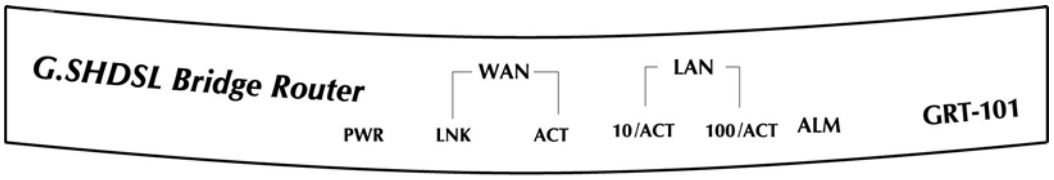


Figure 2-1 GRT-101 Front Panel

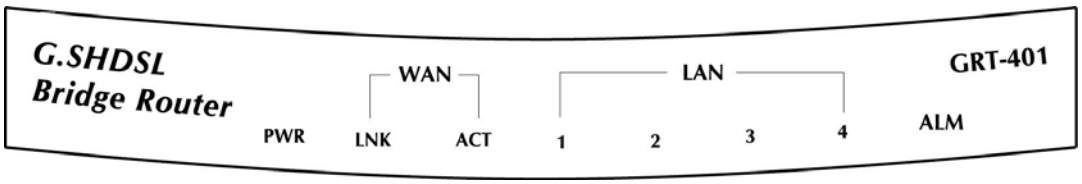


Figure 2-2 GRT-401 Front Panel

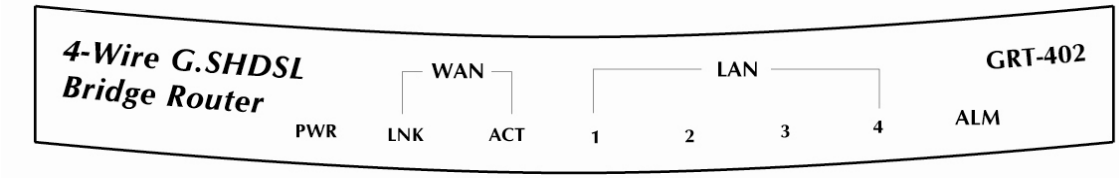


Figure 2-3 GRT-402 Front Panel

The following table describes the LEDs' functions:

Table 2-1 GRT-101 LED Functions

LEDs		Active	Color	Description
PWR		On	Green	Power adaptor is connected to GRT-101
WAN	LNK	On	Green	SHDSL line connection is established
		Blink		SHDSL handshake
	ACT	On	Green	Transmit or receive data over SHDSL link
LAN	10/ACT	On	Green	LAN Speed operates in 10M
	100/ACT	On	Green	LAN Speed operates in 100M
ALM		On	Red	SHDSL connection disconnected
		Blink		SHDSL self test

Table 2-2 GRT-401/GRT-402 LED Functions

LEDs		Active	Color	Description
PWR		On	Green	Power adaptor is connected to GRT-401/GRT-402
WAN	LNK	On	Green	SHDSL line connection is established
		Blink		SHDSL handshake
	ACT	On	Green	Transmit or receive data over SHDSL link
LAN	1	On	Green	Transmit or receive data over LAN 1
	2	On	Green	Transmit or receive data over LAN 2
	3	On	Green	Transmit or receive data over LAN 3
	4	On	Green	Transmit or receive data over LAN 4
ALM		On	Red	SHDSL connection disconnected
		Blink		SHDSL self test

2.2 Rear Panel Ports

The connectors on the rear panel provide Power, LAN, CONSOLE and LINE interfaces.

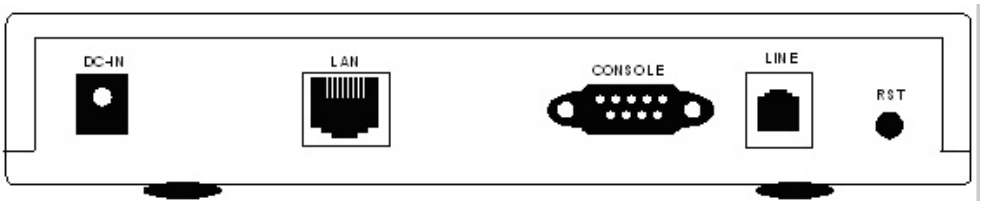


Figure 2-4 GRT-101 Rear Panel

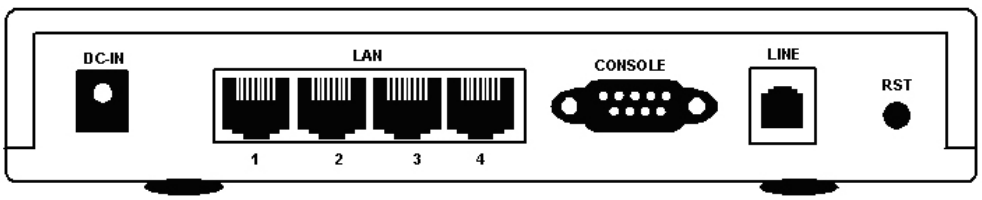


Figure 2-5 GRT-401/GRT-402 Rear Panel

The following table describes the connectors' functions:

Table 2-3 Connector Functions

Connectors	Description
DC-IN	Power adaptor inlet: Input voltage 12VDC
LAN	Ethernet interface for LAN port (RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	SHDSL interface for WAN port (RJ-45)
RST	Reset button for factory default

2.3 Rear Panel Connections

The figure shows the rear panel connections of GRT series**.**

The STU-R is a standalone and is able to place on desktop. All the external wiring is located at the rear panel. The LAN port is a 10 Base-T / 100Base-TX auto-sensing and half/full duplex Ethernet interface and complied with IEEE 802.3 / 802.3u respectively. The console (RS-232C) interface for configuration is menu-driven operation and can also be configured through Ethernet interface by Telnet or Web-based operation.

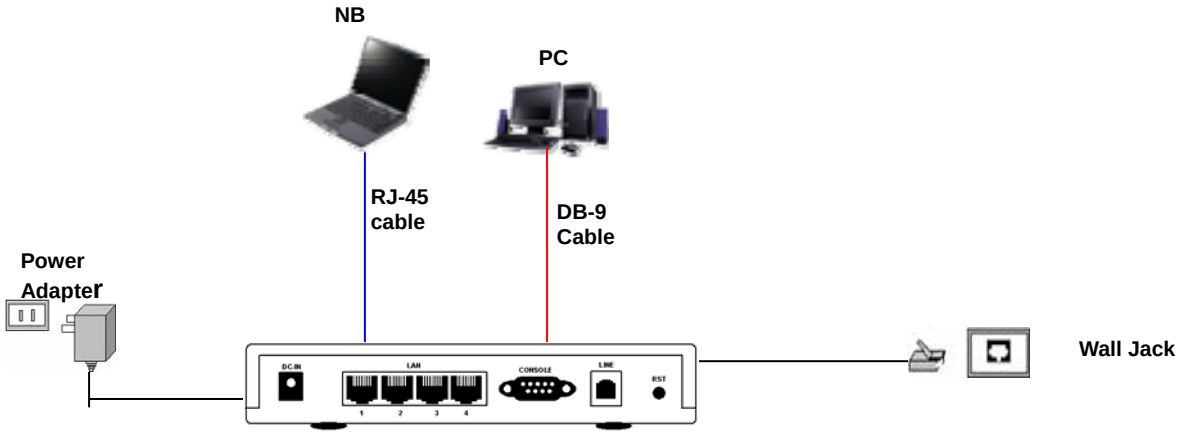


Figure 2-6 Direct Connection with PC or NB

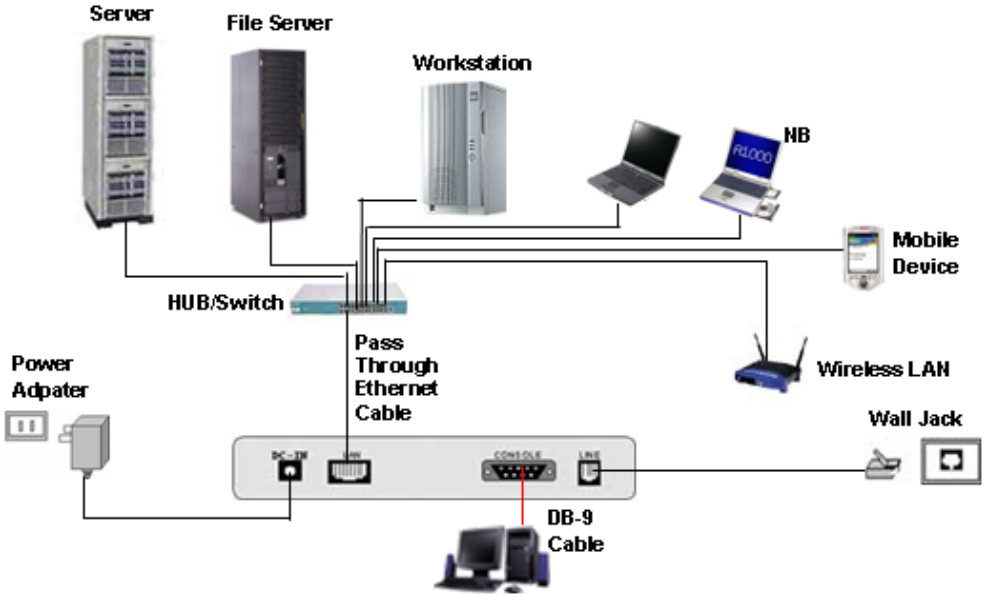


Figure 2-7 Connection with Switch or HUB

Note	The GRT-401 and GRT-402 support auto-MDI (media dependence interface) that auto-detects MDI or MDI-cross with link partner. A standard straight wire UTP cable (EIA568) can be deployed to connect to a PC or Ethernet devices like hubs/switches. The GRT-101 supports MDI interface only.

2.4 Setting up the hardware environment

Step 1: Connect the power adapter to the port labeled DC-IN on the rear panel of the product.

Step 2: Connect the Ethernet cable.

If the GRT-101 is directly connected to PC, the Ethernet crossover cable has to be used (refer to figure 2-6). If the product is connected to a hub or switch, be sure that the hub or switch supports auto-MDI/MDI-X or not. If yes, both crossover and non-crossover Ethernet cables are suitable. If not, only non-crossover Ethernet cable could be used (refer to figure 2-7). Since the GRT-401 and GRT-402 LAN ports support auto-MDI/MDI-X, both crossover and non-crossover Ethernet cables are suitable.

Step 3: Connect the phone cable to the product. Connect the other side of the phone cable to the wall jack.

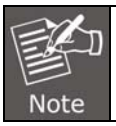
Step 4: Connect the male end of the RS-232 cable to the product and female end to any free COM port in PC.

Step 5: Connect the power adapter by plugging power supply.

Chapter 3 Configuration

3.1 Purpose

This chapter provides information about configuring GRT series.

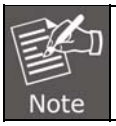


After you have completed all the necessary settings for GRT series, make sure to write the new configuration to NVRAM by "**write**" command and reboot the system, or all of your changes will not take effect.

3.2 Logon Procedure

There are three methods to logon to GRT series: serial console, Telnet, and web interface. For the first-time configuration, perhaps only the serial console mode could be used because applications requiring Internet protocol (IP) communication, such as Telnet and web interface, are not available unless a management IP is configured properly for your local networking environment.

After connecting all the necessary cables described in 1.3 , power on GRT series and select one of the following procedures to access GRT series.



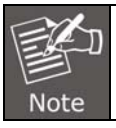
It is recommended that only one configuration application is used to set up GRT series at any given time, that is, Telnet, serial console and the web management interfaces should not be used simultaneously.

3.2.1 Serial console

Check the connectivity of the RS-232 cable from your computer to the serial port of GRT series. Start your terminal access program with VT100 terminal emulation. Configure the serial link with baud rate of 9600, 8 data bits, no parity check, 1 stop bit, and no flow-control, and press the SPACE key until the login screen appears. When you see the login screen, you can logon to GRT series.

User: **admin**

Password: *****



If you have not set any user profile for GRT series, enter the factory default user "**admin**". When the system prompts you for a password, type "**admin**" to enter GRT series.

After you logon to GRT series and before proceeding any further, check the software version of GRT series by the command:

```
                                    PLANET GRT-402
-------------------------------------------------------------
   enable                 Modify command privilege
   status                 Show running system status
>> show                   View system configuration
   ping                   Packet internet groper command
   exit                   Quit system
```

Enter show item to show information of GRT-402.

```
                                    PLANET GRT-402
-------------------------------------------------------------
>> system                 Show general information
   config                 Show all configuration
   script                 Show all configuration in command script
```

```
                                    PLANET GRT-402
-------------------------------------------
Status Window...

General system information
 Model                :GRT-402
 MCSV                 :14A0-FFFF-524FFFFF
 Software Version     :14A0-0002-5241FE95
 Chipset              :CX98102-11Z
 Firmware Version     :G127
 Hostname             :SOHO
 Serial No            :BKLVD3AT0000
 System Up Time       :0DAY/0HR/9MIN

Press 'Enter' to Return Menu Window...
```

There are three utility tools, upgrade, backup and restore, which embedded in the firmware. You can update the new firmware via TFTP upgrade tools and backup the configuration via TFTP backup tool and restore the configuration via TFTP restore tool. For operation on firmware upgrade and backup or restore the system configuration, you must have your own TFTP server software.

Move the cursor " **>>** " to **utility** and press enter.

```
                                        PLANET GRT-402
-------------------------------------------------------------
>> upgrade                  Upgrade main software
   backup                   Backup system configuration
   restore                  Restore system configuration
```

Command: utility upgrade <ip> <file>
Message: Please input the following information.

```
Command: utility upgrade <ip> <file>
Message: Please input the following information.

TFTP server IP address (ENTER for default) <192.168.0.2>: 192.168.0.46
Upgrade filename (ENTER for default) <default.bin>: FW-GRT-402_v524.bin
```

Pressing enter key will perform firmware upgrade.

```
                                        PLANET GRT-402
-------------------------------------------------------------
Utility Running Window...

TFTP server IP address: 192.168.0.46
Upgrade filename: FW-GRT-402_v524.bin

  Connecting...
  Download
  Byte Transfered :       909018 bytes
  Complete

Transfer Complete, Replace Now? (y/n): _
```

3.2.2 Telnet

Make sure the correct Ethernet cable is used for connecting the LAN port of your computer to GRT series. The LAN LNK indicator on the front panel will light up if a correct cable is used. To start your Telnet client with VT100 terminal emulation and connect to the management IP of GRT series, wait for the login screen to appear. When you see the login screen, you can logon to GRT series.

User: **admin**

Password: *****

Note	The factory default management IP and subnet mask are 192.168.0.1 and 255.255.255.0, respectively. If you have not set any user profile for GRT series, enter the factory default user "**admin**". When the system prompts you for a password, type "**admin**" to enter GRT series.

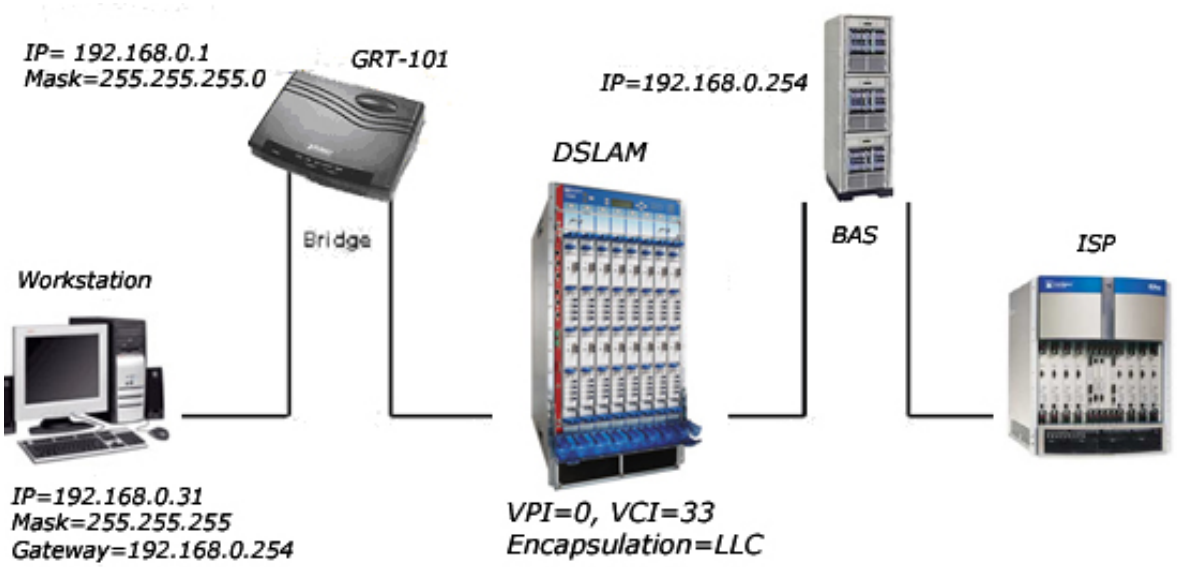
3.2.3 Web browser

Make sure the correct Ethernet cable is used for connecting the LAN port of your computer to GRT series. The LAN LNK indicator on the front panel will light up if a correct cable is used. To start your web browser and connect to the management IP of GRT series, wait for the login screen to appear. When you see the login screen, you can logon to GRT series.

Note	The factory default management IP and subnet mask are 192.168.0.1 and 255.255.255.0, respectively. If you have not changed password setting for web interface, enter the factory default user "**root**". When GRT prompts you for a password, type "**root**".

3.3 Web Operation and Quick Installation Guide

3.3.1 Bridge Mode

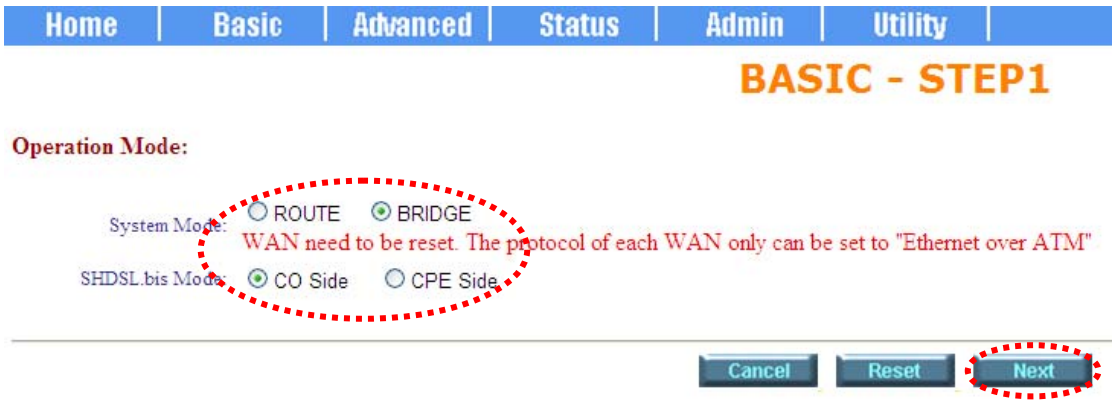


3.3.2 Web UI Configuration

After connection via web browser,

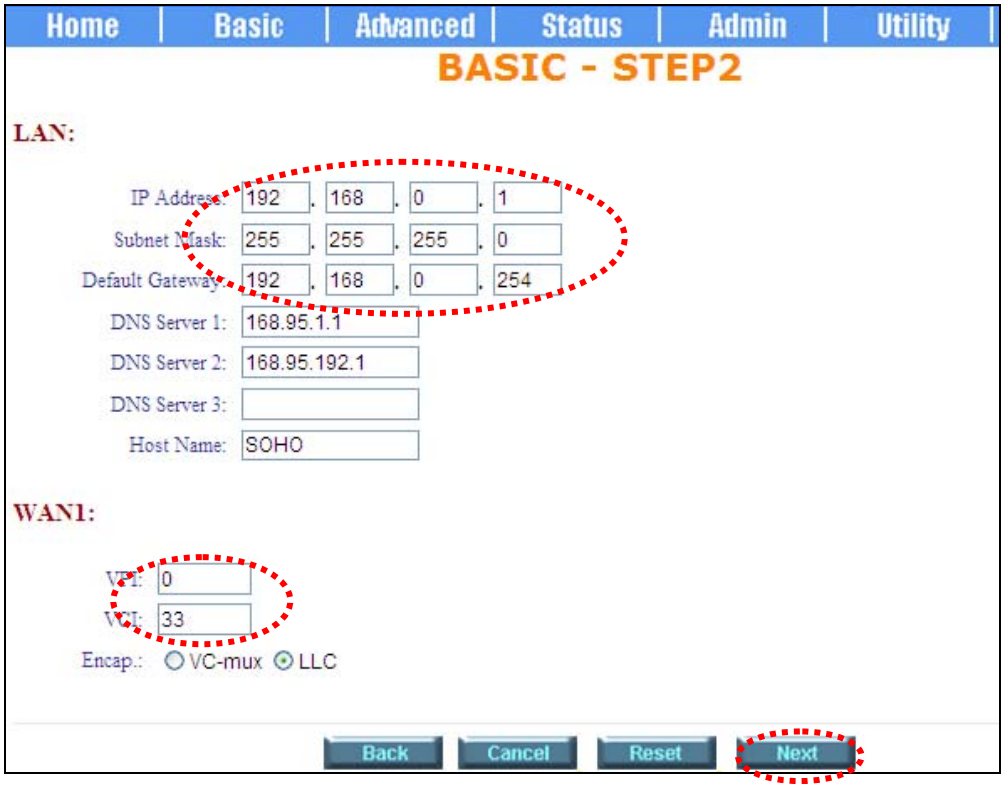
Check Bridge and select CO or CPE in SHDSL mode

to set up bridging mode of the Router and then click Next for the next setting.

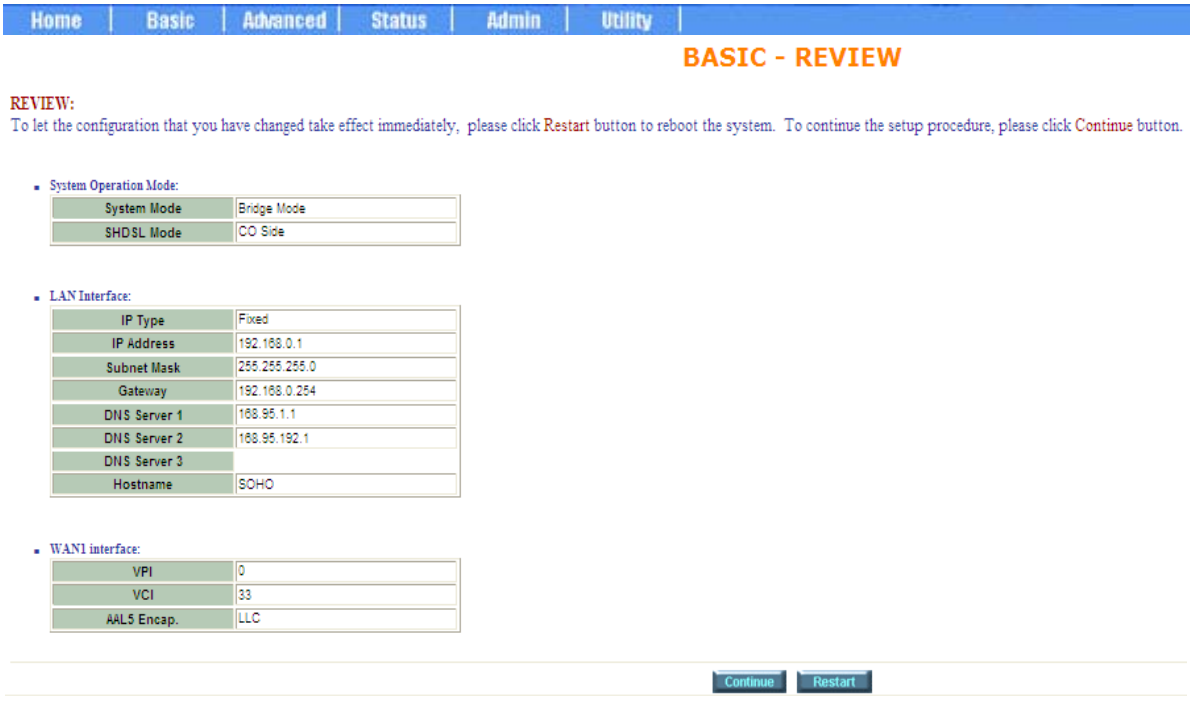


Enter WAN1 VPI: 0 and VCI: 33.
Select WAN1 AAL5 Encap: LLC
Enter LAN IP: 192.168.0.1
Enter LAN Sub-net Mask: 255.255.255.0
Enter Gateway: 192.168.0.254 The Gateway is directly pointed to the BAS IP.
Click Next

Note	You have to do that; otherwise, the new configuration parameters will not affect GRT series.



Click Restart, and GRT series will reboot with the new setting.



3.3.3 Router mode

Routing mode contains DHCP server, DHCP client, and DHCP relay, Point-to-Point Protocol over ATM and Ethernet and IP over ATM and Ethernet over ATM. You have to clarify which Internet protocol is provided by ISP.
Check ROUTE and CPE Side then press Next.
Two SHDSL modes of this product can be set up: Central Office (CO), and Customer Premises Equipment (CPE). For connection with DSLAM, the SHDSL mode is CPE. For LAN to LAN connection, one side must be CO while the other side must be CPE.

3.3.4 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a communication protocol that lets network administrators to manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can be connected to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer. If computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator to supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network. If the DHCP server is enabling, you have to set up the following parameters for processing it as DHCP server.

The embedded DHCP server assigns network configuration information at most 253 users accessing the Internet at the same time.

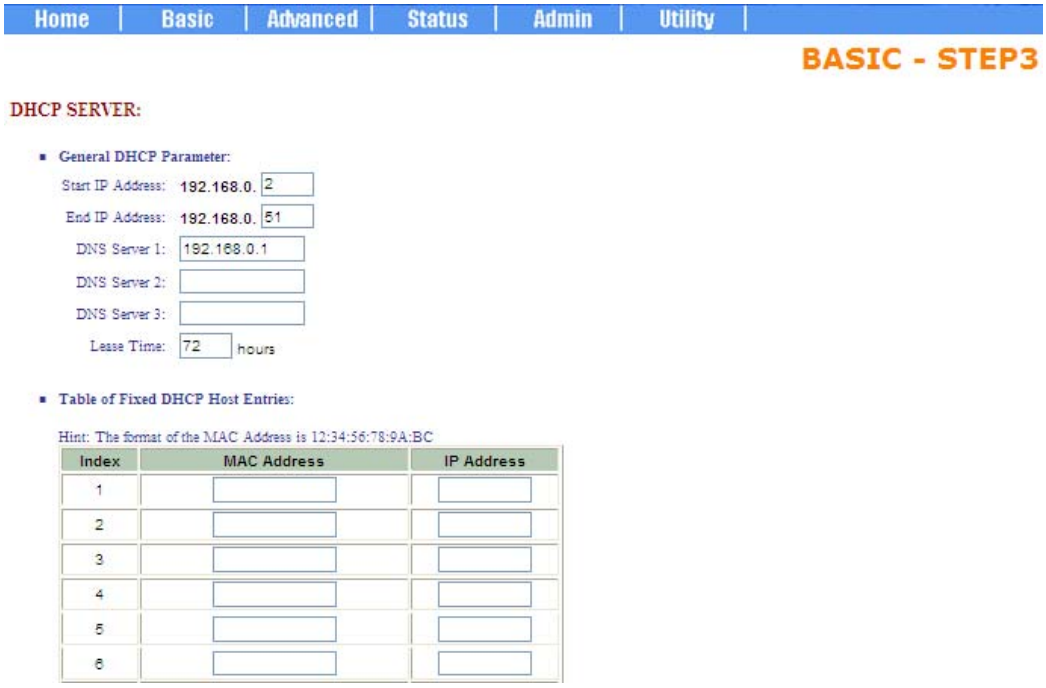
IP type: Fixed
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
Some of the ISPs require the host name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.
Trigger DHCP Service: Server
The default setup is Enable DHCP server.
If you want to turn off the DHCP service,
choose Disable.

For example, if the LAN IP address is 192.168.0.1, the IP range of LAN is 192.168.0.2 to 192.168.0.51. The DHCP server assigns the IP form Start IP Address to End IP Address. The legal IP address range is from 0 to 255, but 0 and 255 are reserved for broadcast so the legal IP address range is from 1 to 254. On the other hand, you cannot assign an IP greater than 254 or less then 1. A lease time of 72 hours indicates that the DHCP server will reassign IP information in every 72 hours.

DNS Server	Your ISP will provide at least one Domain Name Service Server IP. You can type the router IP in this field. The router will act as DNS server relay function.

You may assign fixed IP addresses to some devices while using DHCP, provided that the fixed IP addresses are not within the range used by the DHCP server.

Press Next to setup WAN1 parameters.

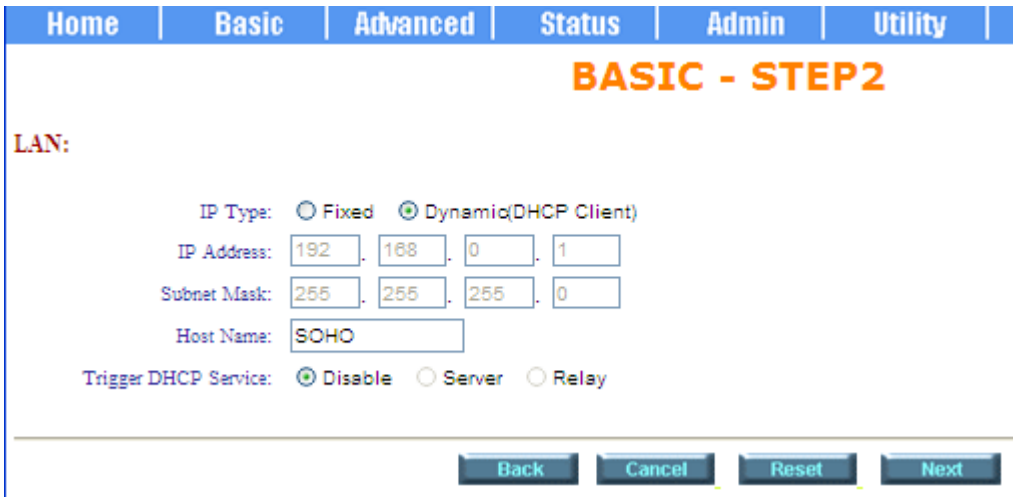


3.3.5 DHCP Client

Some of the ISPs provide DHCP server service by which the PC in LAN can access IP information automatically. To set up the DHCP client mode, follow the procedure.

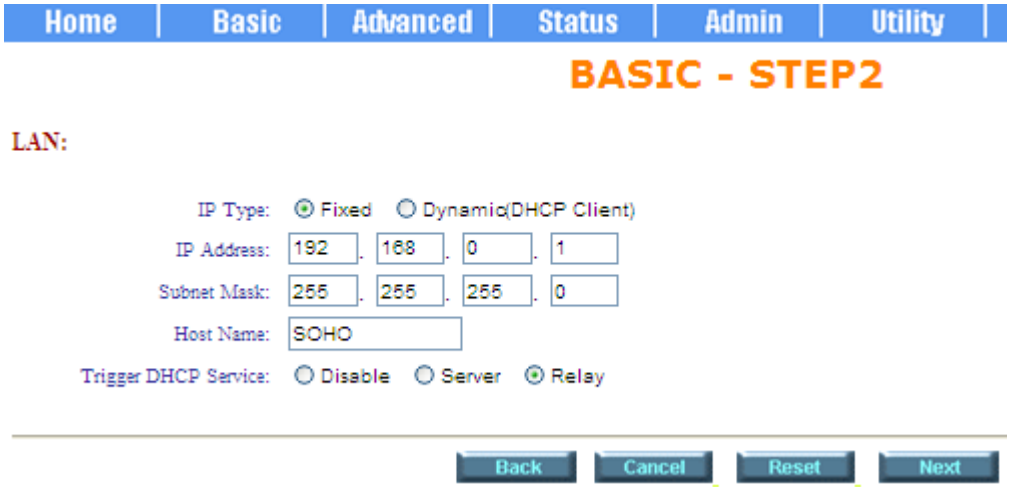
LAN IP Type: Dynamic

Click Next to setup WAN1 parameters.



3.3.6 DHCP Relay

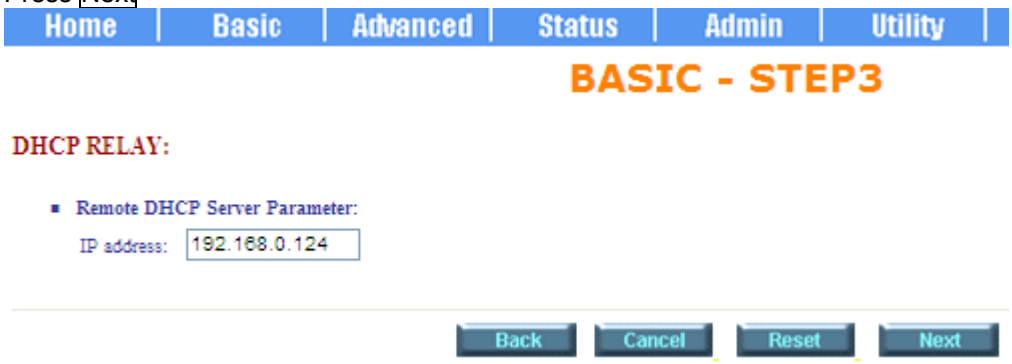
If you have a DHCP server in LAN and you want to use it for DHCP services, the product provides DHCP relay function to meet your need.



IP Type: Fixed
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
Some of the ISPs require the host name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.
Trigger DHCP Service: Relay
Press Next to setup DHCP server parameter.

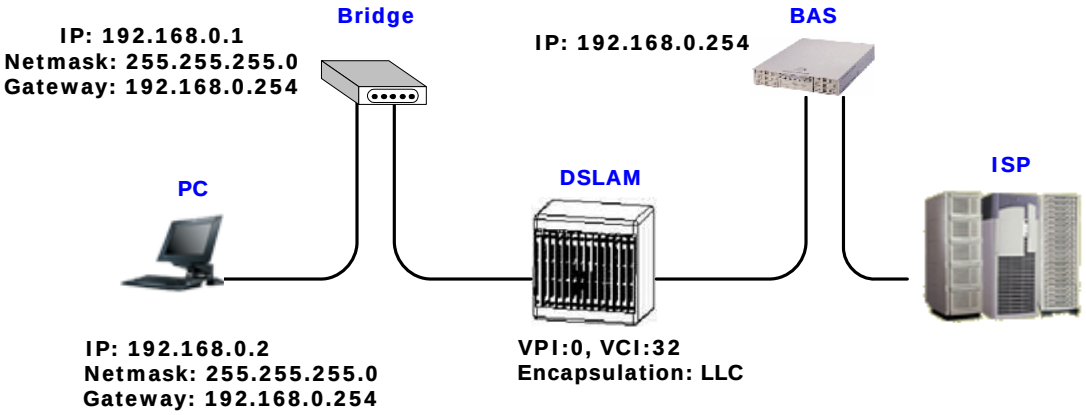
Enter DHCP Server IP address in IP address field.

Press Next



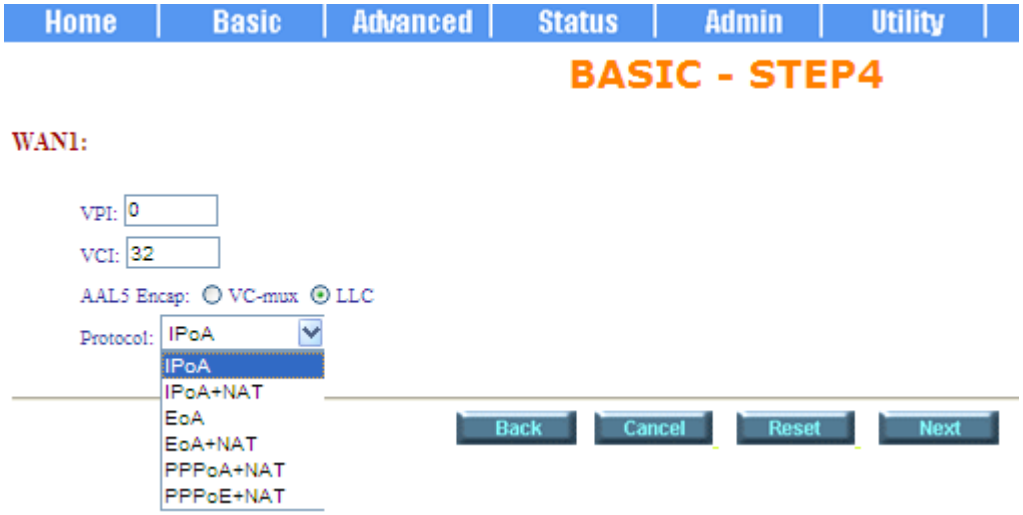
3.3.7 PPPoE and PPPoA

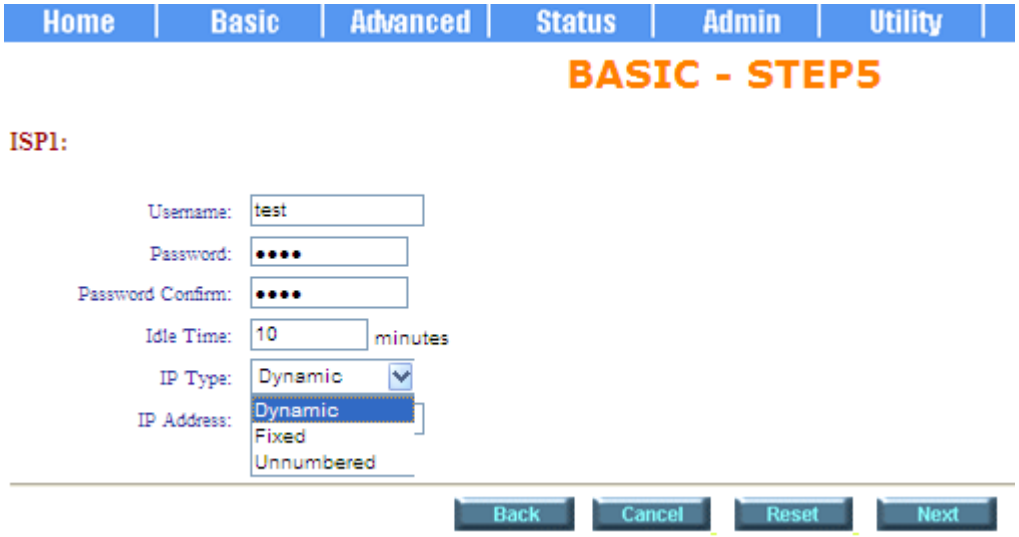
PPPoE (point-to-point protocol over Ethernet) and PPPoA (point-to-point protocol over ATM) are authentication and connection protocols used by many service providers for broadband Internet access. These are specifications for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. PPPoE and PPPoA can be used to office or building. Users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE and PPPoA combine the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol or ATM protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame or ATM frame.



How to set up this mode

Key in the WAN1 parameters:
VPI: 0
VCI: 32
AAL5 Encap: LLC
Protocol: PPPoA + NAT or PPPoE + NAT
Click Next to set up user name and password.



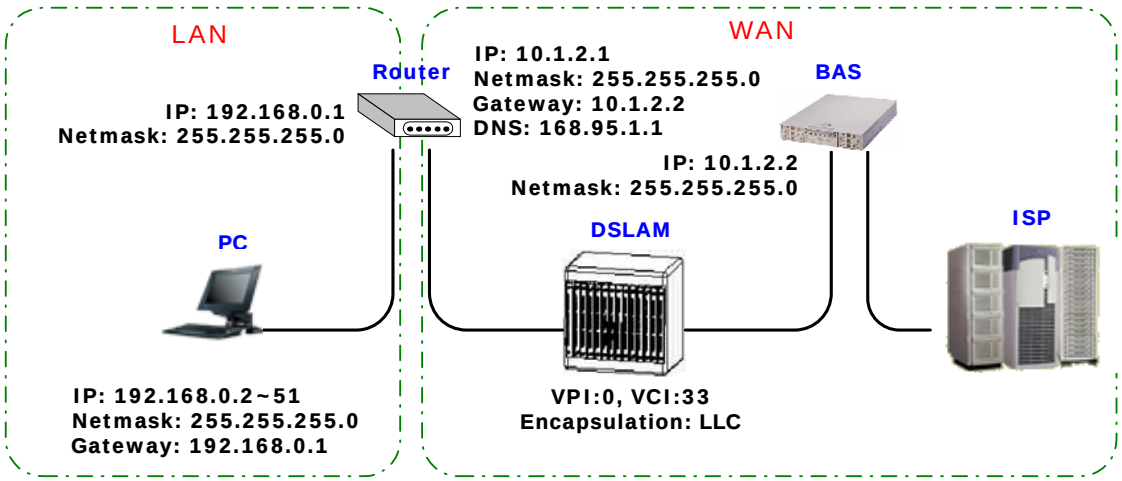


Type the ISP1 parameters.
Username: test
Password: test
Password Confirm: test
Your ISP will provide the user name and password.
Idle Time: 10
You want your Internet connection to remain on at all time, enter 0 in the Idle Time field.
There are three IP types, Dynamic, Static and IP Unnumbered, which you can set up. The default IP type is Dynamic. It means that ISP PPP server will provide IP information including dynamic IP address when SHDSL connection is established. On the other hand, you do not need to type the IP address of WAN1. Some of the ISPs will provide fixed IP address over PPP.
For fixed IP address:
IP Type: Fixed
IP Address: 192.168.1.1
Click Next.

The screen will prompt the parameters that will be written in EPROM. Check the parameters before writing in EPROM.

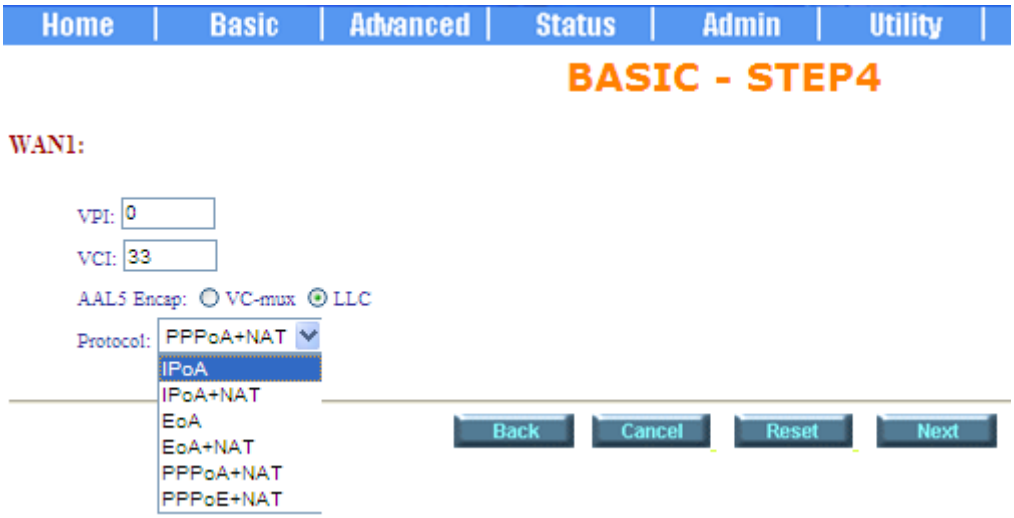
Press Restart to restart the router working with new parameters or press continue to set up another parameter.

3.3.8 IPoA or EoA

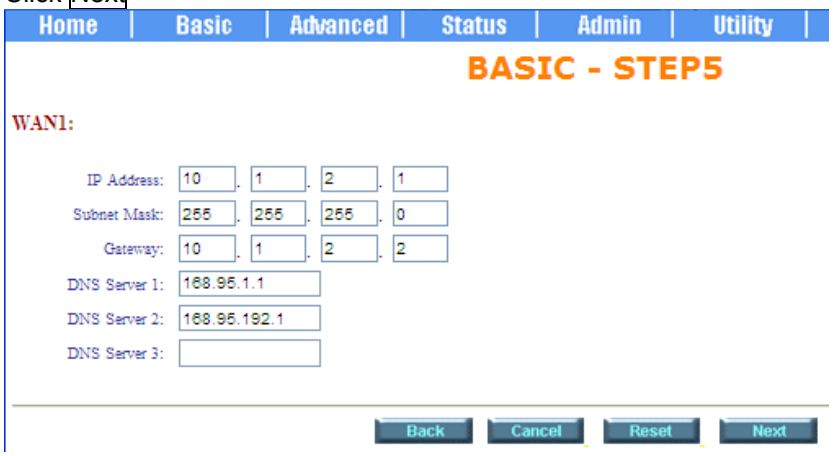


How to set up this mode

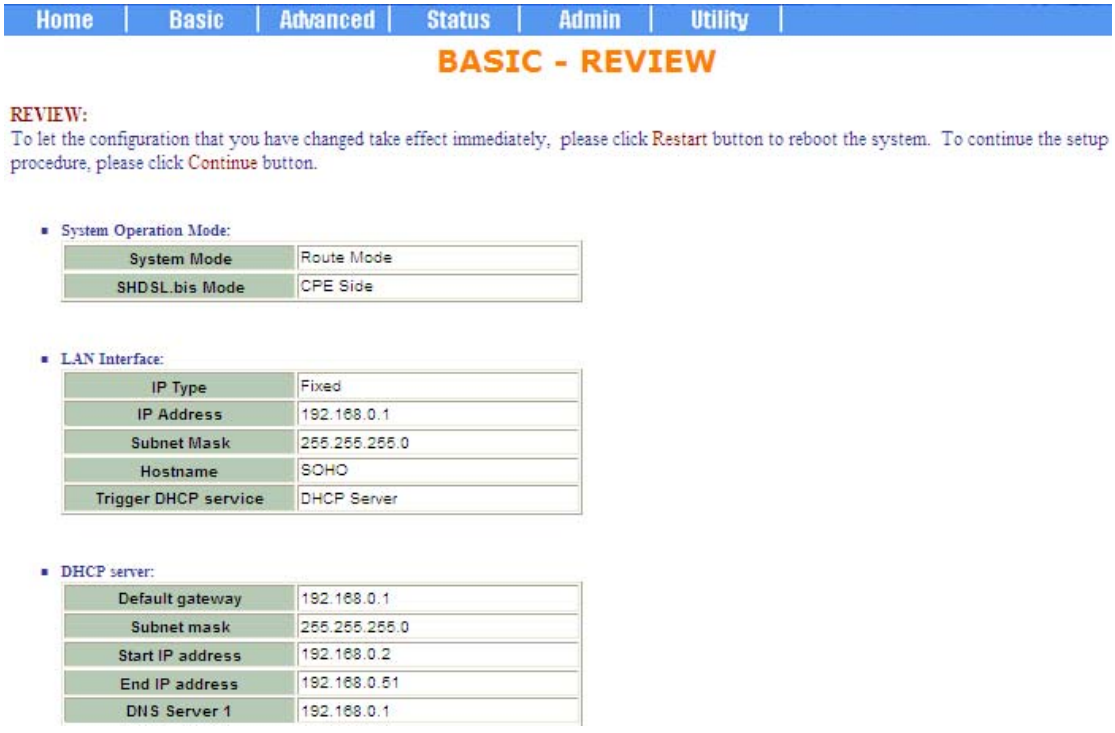
Type the Wan Parameters;
VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: IPoA, EoA, IPoA + NAT or EoA + NAT
Click Next to set up the IP parameters.



IP Address: 10.1.2.1
It is router IP address seem from Internet. Your ISP will provide it and you need to specify here.
Subnet mask: 255.255.255.0
This is the router subnet mask seen by external users on Internet. Your ISP will provide it to you.
Gateway: 10.1.2.2
Your ISP will provide you with the default gateway.
DNS Server 1: 168.95.1.1
DNS Server 1: 168.95.192.1
Your ISP will provide at least one DNS (Domain Name System) Server IP address.
Click Next



The screen will prompt the parameters that will be written in EPROM. Check the parameters before writing in EPROM.



Press Restart to restart the router working with new parameters or press continue to set up another parameter.

- WAN1 interface:

VPI	0
VCI	33
AAL5 Encap.	LLC
Protocol	IPoA+NAT
WAN1 IP address	10.1.2.1
WAN1 subnet mask	255.255.255.0
Gateway	10.1.2.2
DNS Server 1	168.95.1.1
DNS Server 2	168.95.192.1
DNS Server 3	

Continue Restart

Chapter 4 Advanced Setup

Advanced setup contains SHDSL, WAN, Bridge, VLAN, Route, NAT/DMZ, Virtual server and firewall parameters.

4.1 SHDSL.bis

You can set up the Annex type, data rate and SNR margin for SHDSL.bis parameters in SHDSL.bis.

4.1.1 Annex Type:

There are two Annex types: Annex AF and Annex BG . If the router will connect to your ISP, please check with them for the correct setting. If your routers are configured for point to point application, you must choose one of the two types according to which line rate you need.

4.1.2 Link Type:

There are five Line Types for you to choose from: 2-Wire, 4-Wire, Auto Fall Back, StandBy and Multi-link.

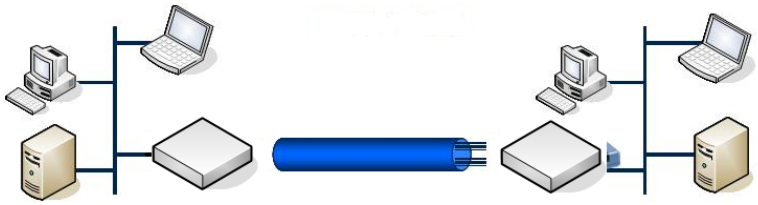
2-wire Mode

2-wire router will provide data rate up to 5.696Mbps.

For 4-wire model, it only can use the first one pair for the single- pair DSL wire application.

4-wire Mode

4-wire router will provide data rate up to **11.392Mbps**.



In this mode, each wire pairs of SHDSL.bis router must be configured with the same line rate. If one pair fails then the entire line must be restarted.

Auto Fall Back Mode

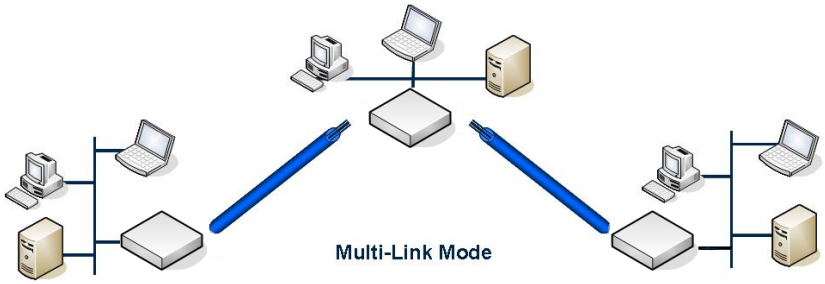
Two DSL pairs are working simultaneously. When one pair of both is disconnected, the other pair will keep working.

Standby Mode

Only one of the two pairs is working; the other pair is standby as backup. If the working pair fails, the standby pair will start up to continue.

Multi–Link Mode

For 4-wire model, each pair will connect to a two different remote device, which may or may not be in the same location. The routers can be used to create a daisy chain or ring network. Channel A used as CO side and Channel B used as CPE side.



4.1.3 TCPAM Type:

TCPAM stands for Trellis Coded Pulse Amplitude Modulation. It is the modulation format that is used in both HDSL2 and SHDSL, and provides robust performance over a variety of loop conditions. SHDSL.bis supports 16 level TCPAM line code(TPCAM-16) or 32 level TCPAM line code(TCPAM-32) to provide a rate/reach adaptive capability, offering enhanced performance (increased rate or reach) and improved spectral compatibility. The default option is Auto. You may assign the different type manually by clicking the caption TPCAM-16 or TPCAM-32. Only Annex AF and BG can apply using TCPAM-32.

4.1.4 Data Rate:

For 2-wire model (n*64kbps)

You can set up the SHDSL.bis data rate in the multiple of 64kbps.

The default data rate is 5696Kbps (n=89).

For using Annex AF or BG

TCPAM32 ; data rate is 192768Kbps ~ 5696Kbps (Nx64kbps, N=312~89)

TCPAM16 ; data rate is 192Kbps ~ 3840Kbps (Nx64kbps, N=3~60)

For using Annex A or B

TCPAM16 ; 192Kbps ~ 2304Kbps (Nx64kbps, N=3~36)

For 4-wire model (n*128kbps)

You can set up the SHDSL.bis data rate in the multiple of 128kbps.

The default data rate is 11392Kbps (n=89).

For using Annex AF or BG

TCPAM32 ; data rate is 3841536Kbps ~ 11392Kbps (Nx128kbps, N=312~ 89)

TCPAM16 ; data rate is 384Kbps ~ 7680Kbps (Nx128kbps, N=3~60)

		2-wire model	4-wire model
Annex AF/BG	TCPAM-16	192~3840 kpbs	384~7680 kbps
	TCPAM-32	192~5696 kpbs	384~11392 kbps

4.1.5 SNR margin:

This is an index for line connection quality. You can see the actual SNR margin in STATUS SHDSL.bis. The larger the SNR margin is, the better the line connection quality is.

The range of SNR margin is -10 to 21.

If you set SNR margin in the field as 3, the SHDSL.bis connection will drop and reconnect when the SNR margin is lower than 3. On the other hand, the device will reduce the line rate and reconnect for better line connection quality.

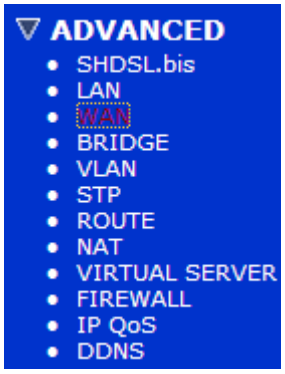
4.1.6 TC Layer:

There are two TC layer setting on this router: EFM layer and ATM layer. It is based on the networks connected: ATM-based Access Network or Ethernet-based Access Network.

Rate Mode: For adaptive mode, you have to configure it in rate mode. The router will adapt the optimal data rate according to the line status.

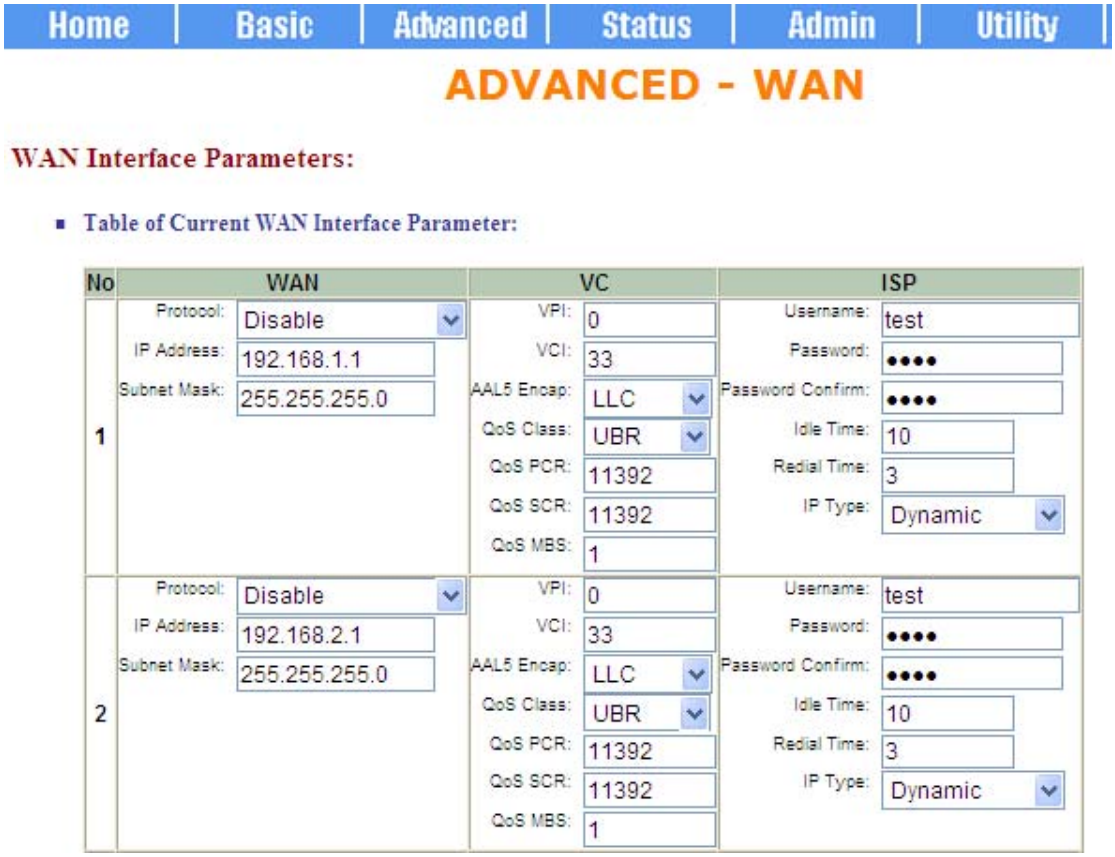
4.2 WAN

The router can support up to 8 PVCs. WAN 1 was configured via **BASIC** menu except QoS. If you want to set up another PVCs such as WAN 2 to 7, those parameters can be configured and set up on the pages of WAN under ADVANCED. On the other hand, you don't need to setup WAN unless except you apply two or more Internet Services with ISPs.



The parameters in WAN Number 1 has been set up in Basic Setup.

If you want to set up additional PVCs, you can configure in WAN 2 to WAN 8.



Enter the parameters:

Protocol: If WAN Protocol is PPPoA or PPPoE with dynamic IP, leave the default WAN IP Address and Subnet Mask as default setting. The system will ingore the IP Address and Subnet Mask information, but leaving erasion or blanks in default setting will cause system error.

If the WAN Protocol is IPoA or EoA, leave the ISP parameters as default setting. The system will ingore the information, but leavingerasion or blanks in default setting will cause system error.

VC-mux (VC-based Multiplexing): Each protocol is assigned to a specific virtual circuit. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC (LLC-based Multiplexing): One VC carries multiptle protocols with protocol identifying information being contained in each packet header. Desapite the extra bandwidth and processing overhead, this method may be advantagrous if it is not practical to have a sepatate VC for each carried protocol.

VPI (Virtual Path Identifier): is for set up ATM Permanent Virtual Channels (PVC).The valid range for VPI is 0 to 255.

VCI (Virtual Channel Identifier is for set up ATM Permanent Virtual Channels (PVC): The valid range for VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic.)

QoS (Quality of Service) class : The Traffic Management Specification V4.0 defines ATM service cataloges that describe both the traffic transmitted by users onto a network as well as the Quailty of Service that the network needs to provide for that traffic. There are four classes to be selected: UBR, CBR, rt-VBR and nrt-VBR. Select CBR to specify fixed bandwidth for voice or data traffic. Select UBR for applications that are not time-sensitive such as e-mail. Select VBR for bursty traffic and bandwidth sharing with other applications.

UBR (Unspecified Bit Rate): is the simplest service provided by ATM networks. There is no guarantee of anything. It is a primary service used for transferring Internet traffic over the ATM network.

CBR (Constant Bit Rate): is used by connections that require a static amount of bandwidth that is available during the connection life time. This bandwidth is characterized by Peak Cell Rate (PCR). Based on the PCR of the CBR traffic, specific cell slots are assigned for the VC in

the schedule table. The ATM always sends a single cell during the CBR connection's assigned cell slot.

VBR-rt (Varible Bit Rate real-time) is intended for real-time applications, such as compressed voice over IP and video comferencing, that require tightly constrained delays and delay variation. VBR-rt is characterized by a peak cell rate (PCR), substained cell rate (SCR), and maximun burst rate (MBR).

VBR-nrt (Varible Bit Rate non-real-time) i*s intended for non-real-time applications, such as FTP, e-mail and browsing.*

PCR (Peak Cell Rate) in kbps: The maximum rate at which you expect to transmit data, voice and video. Consider PCR and MBS as a menas of reducing lantency, not increasing bandwidth. The range of PCR is 384kbps to 11392kbps

SCR (Substained Cell Rate): The sustained rate at which you expect to transmit data, voice and video. Consider SCR to be the true bandwidth of a VC and not the long-term average traffic rate. The range of SCR is 384kbps to 11392kbps.

MBS (Maximum Burst Size): Refers to the maximum number of cells that can be sent at the peak rate. The range of MBS is 1 cell to 255 cells.

Username : Enter the user name exactly as your ISP assigned.

Password: Enter the password associated with the user name above.

Password confirm: Enter the password again for confirmation.

Idle Time: You can specify an idle time on this field when you don't want the connection up all the time.

IP type: A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a differnet one each time you connect to the Internet.

Press Finish to finish setting.

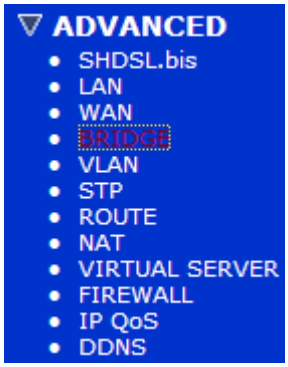
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

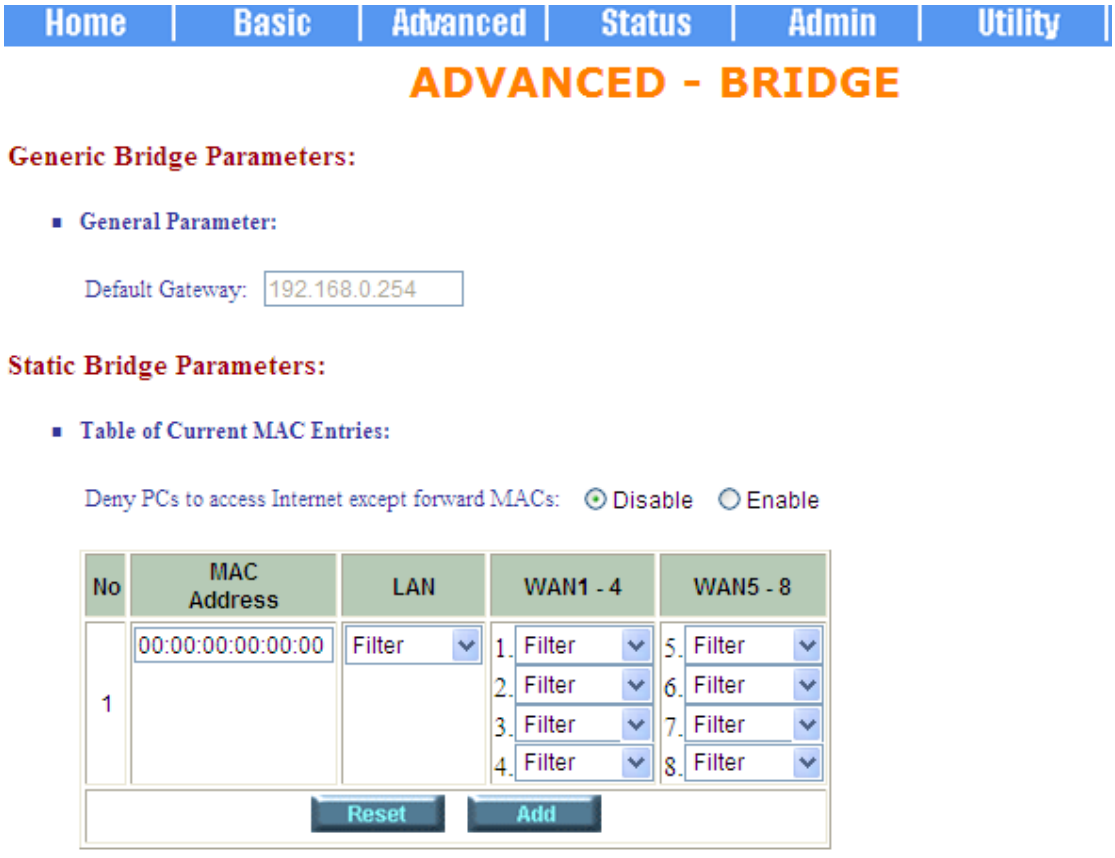
Press Restart to restart the router working with new parameters or press continue to setup other parameters.

4.3 Bridge

If you want to setup advanced filter function while router is working in bridge mode, you can use **BRIDGE** menu to setup the filter/blocking function.

Click Bridge to setup.





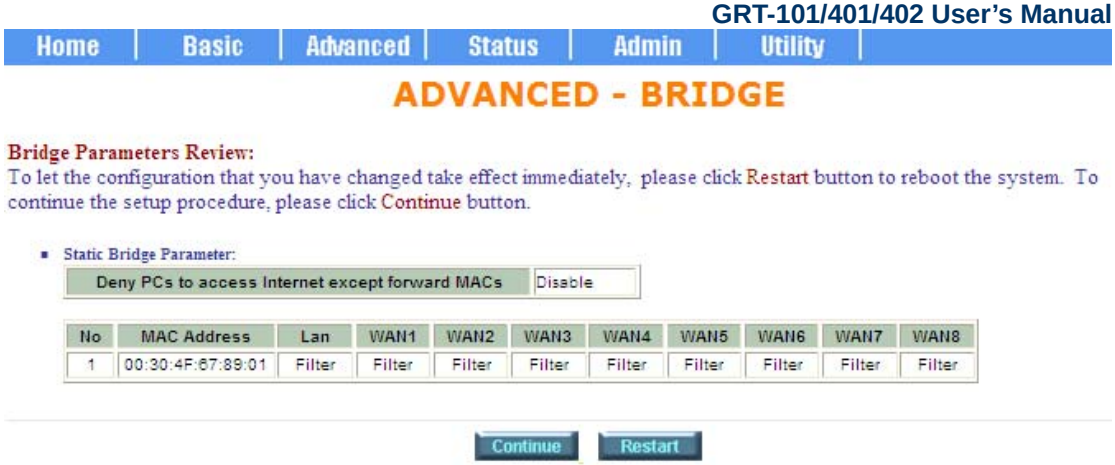
Press Add on the bottom of web page to add the static bridge information.

If you want to filter the designated MAC address of LAN PC to access Internet, press Add to establish the filtering table. Put the MAC address in **MAC Address** field and select Filter in **LAN** field.

If you want to filter the designated MAC address of WAN PC to access LAN, press Add to establish the filtering table. Key the MAC address in **MAC Address** field and select Filter in WAN field.

For example: if your VC is setup at WAN 1, select WAN 1 Filter.

Press Finish on the bottom of web page to review the bridge parameters.

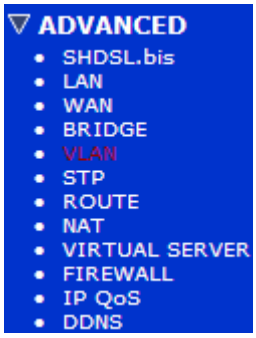


The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press Continue to setup another parameter.

4.4 VLAN

Click VLAN to configure VLAN.

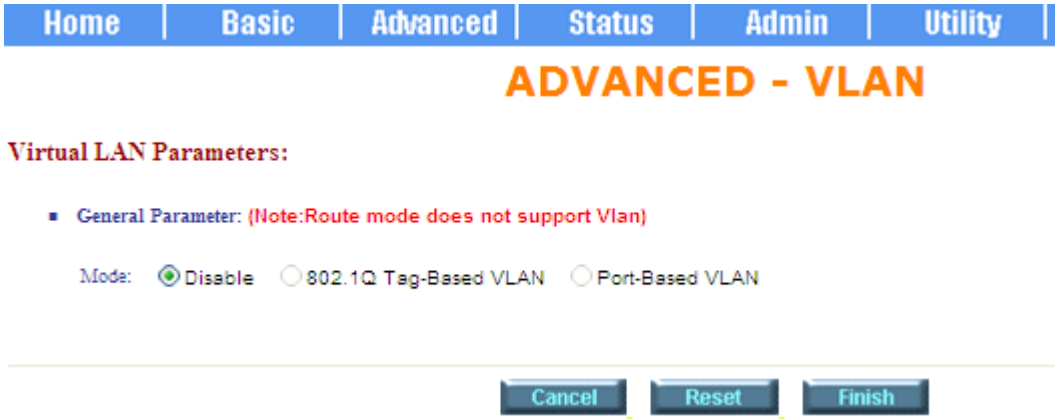


VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group.

With MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN.

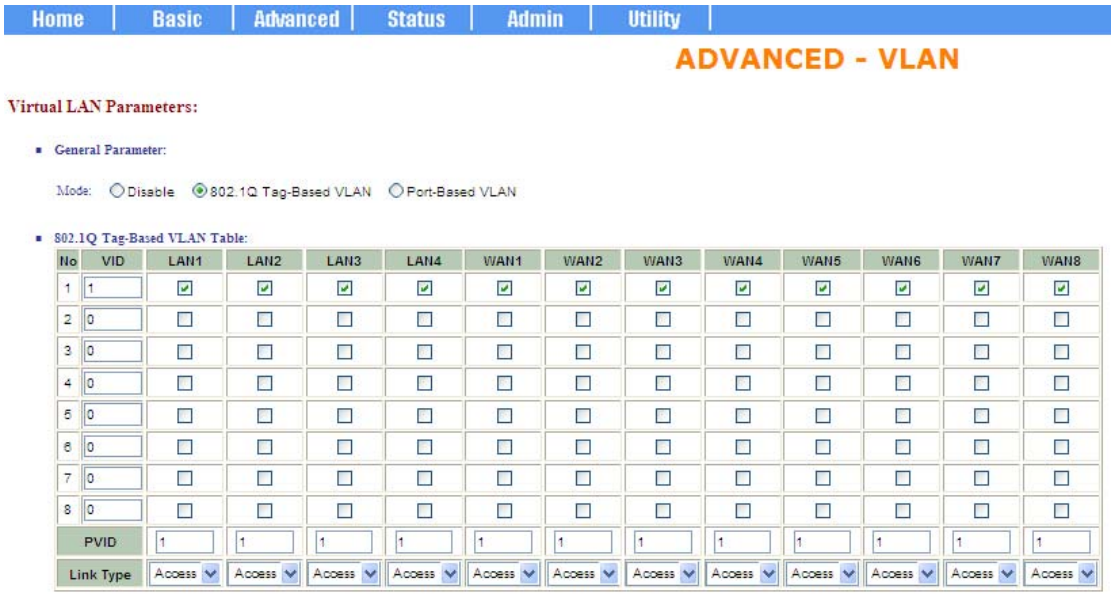
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

The IEEE 802.1Q defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure.



4.4.1 802.1Q Tag-based VLAN

For setting 802.1Q VLAN check the 802.1Q Tag-based VLAN. The screen will prompt as the following.



VID: (Virtual LAN ID) It is a definite number of ID range from 1 to 4094.

PVID: (Port VID) It is an untagged member from 1 to 4094 of default VLAN.

Link Type: Access means the port can receive or send untagged packets.

Trunk means that the port can receive or send tagged packets.

By default, the router initially configures one VLAN, VID=1.

A port such as LAN1 to LAN4 and WAN1 to WAN8 can have only one PVID, but can have as many VIDs as the router can store in the VLAN table.

Ports in the same VLAN group share the same frame broadcast domain, thus increasing network performance through reduced boardcast traffic. VLAN groups can be modified at any

time by adding, moving or changing ports without any re-cabling.

4.4.2 Port-based VLAN

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

For setting Port-based VLAN, Check Port-based VLAN, The screen will prompt as follows:

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

When using the port-based VLAN, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members in the same VLAN. The network administrator typically performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN.

- Port Based VLAN Table:

No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

The default setting is all ports (LAN1 to LAN4 and WAN1 to WAN8) connected together which means all ports can communicate with each other. That is, there are no virtual LANs. The option is the most flexible but the least secure.

- Port Based VLAN Table:

No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐
2	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐
3	☐	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐
4	☐	☐	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

4.5 STP

This Web page allows you to configure Bridge STP Parameters as Disable, STP or RSTP.

STP (Spanning-Tree Protocol) defined in the IEEE 802.1D, is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.
Multiple active paths between stations cause loops in the network. If a loop exists in the network topology, the potential exists for duplication of messages. When loops occur, some switches see stations appear on both sides of the switch. This condition confuses the forwarding algorithm and allows duplicate frames to be forwarded.

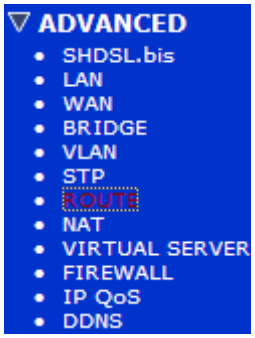
To provide path redundancy, Spanning-Tree Protocol defines a tree that spans all switches in an extended network. Spanning-Tree Protocol forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path.

Spanning-Tree Protocol operation is transparent to end stations, which are unaware whether they are connected to a single LAN segment or a switched LAN of multiple segments. RSTP (Rapid Spanning Tree Protocol) defined in the IEEE 802.1w can be seen as an enhancement of the 802.1D standard. Most parameters have been left unchanged so users familiar with 802.1D can quickly configure the new protocol. In most cases, RSTP performs better than STP.

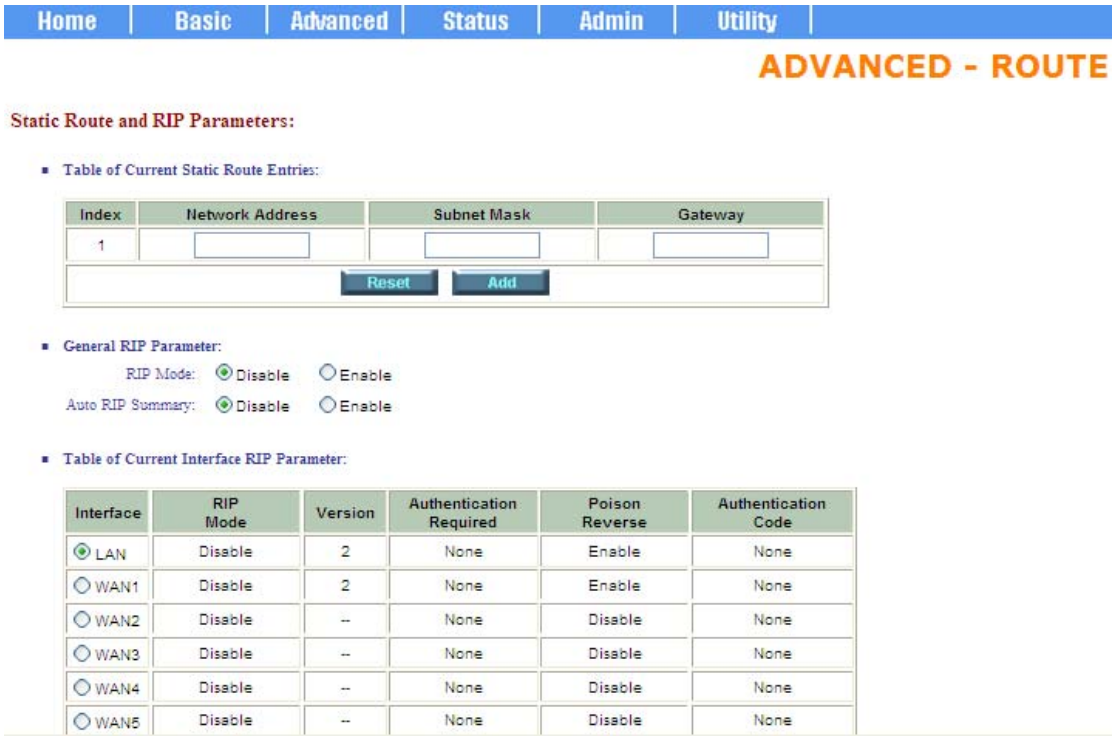
4.6 Route

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

With Dynamic Routing, you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.



Click Route to modify the routing information.



There are maximun 20 entries to set up the static router.

Press Add to add each entry. For example, there are 20 entries as follows:

Static Route and RIP Parameters:

- **Table of Current Static Route Entries:**

Index	Network Address	Subnet Mask	Gateway
1	192.168.1.1	255.255.255.0	192.168.0.254
2	192.168.2.2	255.255.255.0	192.168.0.254
3	192.168.3.3	255.255.255.0	192.168.0.254
4	192.168.4.4	255.255.255.0	192.168.0.254
5	192.168.5.5	255.255.255.0	192.168.0.254
6	192.168.6.6	255.255.255.0	192.168.0.254
7	192.168.7.7	255.255.255.0	192.168.0.254
8	192.168.8.8	255.255.255.0	192.168.0.254
9	192.168.9.9	255.255.255.0	192.168.0.254
10	192.168.10.10	255.255.255.0	192.168.0.254
11	192.168.11.11	255.255.255.0	192.168.0.254
12	192.168.12.12	255.255.255.0	192.168.0.254
13	192.168.13.13	255.255.255.0	192.168.0.254
14	192.168.14.14	255.255.255.0	192.168.0.254
15	192.168.15.15	255.255.255.0	192.168.0.254
16	192.168.16.16	255.255.255.0	192.168.0.254
17	192.168.17.17	255.255.255.0	192.168.0.254
18	192.168.18.18	255.255.255.0	192.168.0.254
19	192.168.19.19	255.255.255.0	192.168.0.254
20	192.168.20.20	255.255.255.0	192.168.0.254

Reset Delete Modify

To modify the RIP (Routing information protocol) Parameters:

RIP Mode: Enable

Auto RIP Summary: Enable

Press Modify

- **General RIP Parameter:**

RIP Mode: Disable Enable

Auto RIP Summary: Disable Enable

- **Table of Current Interface RIP Parameter:**

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	None
WAN1	Disable	2	None	Enable	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Reset Modify

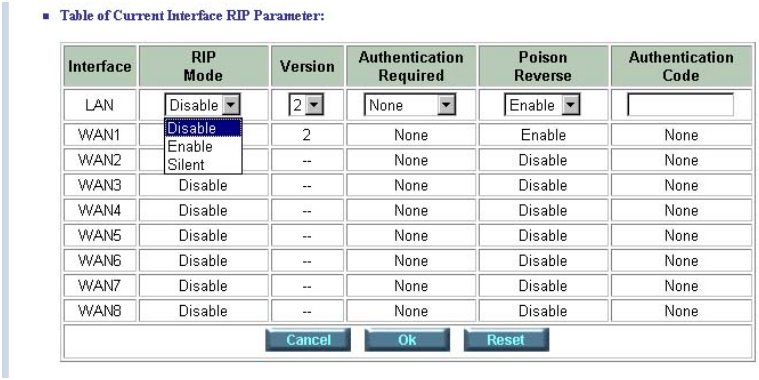
RIP Mode:

This parameter determines how the router handle RIP (Routing information protocol). RIP allows it to exchange routing information with other router.

Disable: The gateway does not participate in any RIP exchange with other routers.

Enable: The router broadcasts the routing table of the router on the LAN and incoporates RIP broadcast by other routers into it's routing table.

Silent: The router does not broadcast the routing table, but it accepts RIP broadcast packets that it receives.

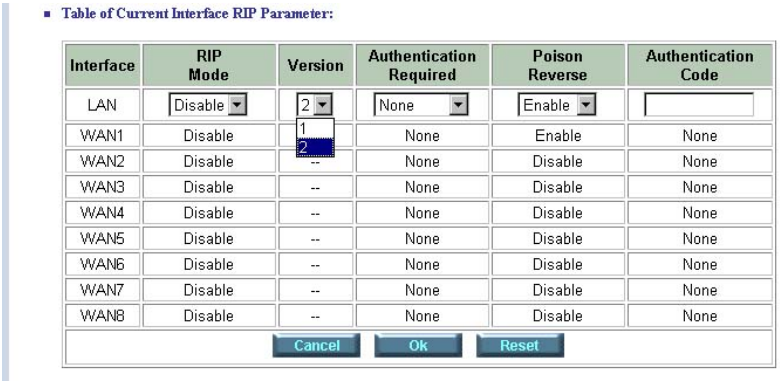


RIP Version:

It determines the format and broadcasting method of any RIP transmissions by the gateway.

RIP v1: it only sends RIP v1 messages only.

RIP v2: it sends RIP v2 messages in multicast and broadcast format.

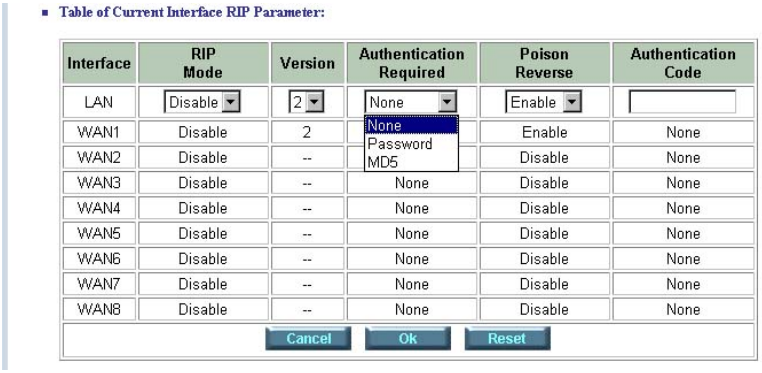


Authentication required:

None: for RIP, there is no need of authentication code.

Password: the RIP is protected by password/authentication code.

MD5: The RIP will be decoded by MD5 then protected by password/authentication code.

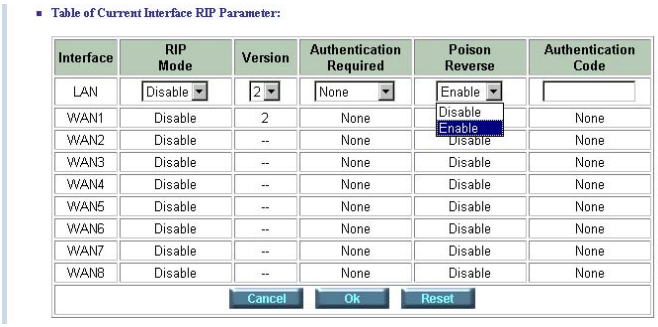


Poison Reserve:

Poison Reserve is for the purpose of promptly broadcast or multicast the RIP while the route is changed. (e.g. shutting down one of the routers in routing table)

Enable: the gateway will actively broadcast or multicast the information.

Disable: the gateway will not broadcast or multicast the information.



Authentication code:

You can set up an authentication code here.

After modifying the RIP parameters, press finish.

The screen will prompt the modified parameter. Check the parameters and press Restart to restart the router or press Continue to set up another parameters.

4.7 NAT/DMZ

NAT *(Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One*

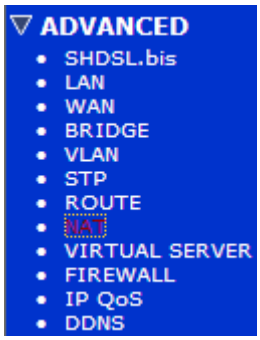
network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and reverse the global IP addresses of incoming packets back into local IP addresses. This ensure security since each outgoing or incoming request must go through a translation process, that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and lets the company to use a single IP address of its communication in the Internet world.

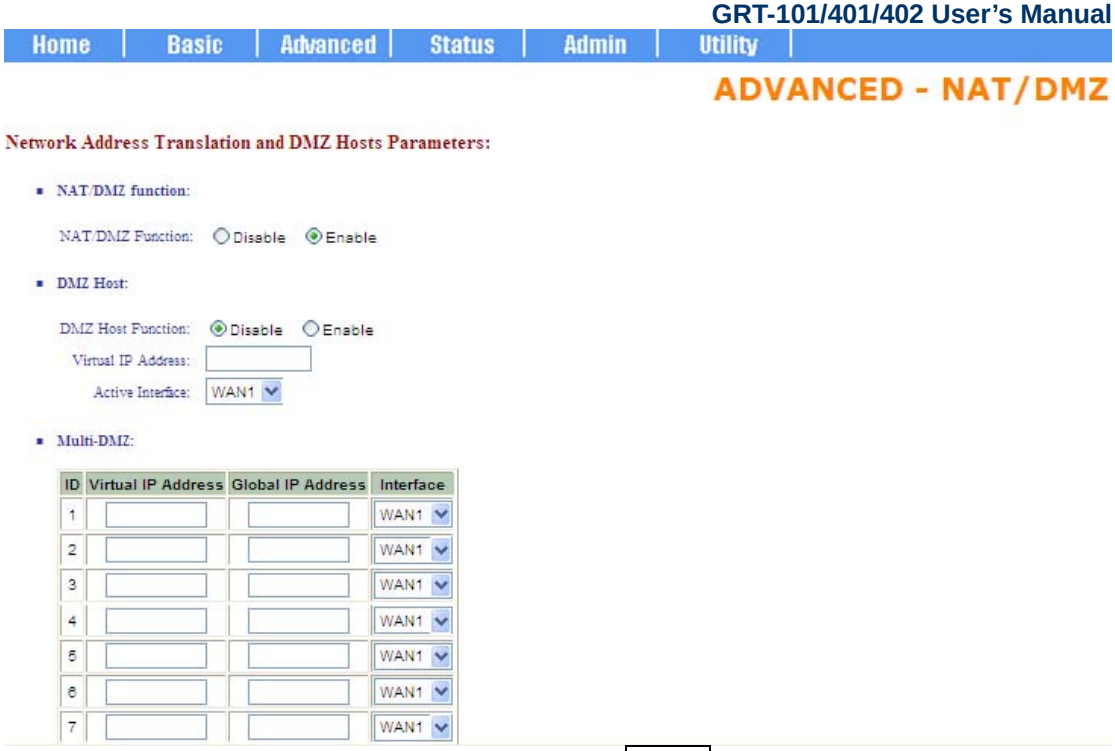
DMZ *(Demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company private network and the outside public network. It prevents outside users from getting direct access to a server that has company private data.*

In a typical DMZ configuration for an enterprise, a separate computer or host receives requests from users within the private network to access via Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests to the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could serve the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted, but no other company information would be exposed.

Press NAT to set up the parameters.





If you want to enable the NAT/DMZ functions, check Enable. The IP address assigned to the WAN will enable DMZ function for the virtual IP address.

4.7.1 Multi-DMZ

Some users have two or more global IP addresses assigned by ISP, which can use multi DMZ. The table is for mapping of global IP address and virtual IP address.

4.7.2 Multi-NAT

Some of the virtual IP addresses (eg: 192.168.0.10 ~ 192.168.0.50) collectively use two of the global IP addresses (eg: 69.210.1.9 and 69.210.1.10). The Multi-NAT table will be set up as:

Virtual Start IP Address: 192.168.0.10

Count: 40

Global Start IP Address: 69.210.1.9

Count: 2

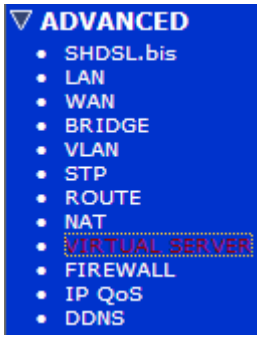
Press Finish to continue to review.

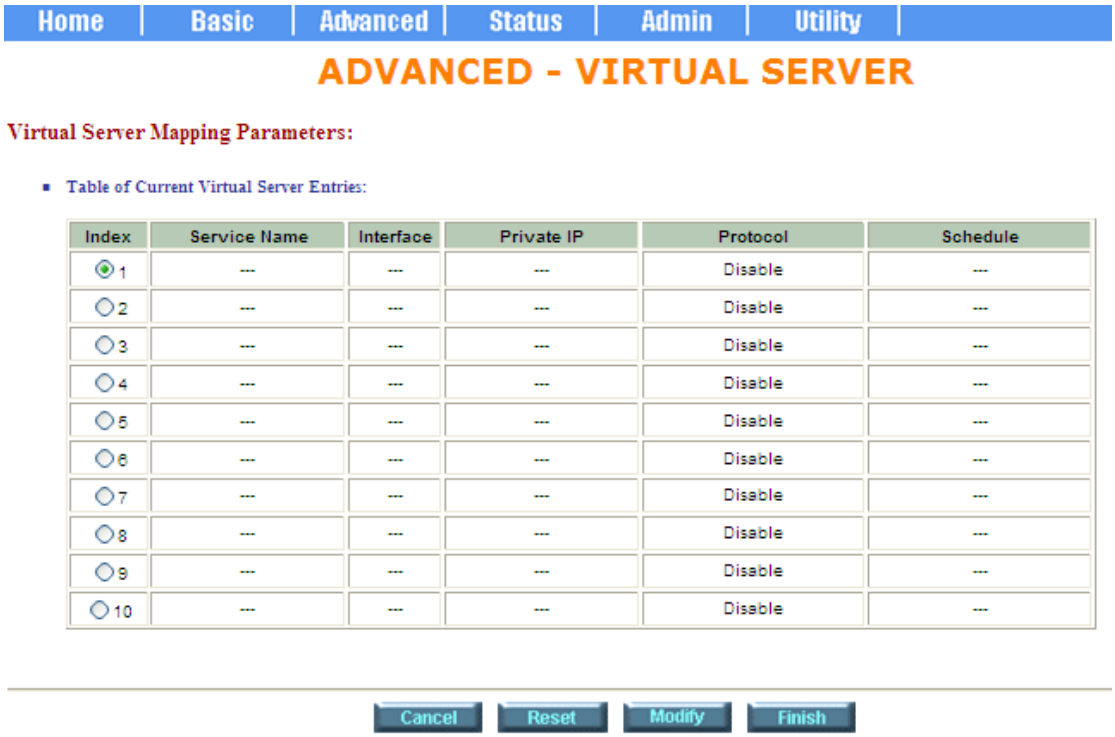
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM. Press Restart to restart the router working with new parameters or Continue to configure another parameter.

4.8 Virtual Server

This section guides you to configure Virtual Servers.

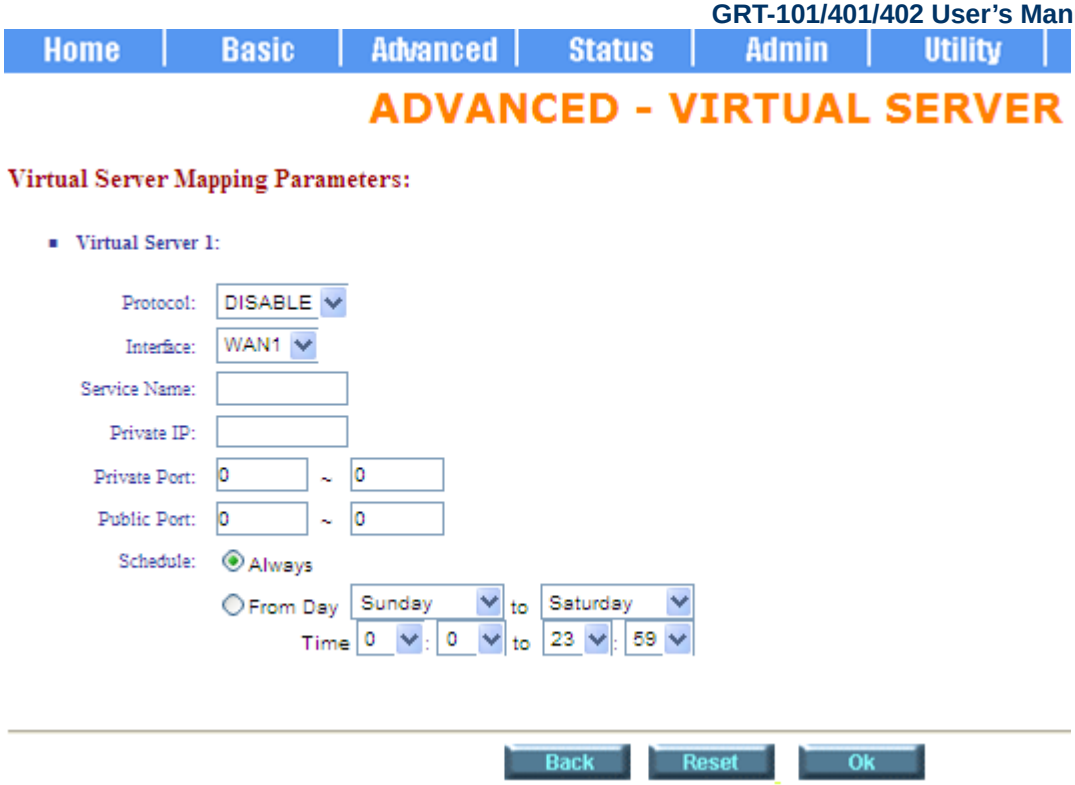
Click Virtual Server to configure the parameters.





Up to ten virtual servers index form 1 to 10 can been configured.

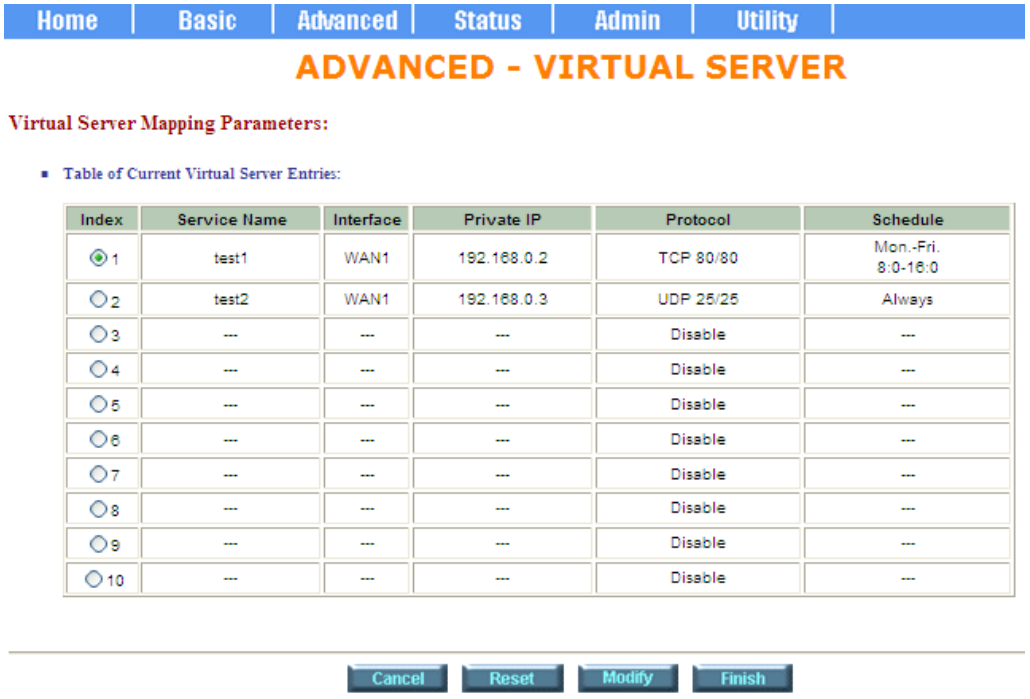
Press Modify to modify index 1.



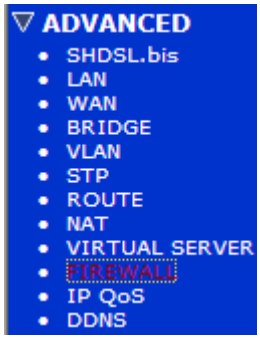
Type the necessary parameters and then click OK.

Press Restart to restart the router or press Continue to set up another function.

For example, you can set up the router as Index 1, protocol TCP, interface WAN1, service name test1, private IP 192.168.0.2, private port 80, public port 80, schedule from Monday to Friday and from 800 to 1600 hours; and index 2, protocol UDP, interface WAN1, service name test2, private IP 192.168.0.3, private port 25, public port 25, schedule always.



4.9 Firewall



A firewall is a set of related programs that protects the resources of a private network from other networks. It prevents hackers to access your private data resource.
There are three security levels: **basic firewall security**, **automatic firewall security** and **advanced firewall security**.

4.9.1 Basic Firewall Security

Check Basic Firewall Security.

This level only enables the NAT firewall and the remote management security. The NAT firewall will take effect when NAT function is enabled. The remote management security by default will block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.
Press Finish to finish setting of firewall and review the parameters.

The screen will prompt the parameters to be recorded in NVRAM. Please check these parameters.

Press Restart to restart the router or press Continue to set up another function.

4.9.2 Automatic Firewall Security

Check Automatic Firewall Security.

This level enables basic firewall security, all DoS protection and the SPI filter function.

Press Finish to complete setting firewall.

The screen will prompt the parameters, which will be written in NVRAM. Please check these parameters.

Press Restart to restart the router or press Continue to set up another function.

User can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter. Please note that an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

4.9.3 Advanced Firewall Security

Check Advanced Firewall Security and then press Finish.

A user can determine the security level for special purpose, environment and applications by configuring the DoS protection and defining an extra packet filter. Please notice that an improper filter policy may degrade the capability of the firewall and even block the normal

network traffic. It can set up the DoS protection parameters

SYN flood: A SYN flood is a form of denial-of-service attack, attempts to slow your network by requesting new connections but not completing the process to open the connection. Once the buffer for these pending connections is full a server will not accept any more connections and will be unresponsive.

ICMP flood: A sender transmits a volume of ICMP request packets to cause all CPU resources to be consumed serving the phony requests.

UDP Flood: A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol (UDP). A sender transmits a volume of requests for UDP diagnostic services which cause all CPU resources to be consumed serving the phony requests.

Ping of Death: A ping of death (abbreviated "POD") attack attempts to crash your system by sending a fragmented packet, when reconstructed is larger than the maximum allowable size.

Land attack: A land attack is an attempt to slow your network down by sending a packet with identical source and destination addresses originating from your network.

IP Spoofing: IP Spoofing is a method of masking the identity of an intrusion by making it appeared that the traffic came from a different computer. This is used by intruders to keep their anonymity and can be used in a Denial of Service attack.

Smurf attack: The Smurf attack is a way of generating a lot of computer network traffic to a

victim host. That is a type of denial-of-service attack. A Smurf attack involves two systems. The attacker sends a packet containing an ICMP echo request (ping) to the network address of one system. This system is known as the amplifier. The return address of the ping has been faked (spoofed) to appear to come from a machine on another network (the victim). The victim is then flooded with responses to the ping. As many responses are generated for only one attack, the attacker is able use many amplifiers on the same victim.

Fraggle attack: A Fraggle attack is a type of denial-of-service attack where an attacker sends a large amount of UDP echo traffic to IP broadcast addresses, all of it having a fake source address. This is a simple rewrite of the smurf attack code.

For SYN attack, ICMP flood and UDP flood, they can set up the threshold of packets number per second. The default values are 200 packets per second. If everything is working properly, you probably do not need to change the threshold setting as the default threshold values. Reduce the threshold values if your network is slower than average.

Traditional firewall is stateless meaning they have no memory of the connections of data or packets that pass through them. Such IP filtering firewalls simply examine header information in each packet and attempt to match it to a set of define rule. If the firewall finds a match, the prescribe action is taken. If no match is found, the packet is accepted into the network, or dropped, depending on the firewall configuration.

Packet filter

Click Next to set up the packet filtering parameters.

If you want to configure the Packet Filtering Parameters, choose **Enable** and press Add.

It can set up the packet filter rule parameters:

Select the Protocol and configure the parameter.

Protocol: ANY, TCP, UDP, ICMP, GRE, RSVP, ESP and AH. (ANY means all protocols)

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
GRE	Generic Routing Encapsulation
RSVP	Resource Reservation Protocol
ESP	Encapsulating Security Payload
AH	Authentication Header

Direction: INBOUND (from WAN to LAN) or OUTBOUND (from LAN to WAN)

Action: DENY (block) or PERMIT (allow)

Description: Type a description for your customized service..

Src. IP Address: The source addresses or ranges of addresses to which this packet filter rule applies. (Address 0.0.0.0 is equivalent any)

Dest. IP Address: The destination addresses or ranges of addresses to which this packet filter rule applies. (Address 0.0.0.0 is equivalent any)

Schedule: Select everyday (always) or the day(s) of the week to apply the rule. Enter the start and end times in the hour-minute format to apply the rule.

For example, if you want to ban all of the protocols from the IP (e.g.: 200.1.1.1) to access the all PCs (e.g.: 192.168.0.2 ~ 192.168.0.50) in the LAN, key in the parameter as:

Protocol: ANY

Direction: INBOUND (INBOUND is from WAN)

Action: DENY

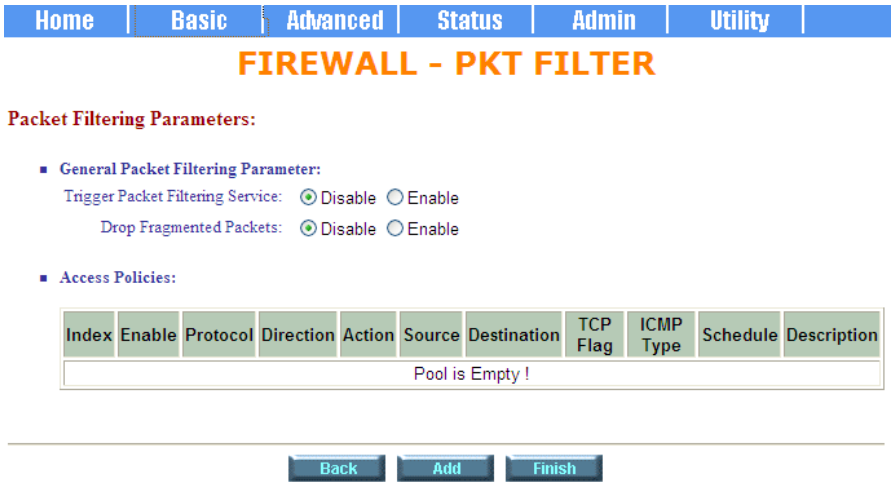
Description: Hacker

Src. IP Address: 200.1.1.1

Dest. IP Address: 192.168.0.2-192.168.0.50

Schedule: You can set always or any time range which you want

Press OK to finish.



The screen will prompt the configured parameters.

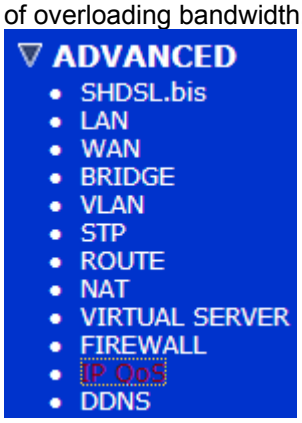
Check Enable on Trigger Packet Filtering Service item, to activate the packet filtering service.

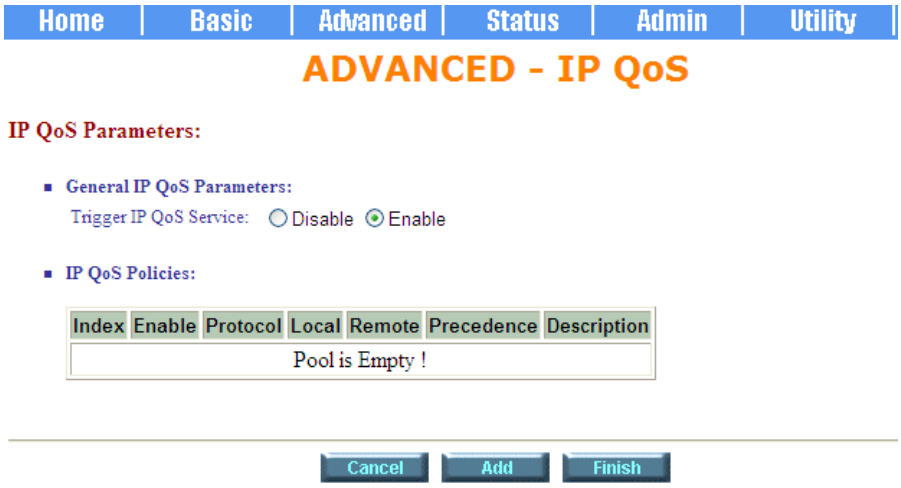
Check Enable on Drop Fragmented Packets item, to activate the drop fragmented packets operation.

You can modify or delete the access policies by clicking Modify or Delete command.

4.10 IP QoS

IP QoS is a function to decide the priorities of setting IPs to transfer packets under the situation of overloading bandwidth.





Check Enable at item Trigger IP QoS Service in General IP QoS Parameter, which will turn on this IP QoS function.

Click Add on the bottom of the web page to begin a new entry in IP QoS Policy table.

Description: A brief statement describing this policy

Local IP: type IP address of local host in prioritized session.

Remote IP: type IP address of remote host in prioritized session.

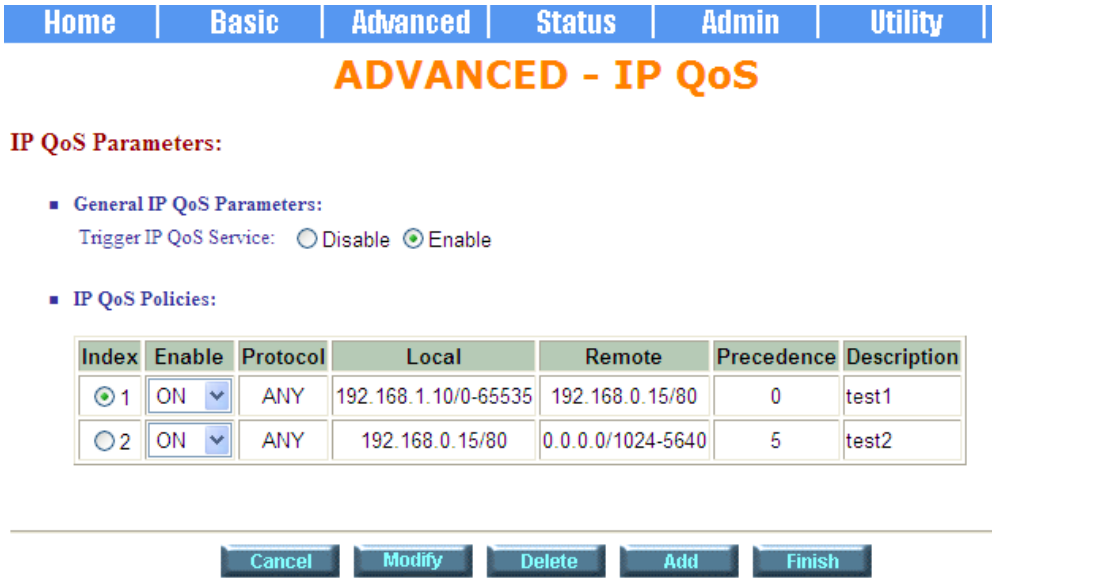
Local Port: type the service port number of local host in prioritized session.

Remote Port: type the service port number of remote host in prioritized session.

Protocol: identify the transportation layer protocol type you want to prioritize, e.g. **TCP** or **UDP**. The default is **ANY**.

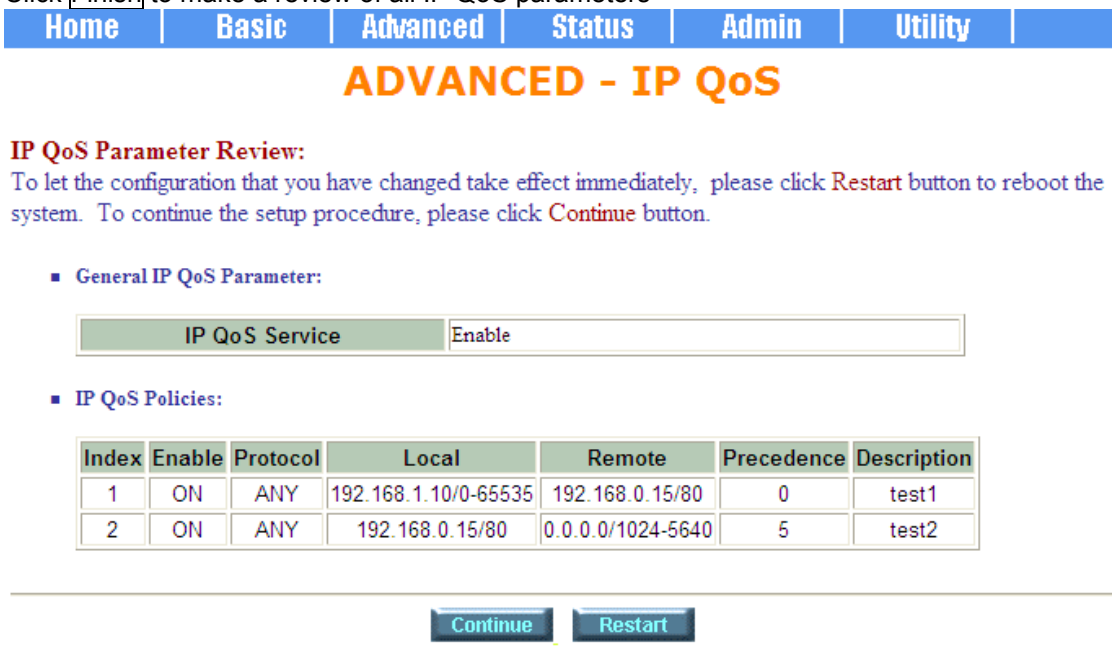
Precedence: type the session's prioritized level you classify, "**0**" is lowest priority, "**5**" is highest priority.

Click OK when all parameters are finished.



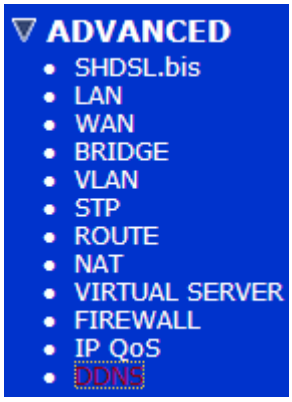
You can modify or delete the policies by clicking Modify or Delete command.

Click Finish to make a review of all IP QoS parameters



To immediately take effect the IP QoS configuration you have changed, please click Restart button to reboot the system. To continue the setup procedure, please click Continue button.

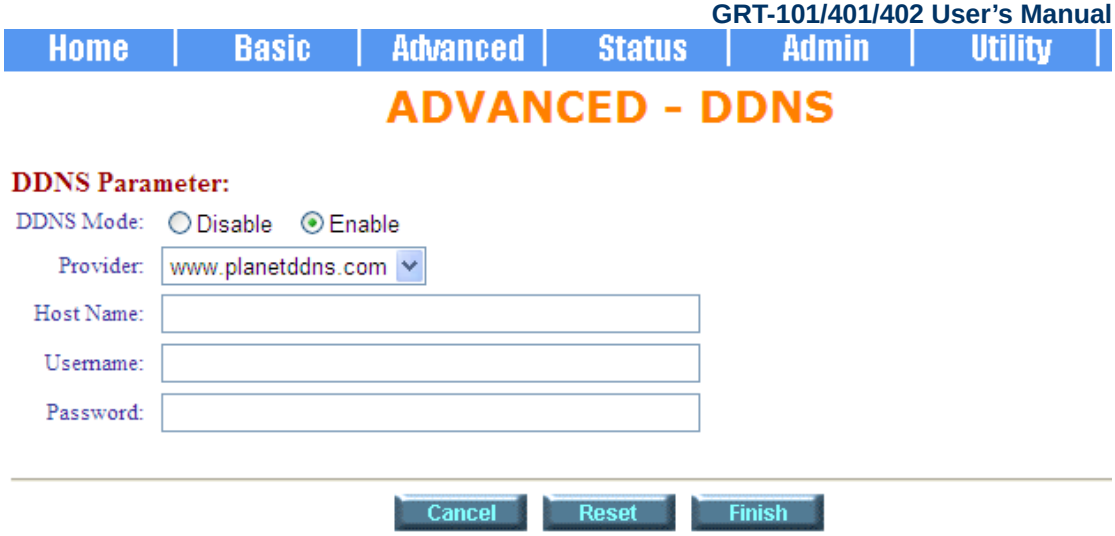
4.11 DDNS



Stands for Dynamic Domain Name Server

The device supports DDNS that it's free for PLANET's customers.

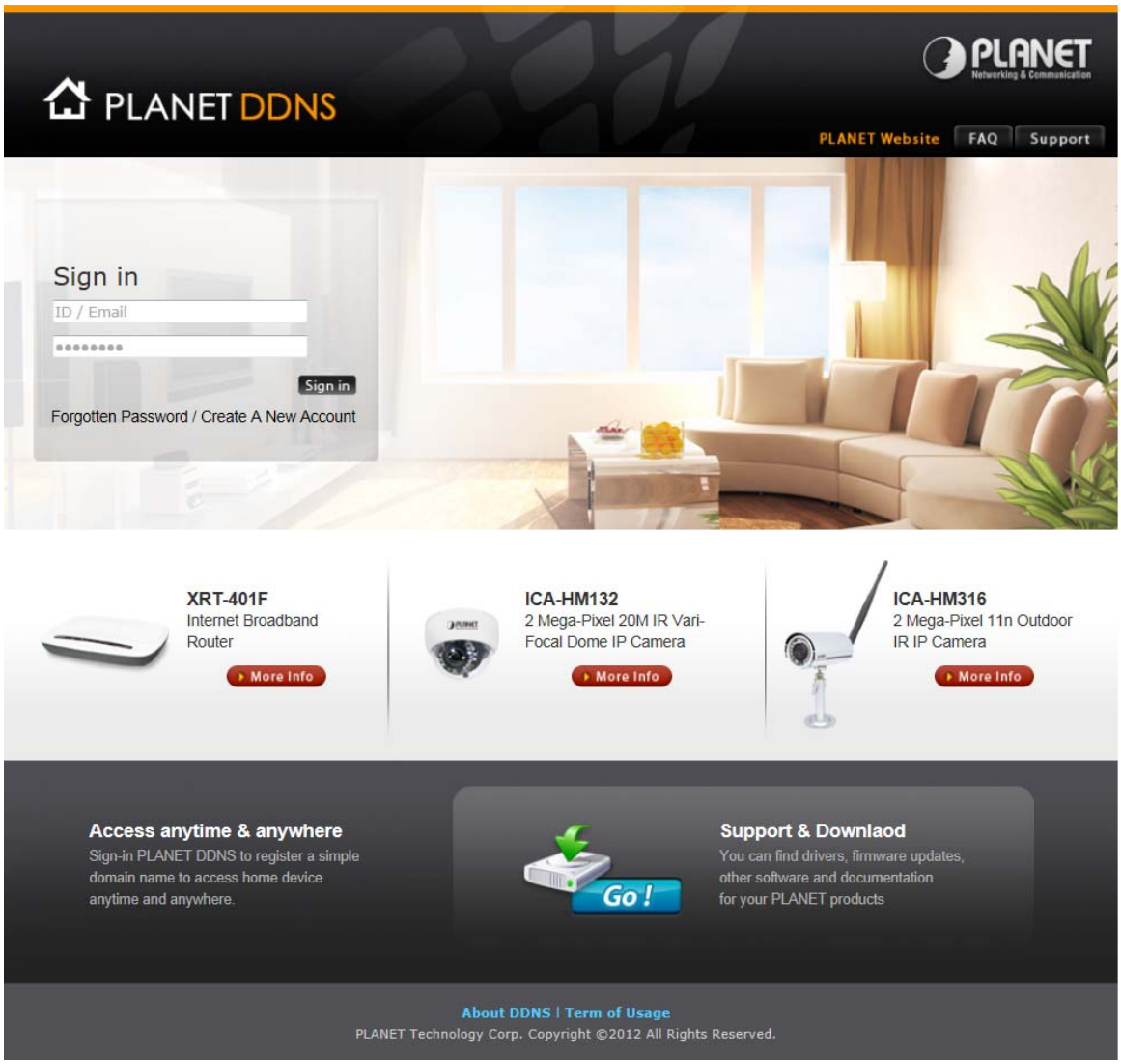
Check enable to enable this function.



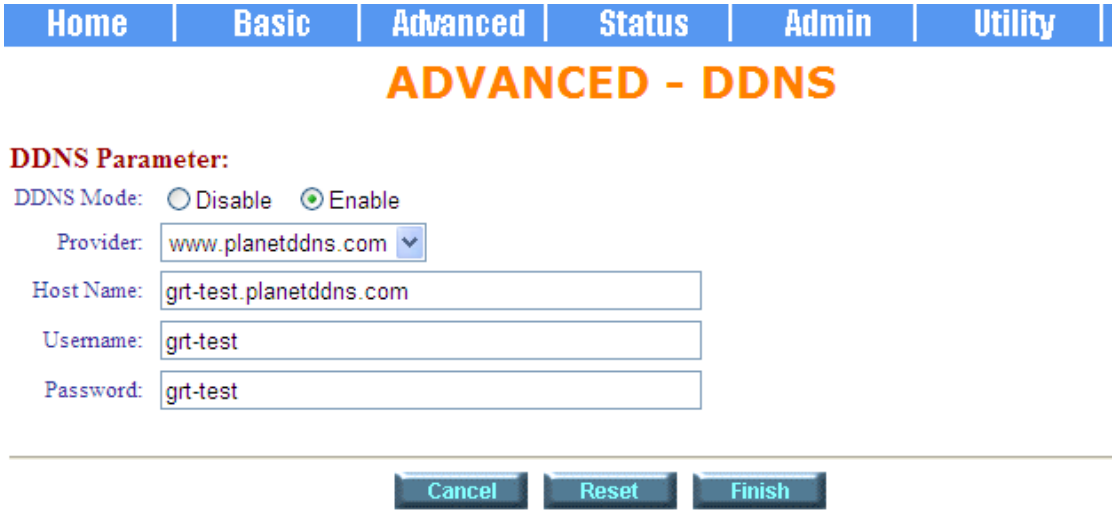
Step 1: Enable DDNS option through accessing web page of GRT series.

Step 2: Select on DDNS server provide, and register an account if you have not used yet.

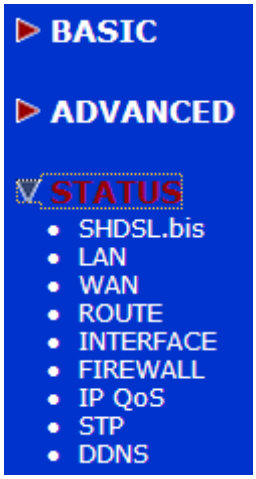
Let's take dyndns.org as an example. Register an account in http://planetddns.com



After adding new account, fill in the information below.



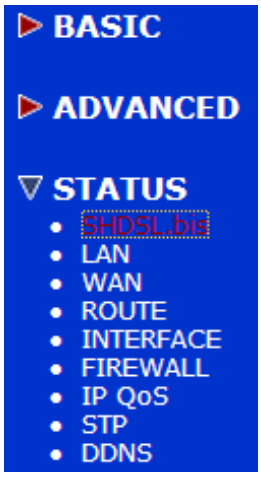
Chapter 5 Status

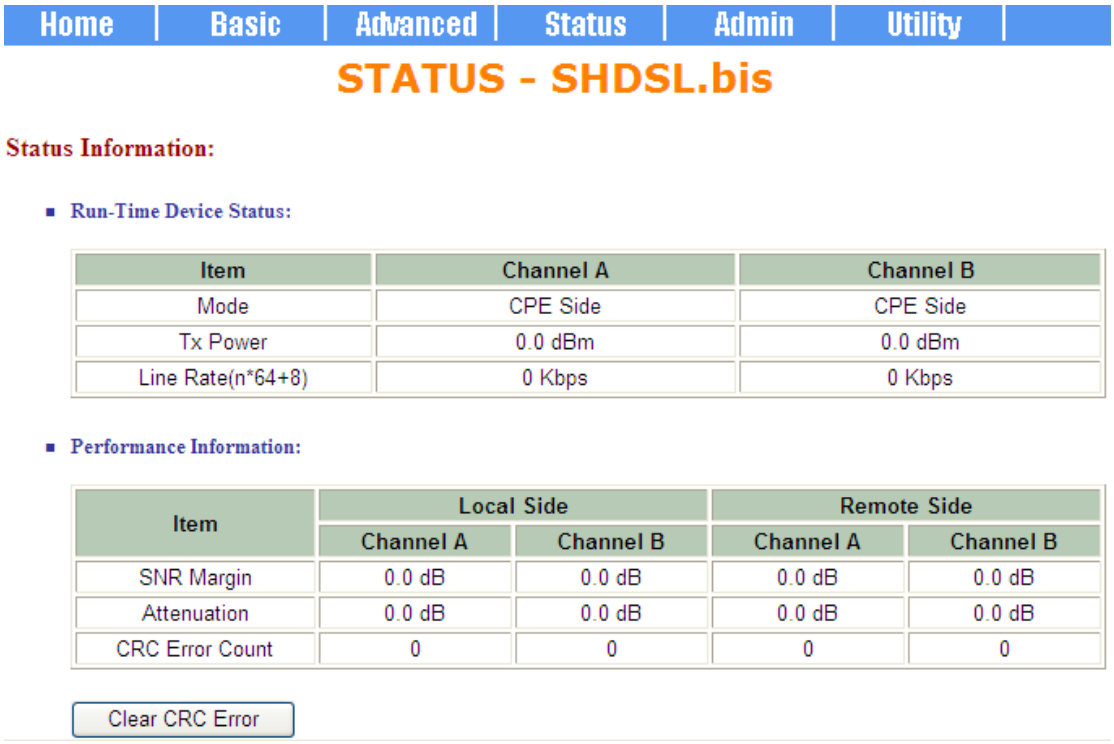


On STATUS item, you can monitor the following:

SHDSL.bis	Mode, Line rate and Performance information including SNR margin, atteunation and CRC error count.
LAN	IP type, MAC address, IP address, Subnet mask and DHCP client table: Type, IP address and MAC address.
WAN	WAN interface information. 8 WAN interface including IP address, Subnet Mask, VPI/VCI, Encapsulation, Protocol and Flag.
ROUTE	IP routing table including Flags, Destination IP/Netmask.Gateway, Interface and Portname.
INTERFACE	LAN and WAN statistics information.
FIREWALL	Current DoS protection status and dropped packets statistics.
IP QoS	Show IP QoS statistics on LAN interface
STP	STP information include Bridge parameter and Ports Parameter
DDNS	Show status of PLANET DDNS

5.1 SHDSL.bis





The status information shows this is a 4-wire model which has both channel A and B. If the router is connected to a remote side, it can also show the performance information of remote side.

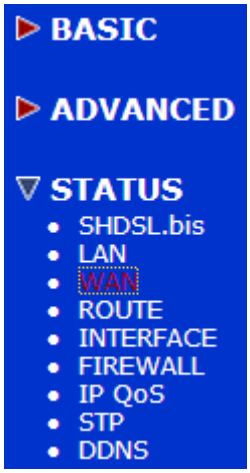
If the router is 2-wire model, you will not see any information on channel B.

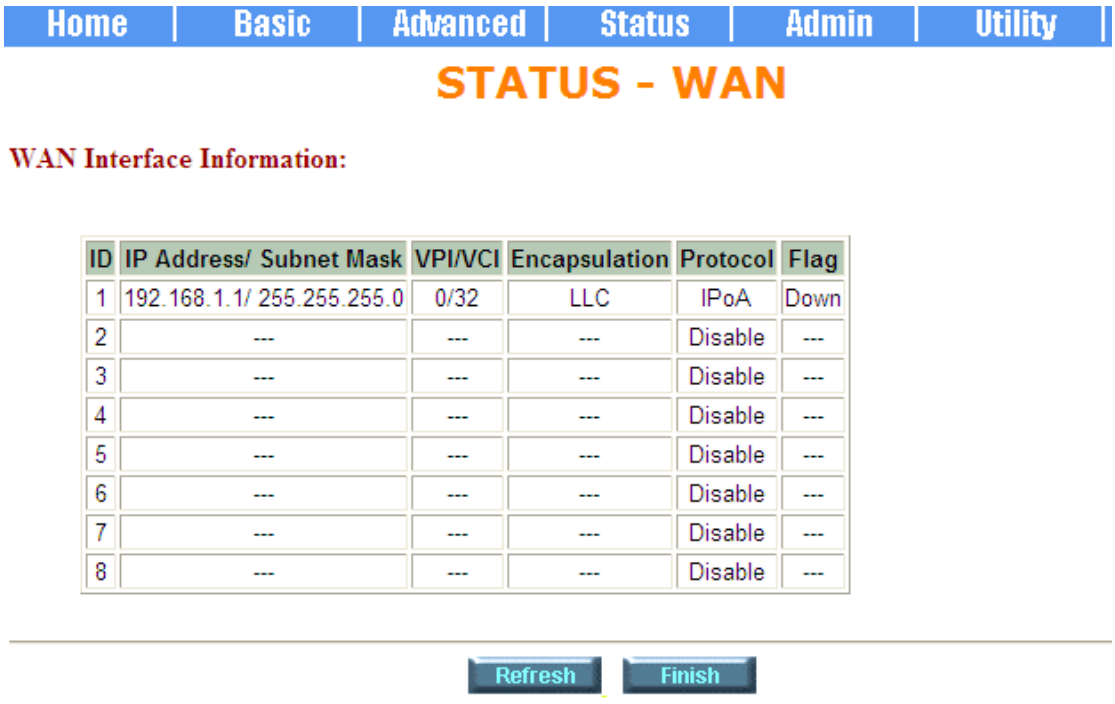
Click Clear CRC Error to clear the CRC error count.

5.2 LAN

This information shows the LAN interface status and DHCP client table.

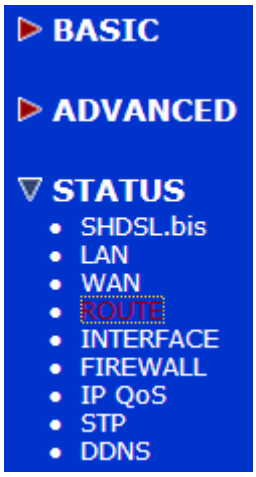
5.3 WAN



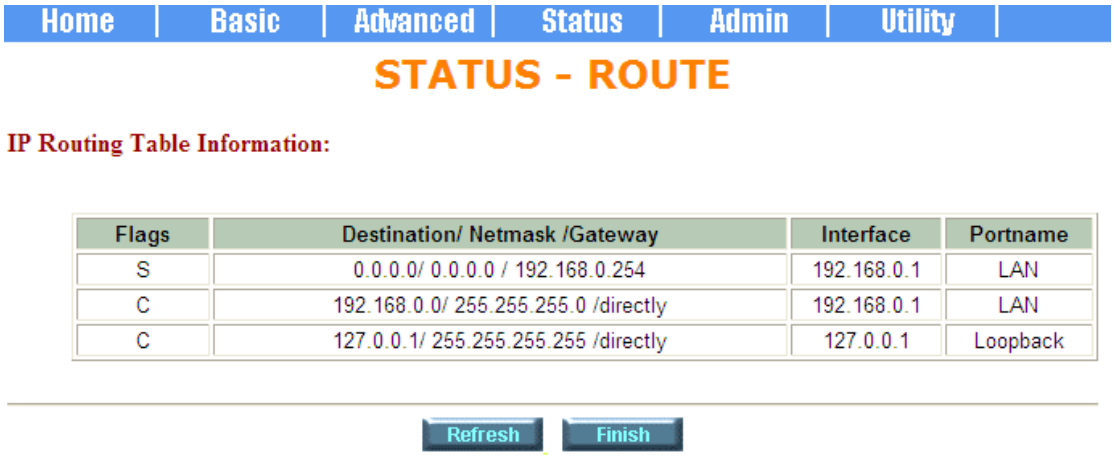


This information shows the status of all eight WAN interfaces.

5.4 ROUTE

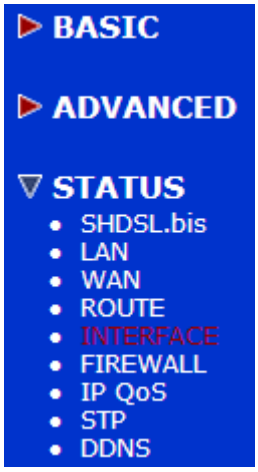


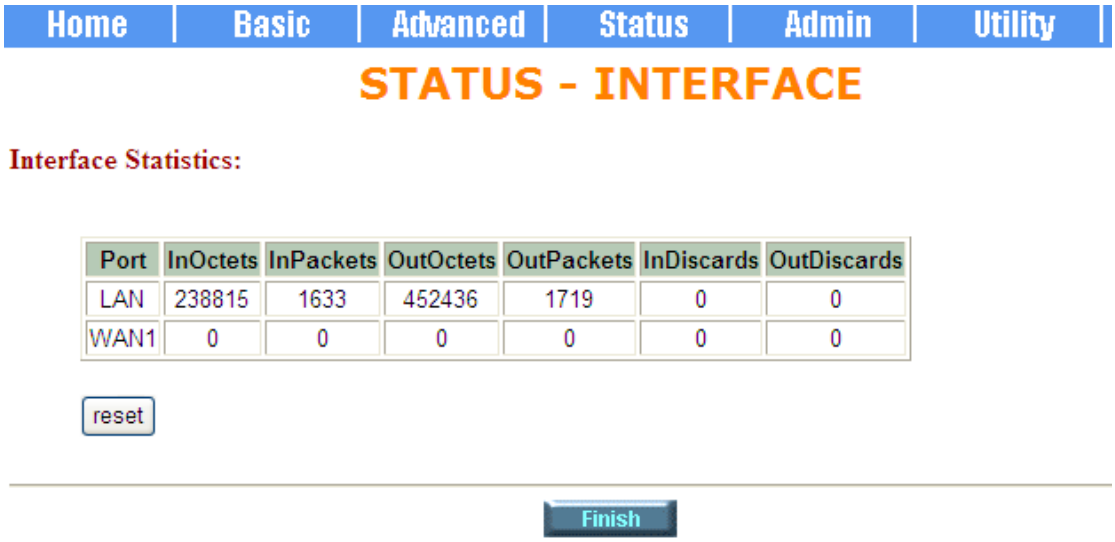
Routing tables contain a list of IP addresses. Each IP address identifies a remote router (or other network gateway) that the local router is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specify the destination IP address ranges that remote device will accept.



This information shows the IP routing table.

5.5 INTERFACE





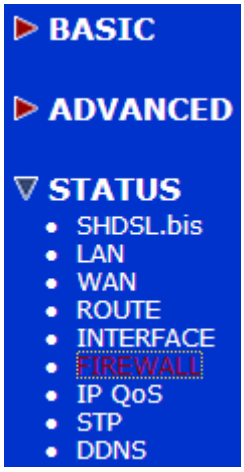
This table shows the interface statistics.

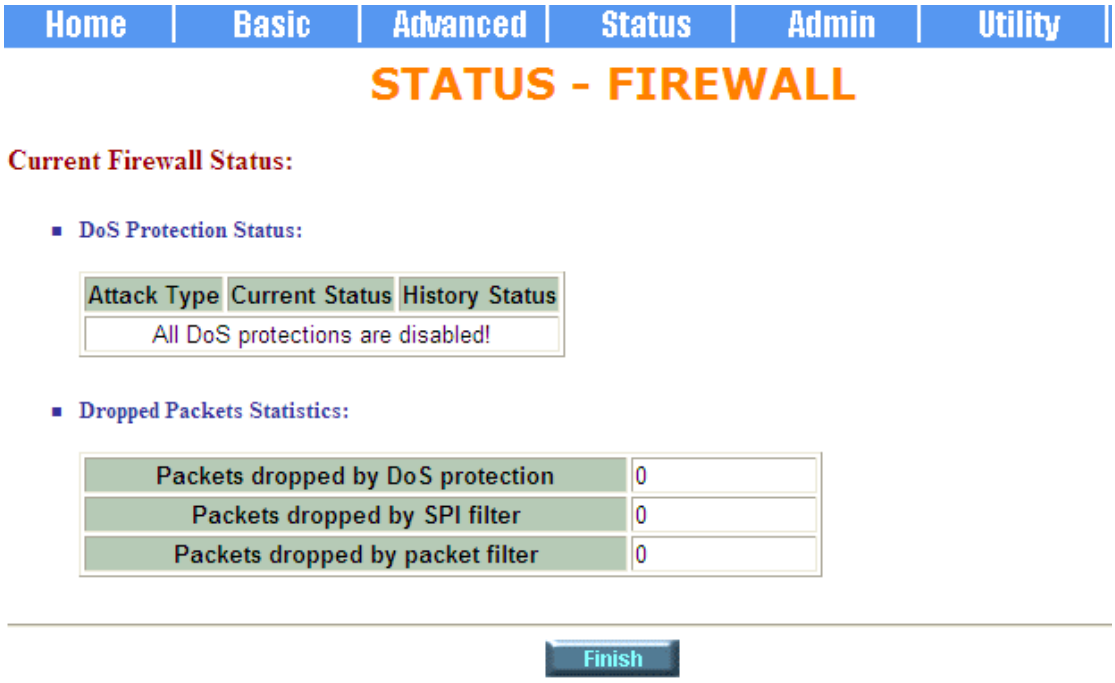
Octet is a group of 8 bits, often referred to as a byte.

Packet is a formatted block of data carried by a packet mode computer networks, often referred to the IP packet.

InOctets	The field shows the number of received bytes on this port
InPactets	The field shows the number of received packets on this port
OutOctets	The field shows the number of transmitted bytes on this port
OutPactets	The field shows the number of transmitted packets on this port
InDiscards	The field shows the discarded number of received packets on this port
OutDiscards	The field shows the discarded number of transmitted packets on this port

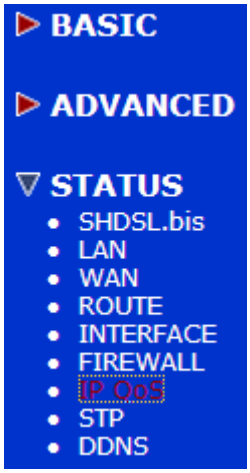
5.6 FIREWALL

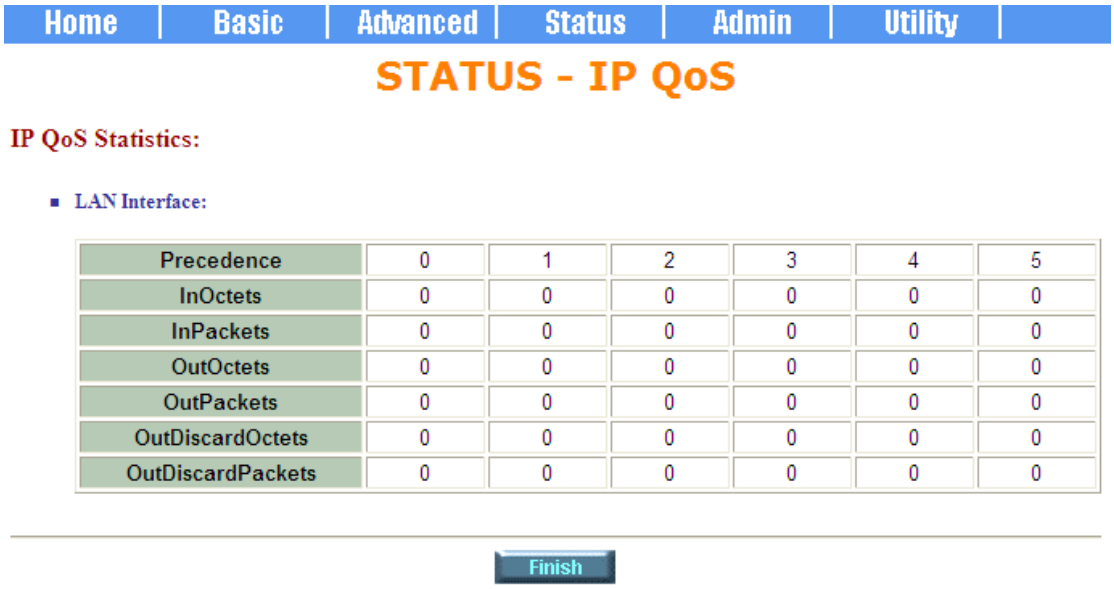




This information shows firewall status: DoS protection and dropped packets statistics.

5.7 IP QOS





This information shows IP QoS statistics.

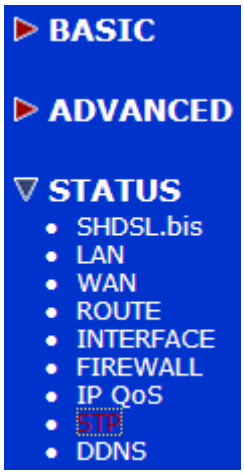
Octet is a group of 8 bits, often referred to as a byte.

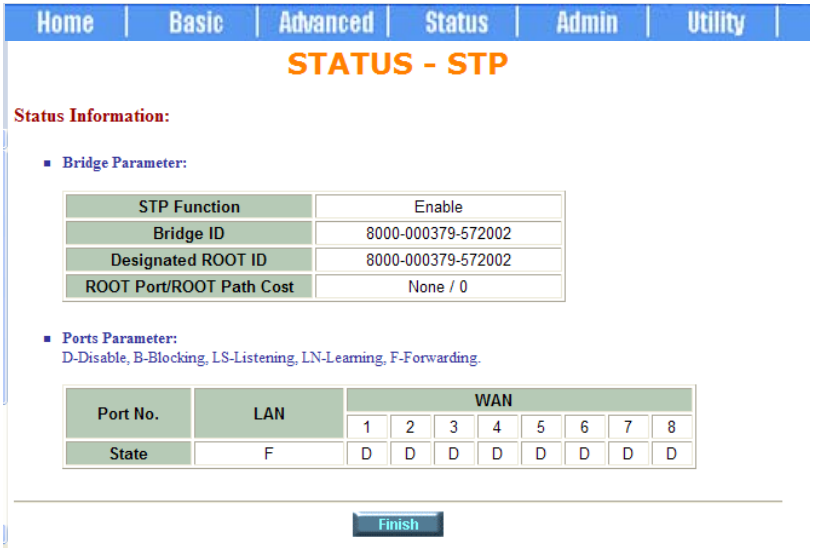
Packet is a formatted block of data carried by a packet mode computer networks, often referred to the IP packet.

InOctets	The field shows the number of received bytes on this port
InPactets	The field shows the number of received packets on this port
OutOctets	The field shows the number of transmitted bytes on this port
OutPactets	The field shows the number of transmitted packets on this port
OutDiscardsOctets	The field shows the discarded number of transmitted bytes on this port

OutDiscardsPackets	The field shows the discarded number of transmitted packets on this port

5.8 STP





This information shows the STP parameter:

The bridge parameters have:

Bridge ID: The bridge ID of a configuration message is an 8-byte field. The six low order bytes are the MAC address of the switch. The high order two-byte (unsigned 16-bit integer) field is the bridge priority number.

Designated Root ID: The unique Bridge Identifier of the Bridge assumed to be the Root, this parameter is used as the value of the Root Identifier parameter in all CBPDUs transmitted by the Bridge.

Root Port: Identifies the Port through which the path to the Root is established, and is not

significant when the Bridge is the Root and is set to zero. It is the Port Identifier of the Port that offers the lowest Cost Path to the Root

Root Path Cost: The Cost of the Path to the Root from this Bridge, this is equal to the sum of the values of the Designated Cost and Path Cost parameters held for the Root Port. When the Bridge is the Root, this parameter is zero.

The ports parameters have:

Learning: This is when the modem creates a switching table that will map MAC addresses to port number.

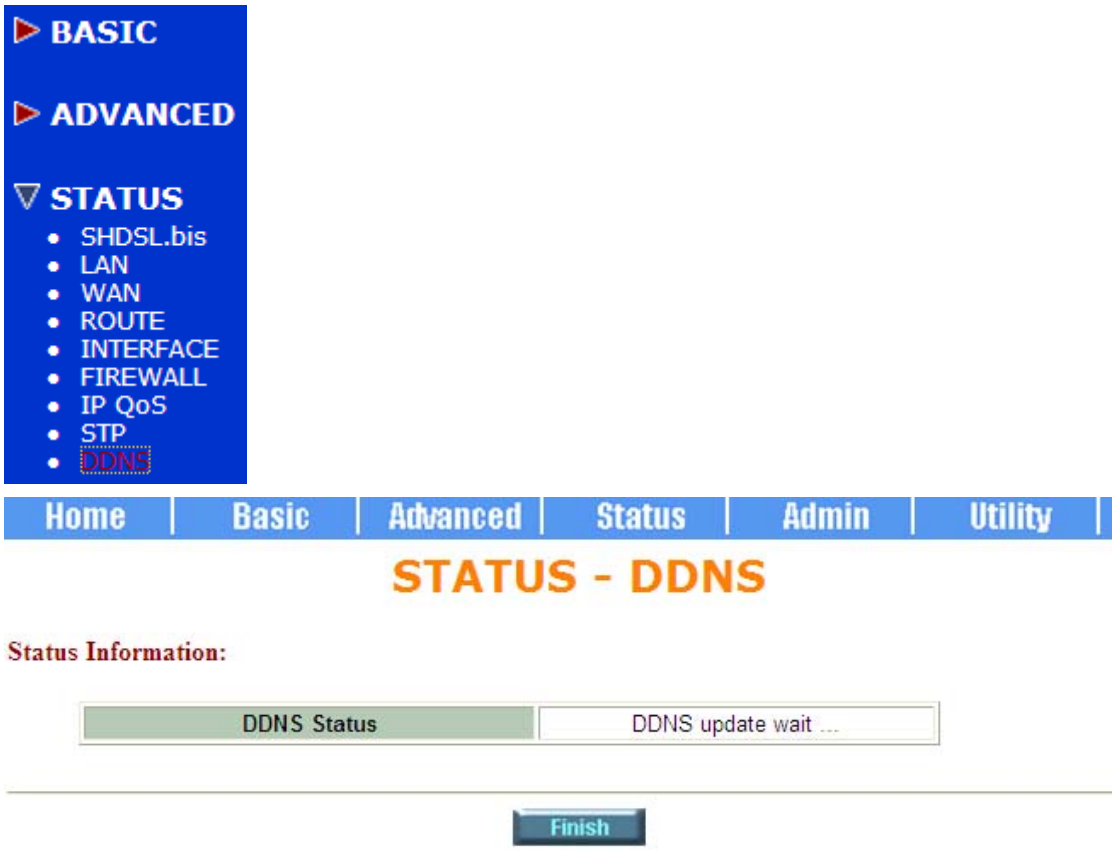
Listening: This is when the modem processes BPDU's that allow it to determine the network topology.

Forwarding: When a port receives or sends data. In other words, this is operating normally.

Disabled: This is when the network administrator has disabled the port.

Blocking: this means the port was blocked to stop a looping condition.

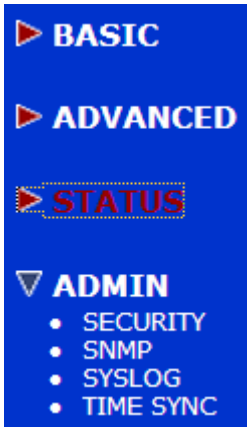
5.9 DDNS



This information shows DDNS statistics.

Chapter 6 Administration

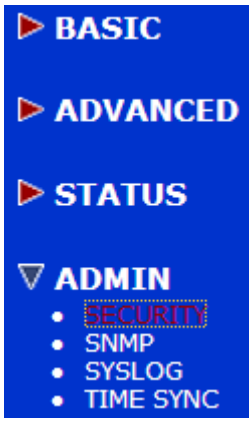
This session introduces security and simple network management protocol (SNMP) and time synchronous.



6.1 Security

For system secutiry, suggest to change the default user name and password in the first setup otherwise unauthorized persons can access the router and change the parameters.
There are three ways to configure the router, Web browser, telnet and serial console.

Press Security to set up the parameters.



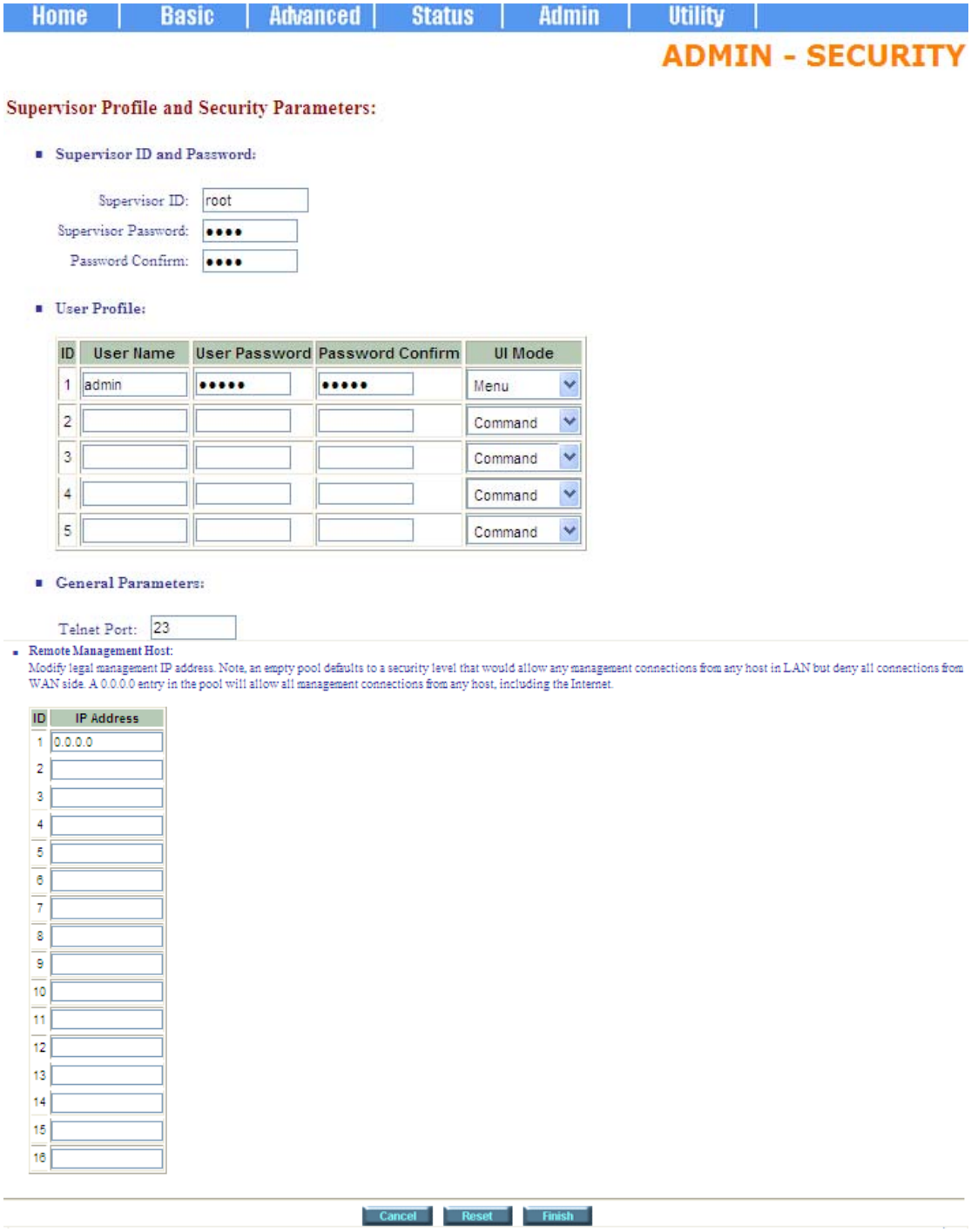
For greater security, change the Supervisor ID and password for the router. If you don't set them, all users on your network can be able to access the router using the default Supervisor IP and Supervisor Password is "***root***".

You can authorize five legal users to access the router via telnet or console only. There are two UI modes: **menu driven mode** and **line command mode** to configure the router. There are two UI modes, menu and command mode for telnet or console mode to set up the Router. The Menu means menu driven interface mode and Command means line command mode. We will

not discuss command mode in this manual.

The default user name and password are *"**admin**"*.

Legal address pool will set up the legal IP addresses from which authorized person can configure the router. This is the more secure function for network administrator to set up the legal address of configuration.



This is the default supervisor ID and password is "***root***". It is highly recommended that you change this for security purpose.

Supervisor ID: Type the new ID

Supervisor Password: Type the existing password ("***root***" is the default password when shipped)

Password Confirm: Retype your new password for confirmation.

Telnet Port: For Telnet, you may change the default service port by typing the new port number. If you change the default port number then you will have to let user who wish to use the service know the new port number. The default value is 23.

On trust host list, configured 0.0.0.0 will allow all hosts on Internet or LAN to access the router.

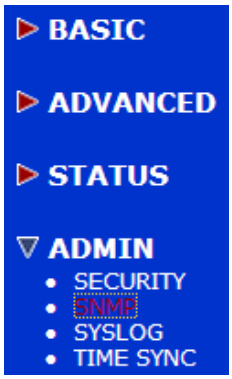
Leaving blank of trust host list will cause blocking all PC from WAN to access the router. On the other hand, only PC in LAN can access the router.

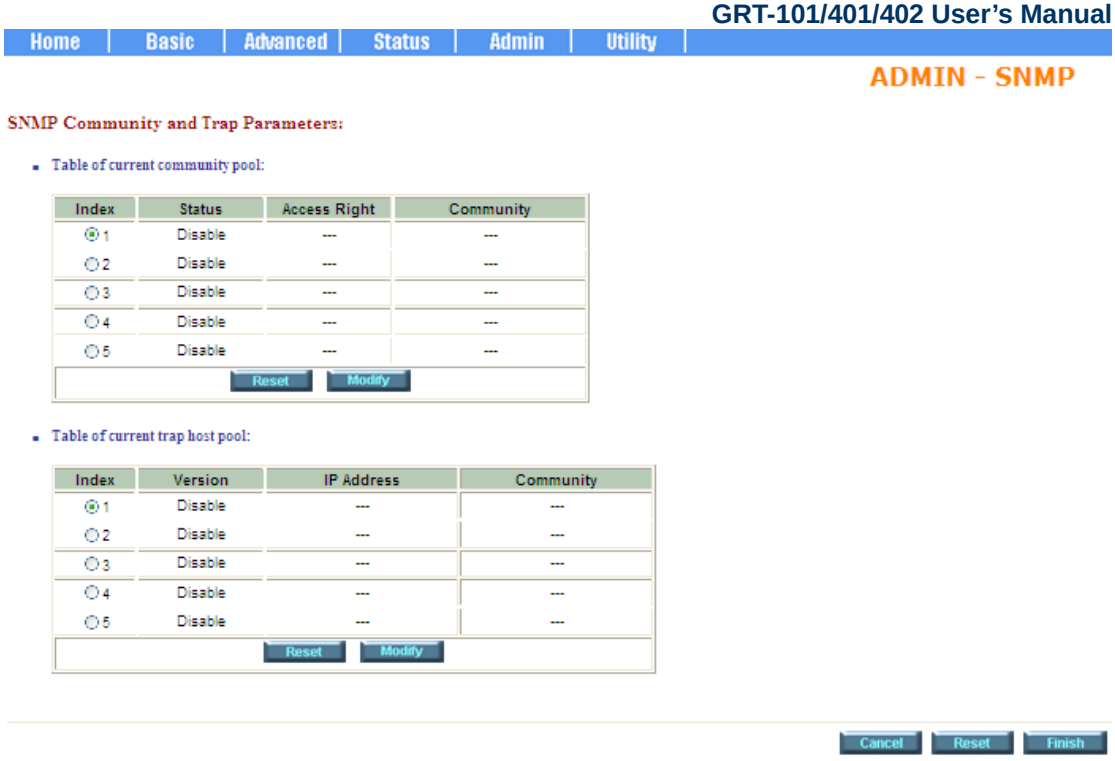
If you type the exact IP address in the field, only the host on this listing can access to the router.
Click Finish to finish the setting.

The browser will prompt the all configured parameters and check it before writing into NVRAM. Press Restart to restart the gateway working with the new parameters and press Continue to set up other parameters.

6.2 SNMP

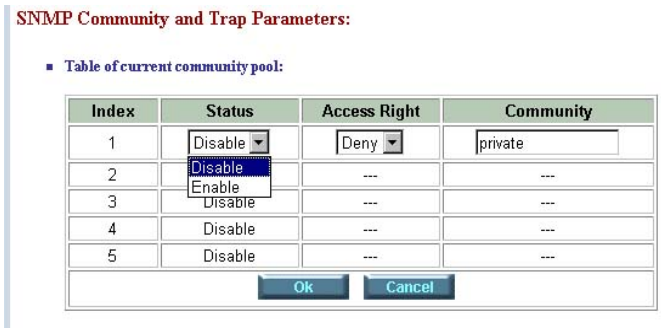
Simple Network Management Protocol (SNMP) provides for the exchange of messages between a network management client and a network management agent for remote management of network nodes. These messages contain requests to get and set variables that exist in network nodes in order to obtain statistics, set configuration parameters, and monitor network events. SNMP communications can occur over the LAN or WAN connection. The router can generate SNMP traps to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security. This router support MIB I and MIB II.
Click SNMP to configure the parameters.



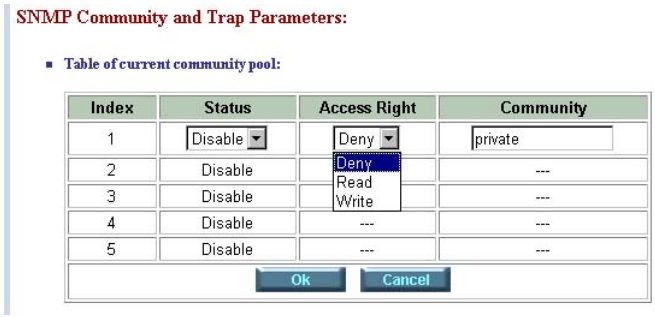


6.2.1 Community pool

Press Modify to modify the community pool. You can set up the access authority.



SNMP **Status**: Enable



Access Right: Deny for deny all access

Read for access read only

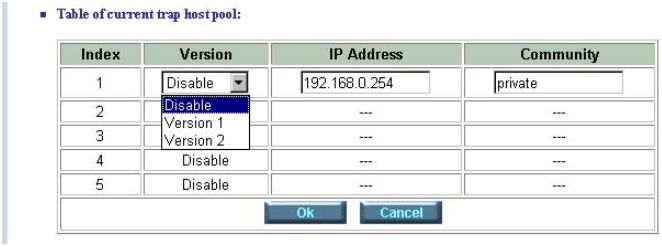
Write for access read and write.

Community: it serves as password for access right.

After configuring the community pool, press OK.

6.2.2 Trap host pool

SNMP trap is an informational message sent from an SNMP agent to a manager. Click Modify to modify the trap host pool.



Version: select version for trap host. (Version 1 is for SNMPv1; Version 2 for SNMPv2).

IP Address: type the trap host IP address

Community: type the community password. The community is set up in community pool.

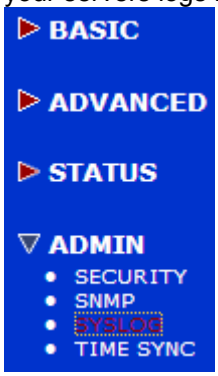
Press OK to finish the setup.

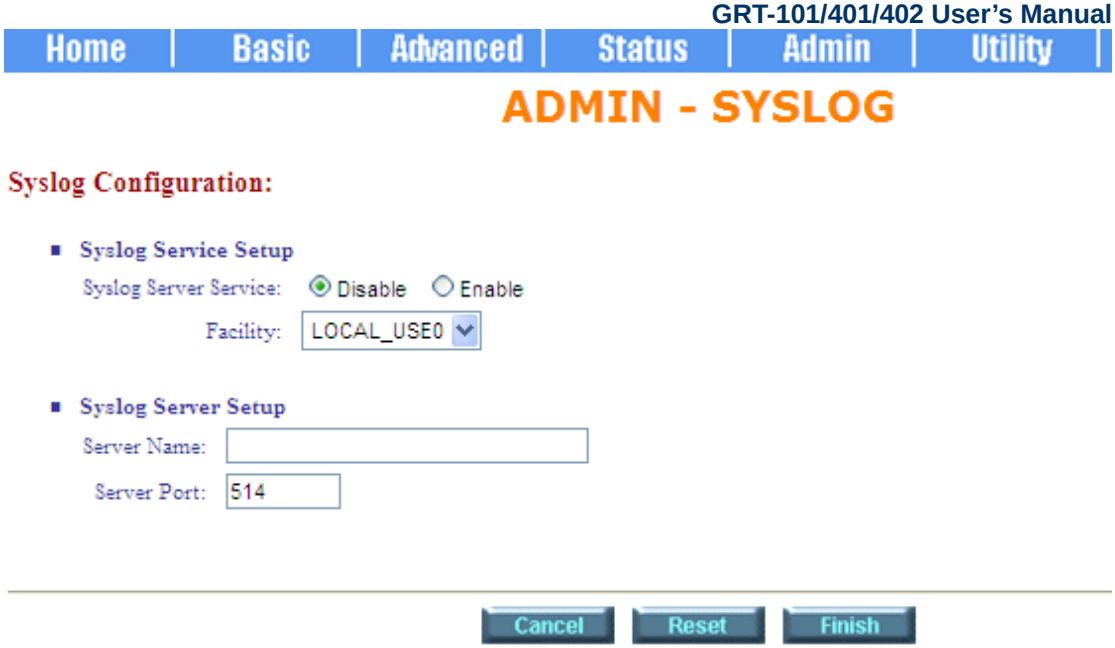
The browser will prompt the configured parameters and check it before writing into NVRAM.

Press Restart to restart the gateway working with the new parameters and press Continue to set up other parameters.

6.3 SYSLOG

Syslog is a standard method of centralizing various logs. You can use a syslog server to store your servers logs in a remote location for later perusal or long-term storage.





To send logs to the LOG server, you must configure the other servers from your network to send logs to that server.

Syslog Service setup

1. Check the enable item of **Syslog Server Service** to turn on syslog service.
2. Select the syslog server facility. The log facility allows you to send logs to different files in the syslog server.

Syslog Server Setup

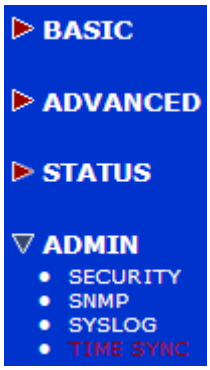
3. Specify a server name to which all syslog messages will be sent.
4. Specify a UDP port number to which the syslog server is listening. The default value is 514. Make sure this is not blocked from your firewall.

Press Finish to finish the setup. The browser will prompt the configured parameters and check it before writing into NVRAM.

6.4 Time Sync

Time synchronization is an essential element for any business that relies on an IT system. The reason for this is that these systems all have clocks that are the source of time for files or operations they handle. Without time synchronization, time on these systems varies with each other or with the correct time and this can cause-, firewall packet filtering schedule processes to fail, security to be compromised, virtual server works in wrong schedule.

Click TIME SYNC

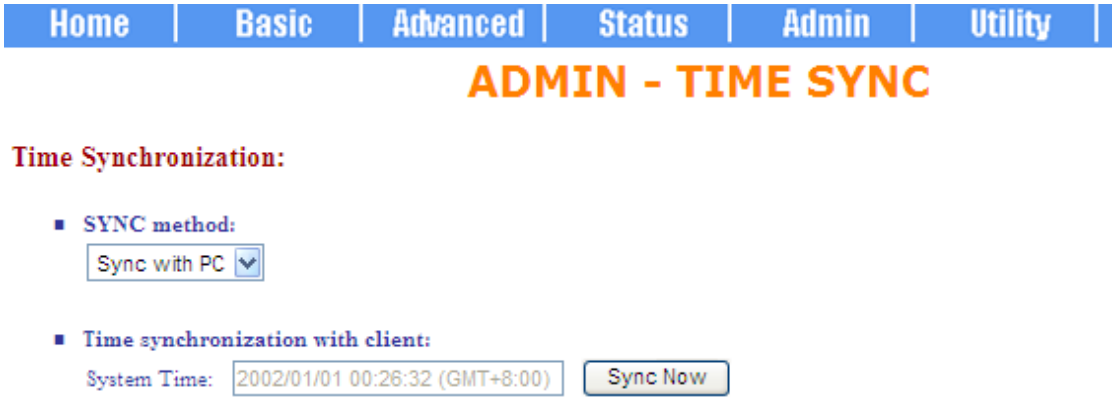


Time synchronization has two methods:

Sync with PC	Synchronization with PC
SNTP v4.0.	Simple Network Time Protocol with Version 4

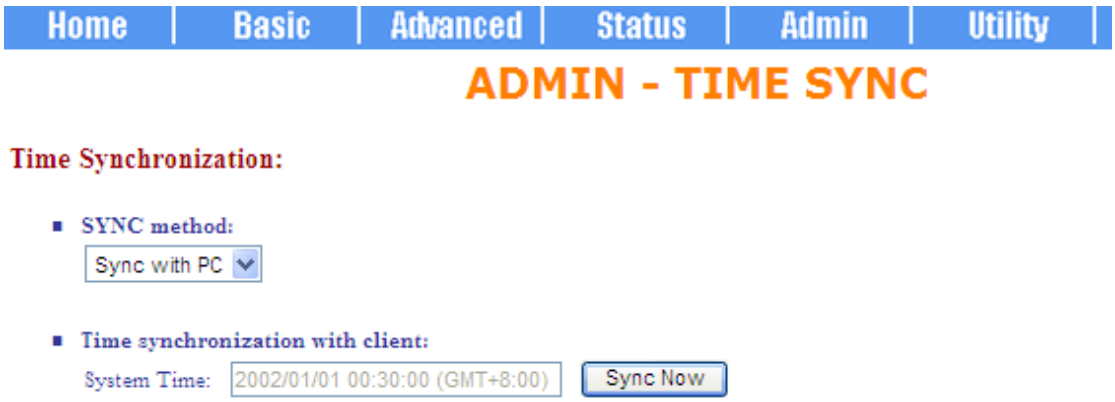
6.4.1 Synchronization with PC

For synchronization with PC, select Sync with PC. The router will synchronize the time with the connecting PC. The function can be supported in both bridge and router modes.



6.4.2 SNTP v4.0

For using the SNTP, select SNTP v4.0.



SNTP is the acronym for Simple Network Time Protocol, which is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. SNTP can be used when the ultimate performance of the full NTP implementation. The function is only supported in router mode.

Service: Enable

Time Server 1, Time Server 2 and Time Server 3: All of the time server around the world can be used but suggest using the time server nearby to your country. You can set up maximum three time server on here.

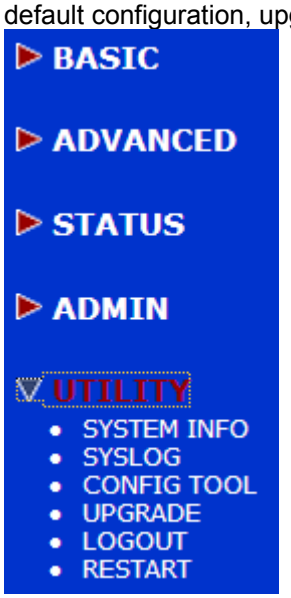
Time Zone: Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.

Update Period: How many times the router can resynchronize to time server. The unit is second.

Press Finish to finish the setup. The browser will prompt the configured parameters and check it before writing into NVRAM.

Chapter 7 Utility

This section will describe the utility of the product including system information, load the factory default configuration, upgrade the firmware logout and restart the gateway.

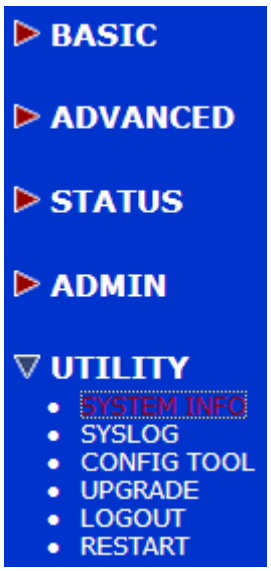


This section will describe the utility of the product including:

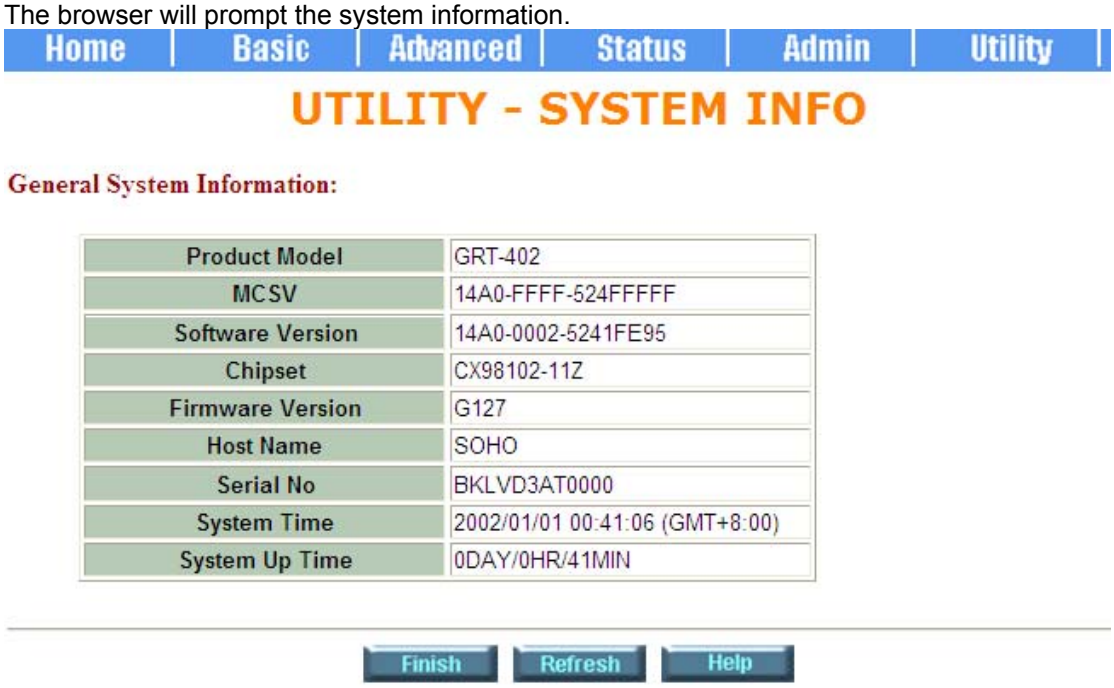
SYSTEM INFO	Show the system information
SYSLOG	Capturing log information
CONFIG TOOL	Load the factory default configuration, restore configuration and backup configuration
UPGRADE	Upgrade the firmware
LOGOUT	Logout the system
RESTART	Restart the router.

7.1 System Info

Click System Info for reviewing the information.



The browser will prompt the system information.



It will display general system information including: MCSV, software version, chipset, firmware version, Host Name, System Time and System Up Time.

MCSV: For internal identification purposes.

Software Version: This is the router's firmware version. Sometimes the technicians need it to troubleshoot problems.

Chipset: This is the SHDSL.bis chipset model name.

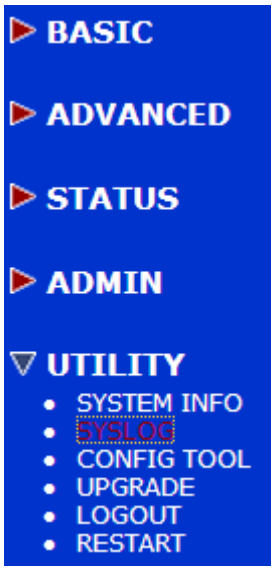
Firmware Version: This is the chipset's firmware version.

Host Name: This is the system name in BASIC Setup. It is for identification purposes.

System Time: This field displays the router's present date and time.

System Up Time: This is the total time that the router has been on.

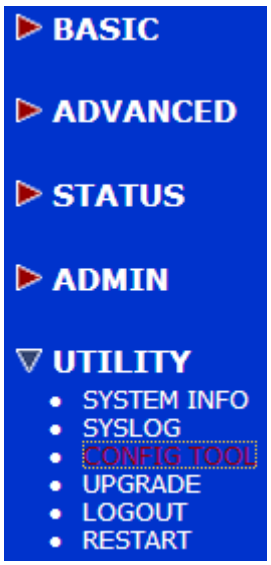
7.2 SYSLOG



SHDSL.bis routers support detailed logging via Syslog function. The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event message. The router can generate a syslog message and send it to a syslog server.

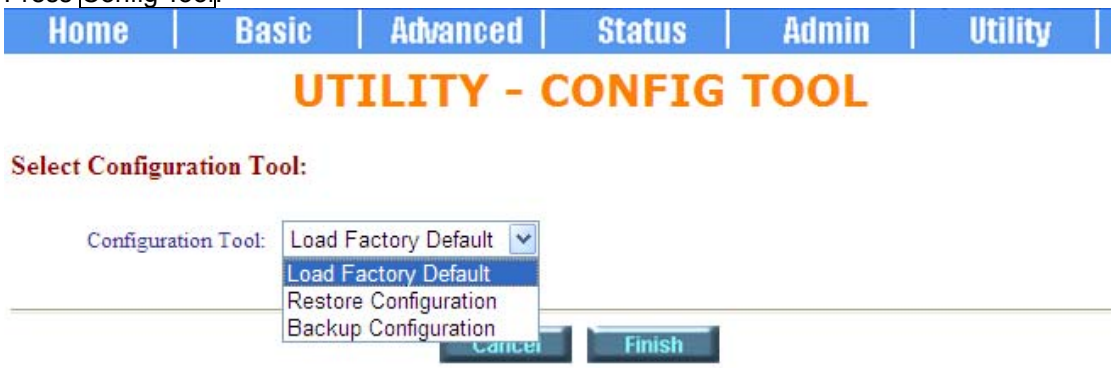
Press SYSLOG to send the syslog messages as shown below:

7.3 Config Tool



This configuration tool has three functions: Load Factory Default, Restore Configuration and Backup Configuration.

Press Config Tool.



Choose the function and then press finish.

7.3.1 Load Factory Default

Load Factory Default: It will load the factory default parameters to the router.

Note	**This action will change all of the settings to factory default value. In other words, you will lose all the existing configured parameters.**

7.3.2 Restore Configuration

Sometimes the configuration could crush accidentally. It will help you to recover the backup configuration easily.

Click Finish after selecting Restore Configuration.

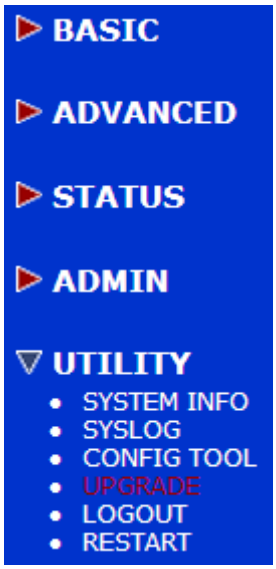
Browse the route of backup file then press Finish. Browse the location of restore file name or enter the name directly. Then press OK. The router will automatically restore the saved configuration.

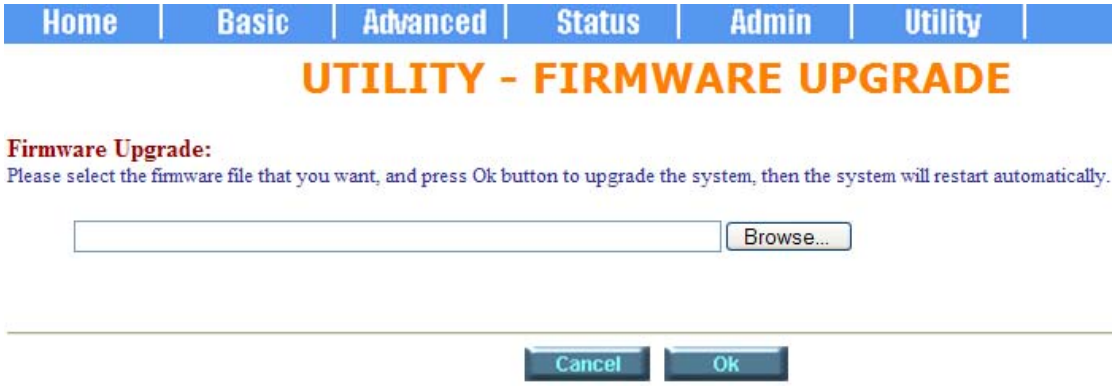
7.3.3 Backup Configuration

After completing the configuration of the router, please use this function to back up your router parameters in the PC. Select the Backup Configuration and then press Finish. Browse the location of backup file name or enter the name directly. Then press OK. The router will automatically back up the configuration. If you don't enter a file name, the system will use the default: *config1.log*

7.4 Upgrade

You can upgrade the gateway using the upgrade function.
Press Upgrade in UTILITY.

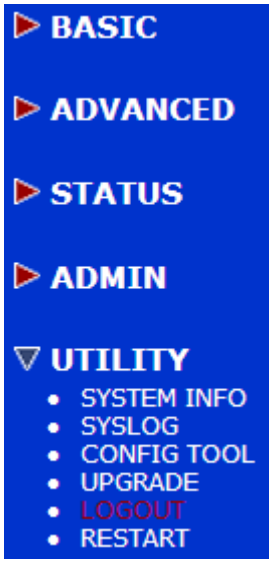




Select the firmware file name by clicking Browse on your PC or NB, and then press OK button to upgrade. The system will reboot automatically after finishing the firmware upgrade operation.

7.5 Logout

To logout the router, press LOGOUT in UTILITY.



To logout system and close window, click the LOGOUT in UTILITY

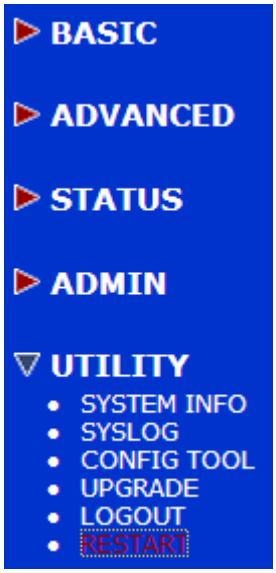
UTILITY - LOGOUT

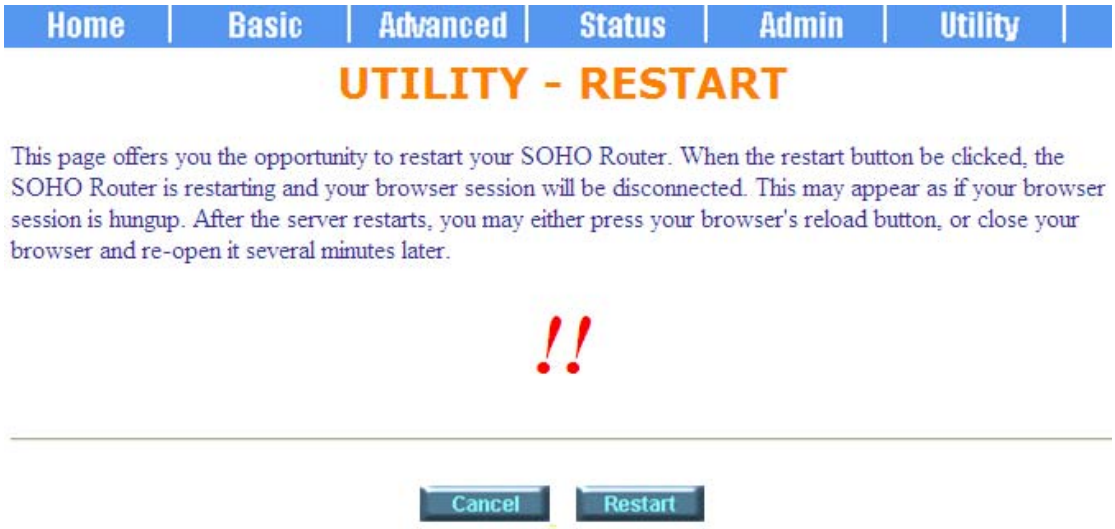
This page offers you the opportunity to quit your SOHO Router. When the YES button be clicked, the SOHO Router is logout and your browser window will be closed.

When clicking the Yes button, the Router will logout and browser window will close.

7.6 Restart

To restart the router, click the RESTART in UTILITY.

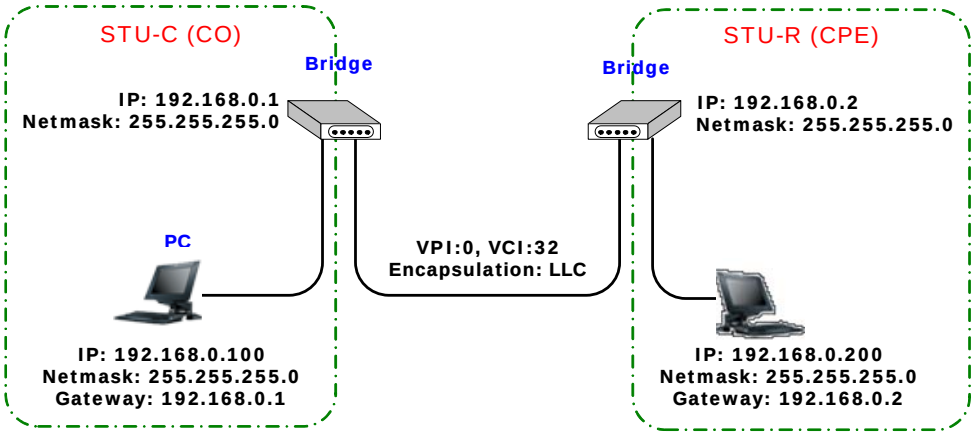




Press Restart to reboot the router.

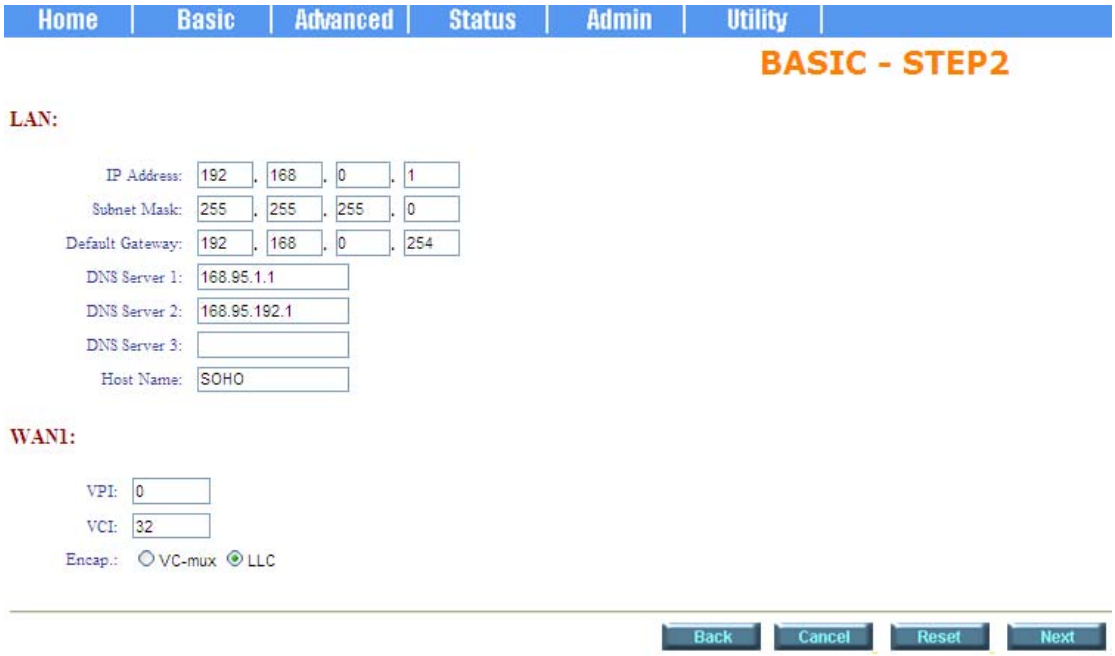
When the restart button is clicked, the router will restart and the browser session will be disconnected. This may appear as if your browser session is hung up. After the router restarts, you may either click the browser's reload button or close the browser and re-open it later.

Chapter 8 . LAN-to-LAN Connection in Bridge Mode



8.1 CO side

Check Bridge and CO Side to set up bridging mode of the Router and then click Next.



Enter **LAN** Parameters

IP: 192.168.0.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

Host Name: SOHO

Enter **WAN1** Parameters

VPI: 0

VCI: 32

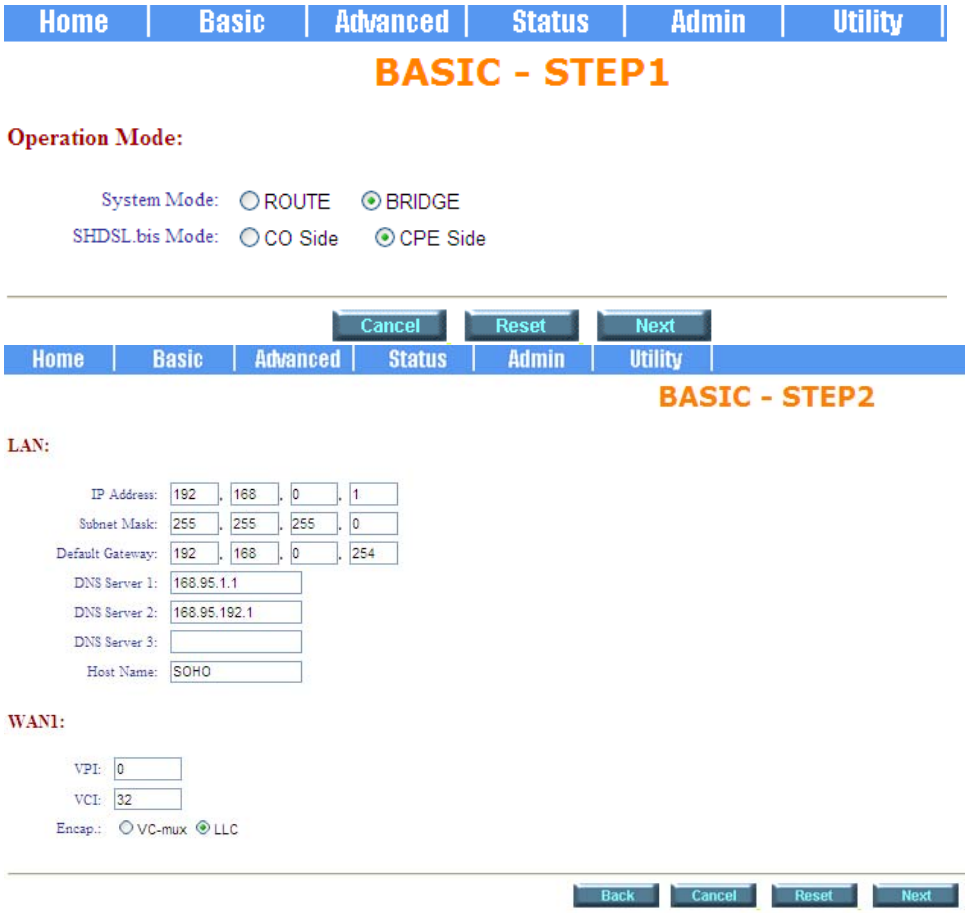
Check LLC

Click Next

The screen will prompt the new configured parameters. Check the parameters and click Restart The router will reboot with the new setting.

8.2 CPE Side

Check Bridge and CO Side to set up Bridge mode of the Router and then click Next.



Enter **LAN** Parameters

IP: 192.168.0.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.2

Host Name: SOHO

Enter **WAN1** Parameters

VPI: 0

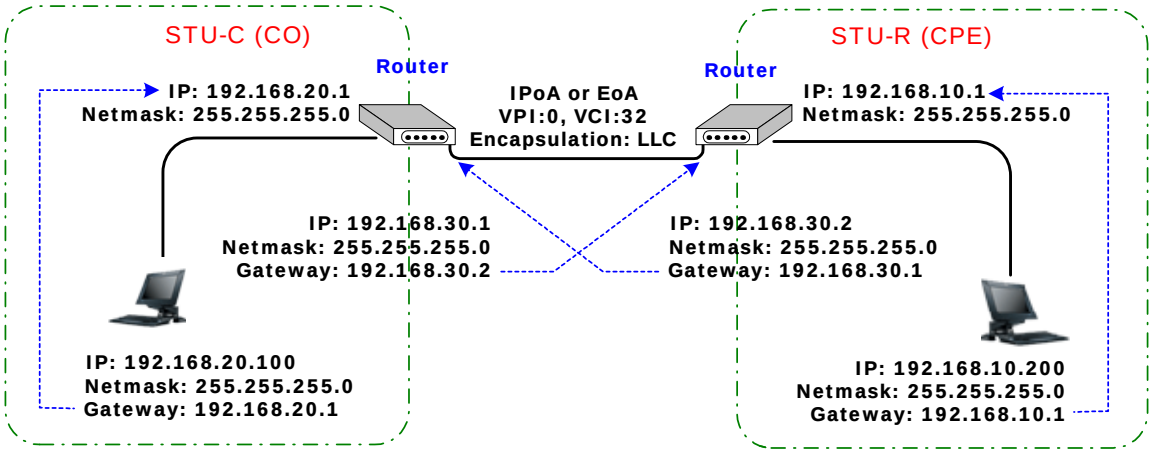
VCI: 32

Check LLC

Click Next

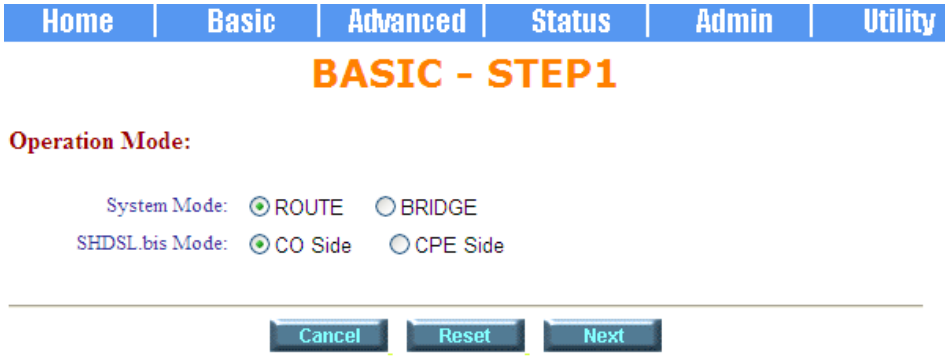
The screen will prompt the new configured parameters. Check the parameters and click Restart The router will reboot with the new setting.

Chapter 9 LAN to LAN Connection in Routing Mode



9.1 CO Side

Check ROUTE and CO Side to set up Routing mode of the Router and then click Next



Type **LAN** parameters:

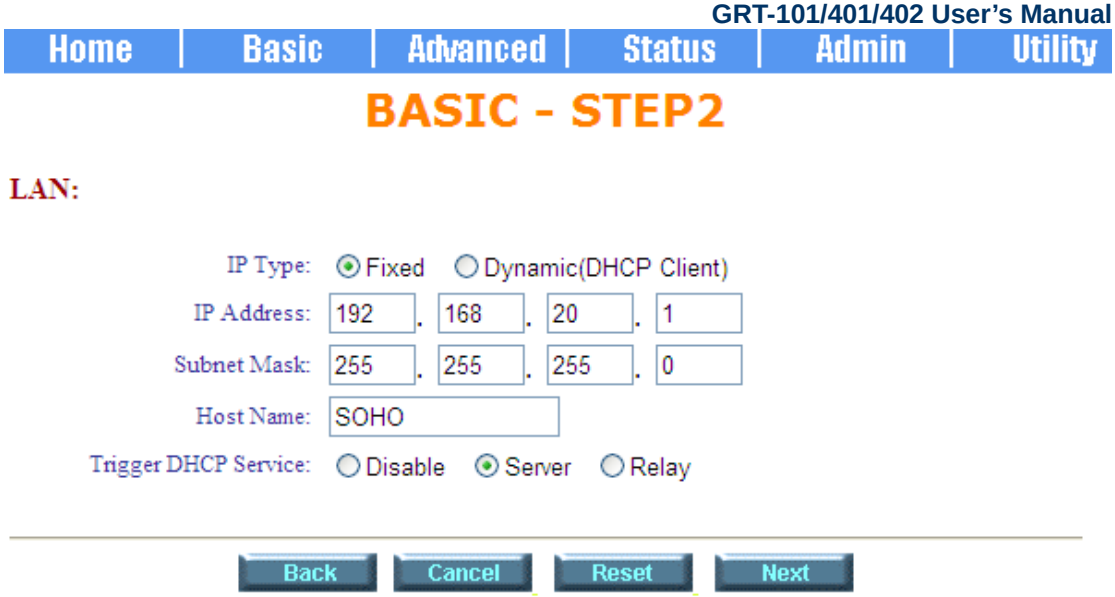
IP Address: 192.168.20.1

Subnet Mask: 255.255.255.0

Host Name: SOHO

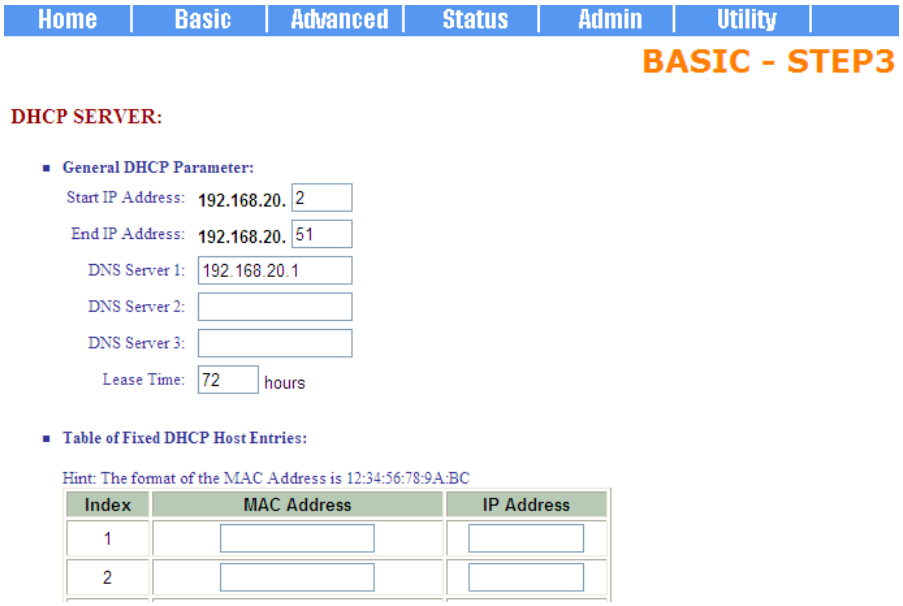
DHCP Service: Disable or Enable

For more **DHCP** service, review the chapter on DHCP Service



The range of DHCP is from 192.168.20.2 to 192.168.20.51.

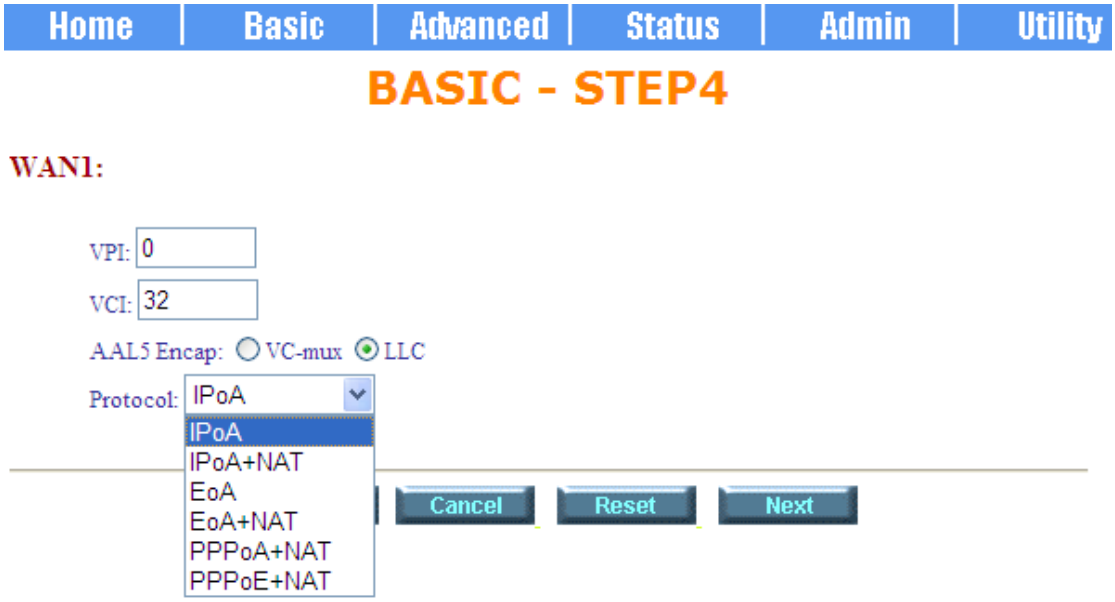
User also can set and fix IP in the table below.



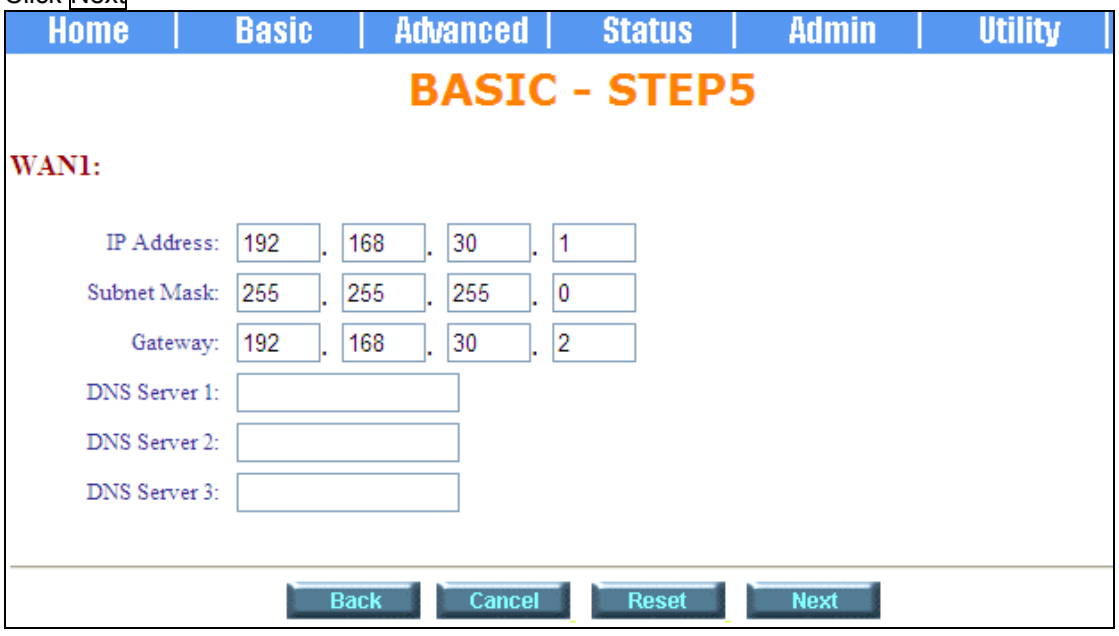
Type the Wan Parameters;
VPI: 0
VCI: 32
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT

Note	The Protocol used in CO and CPE have to be the same.

Click Next to set up the IP parameters.



IP Address: 192.168.30.1
Subnet mask: 255.255.255.0
Gateway: 192.169.30.2
Click Next

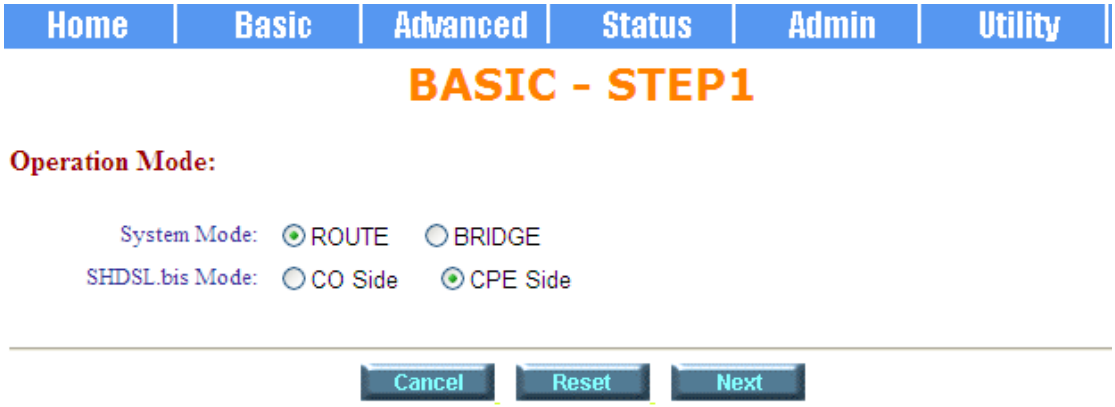


The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

Press Restart to restart the router working with new parameters or press continue to set up another parameter.

9.2 CPE side

Check ROUTE and CPE Side, and then press Next.



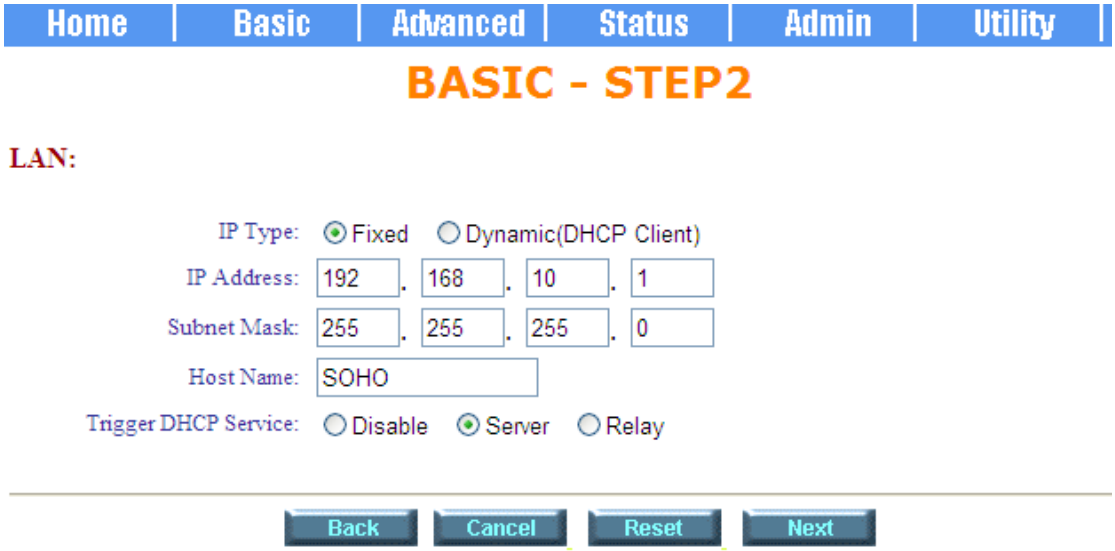
Type LAN parameters:

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

Host Name: SOHO

DHCP Service: Disable or Enable



The range of DHCP is from 192.168.20.2 to 192.168.20.51.

User also can set and fix IP in the table below.

Type the **WAN1** Parameters;

VPI: 0

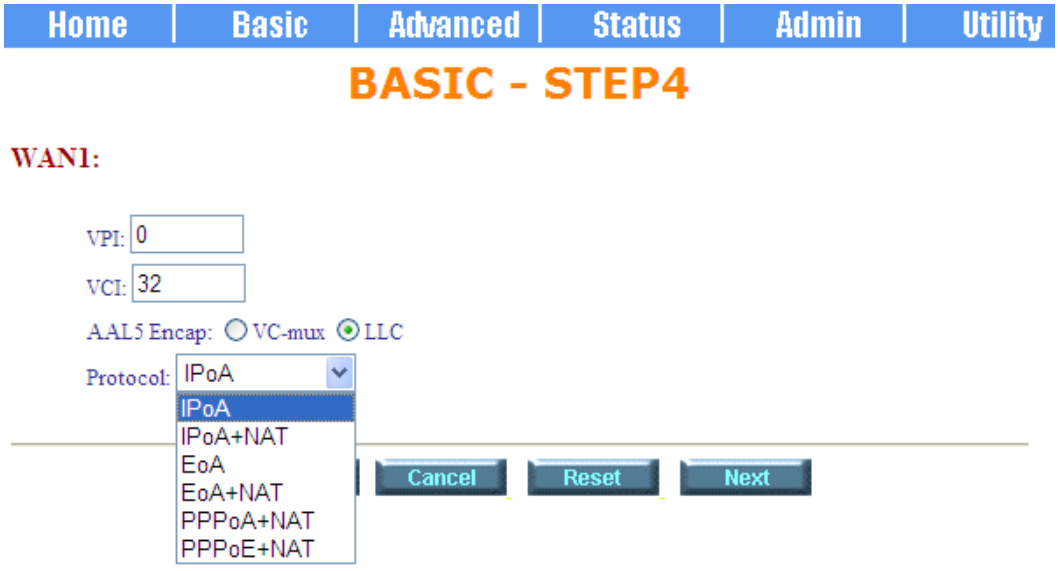
VCI: 32

AAL5 Encap: LLC

Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT

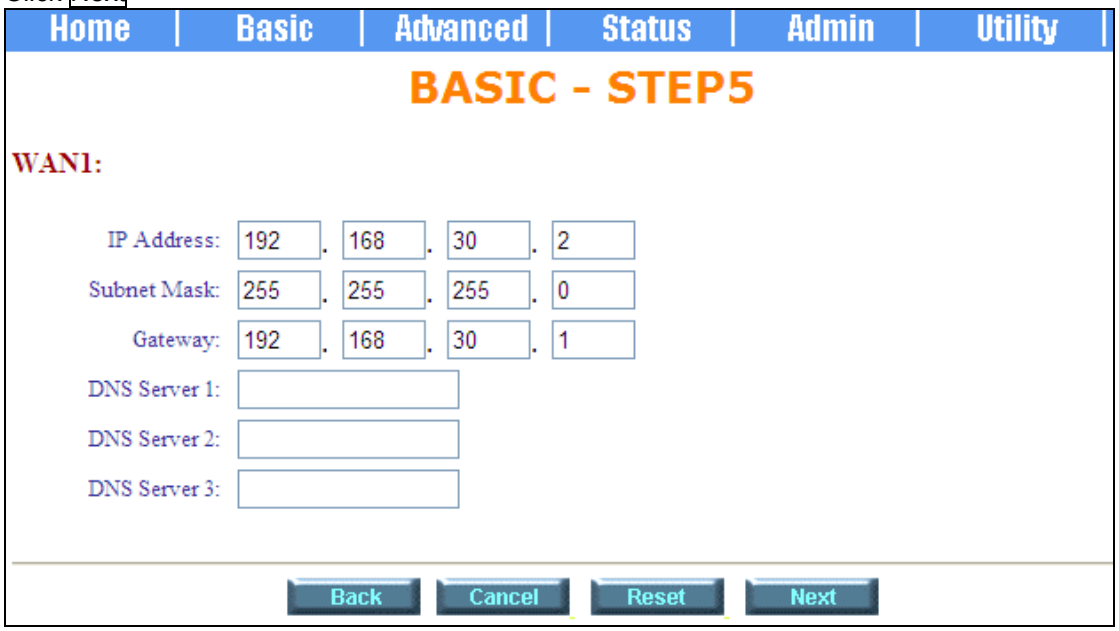
Note	The Protocol used in CO and CPE have to be the same.

Click Next to set up the IP parameters.



Click Next to set up the IP parameters.
IP Address: 192.168.30.2

Subnet mask: 255.255.255.0
Gateway: 192.169.30.1
Click Next



The screen will prompt the parameters that will be written in EPROM. Check the parameters before writing in EPROM.

Press Restart to restart the router working with new parameters or press continue to set up another parameter.

Chapter 10 . Configuration via Serial Console or Telnet with Menu Driven Interface

10.1 Serial Console

Check the connectivity of the RS-232 cable from your computer to the serial port of ROUTER. Start your terminal access program with VT100 terminal emulation. Configure the serial link with the following values:

Parameter	Value
Baud rate	9600
Data Bits	8
Parity Check	No
Stop Bits	1
Flow-control	No

Press the SPACE key until the login screen appears. When you see the login screen, you can logon to Router.

Only SPACE key invoke the login prompt. Pressing other keys does not work.

```
User: admin
Password: *****
```

The factory default user and passwords are both "admin".

10.2 Telnet

Make sure the correct Ethernet cable connects the LAN port of your computer to this Router. The LAN LNK LED indicator on the front panel will light up if a correct cable is used. To start your Telnet client with VT100 terminal emulation and connect to the management IP of Router, wait for the login prompt appears. Input User and Password after login screen pops up.

```
User: admin
Password: *****
```

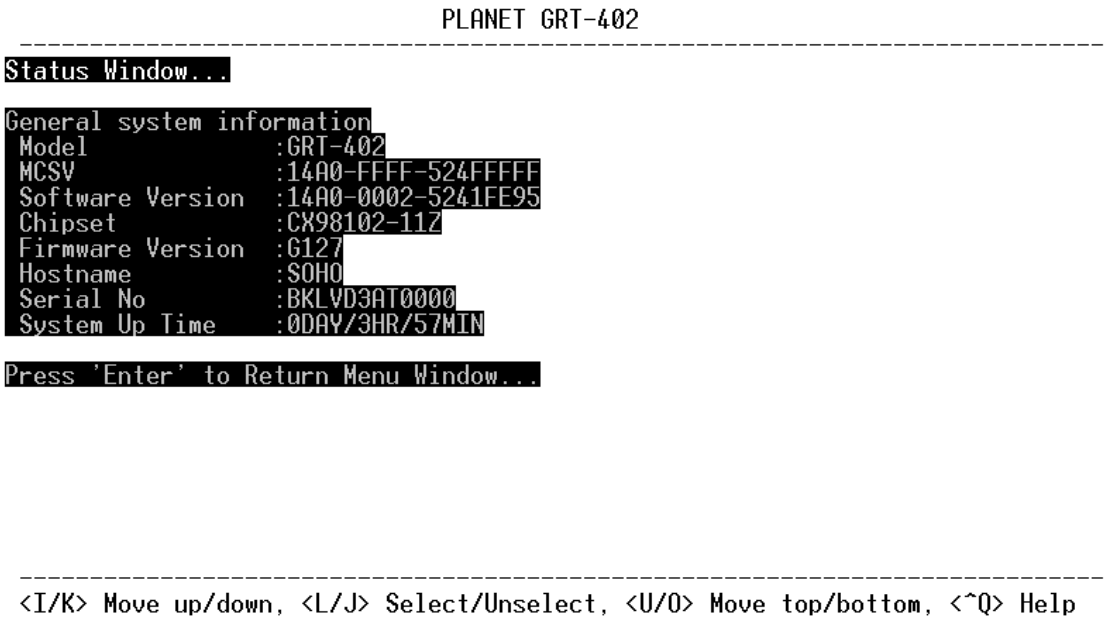
Note	The default IP address is 192.168.0.1.

10.3 Operation Interface

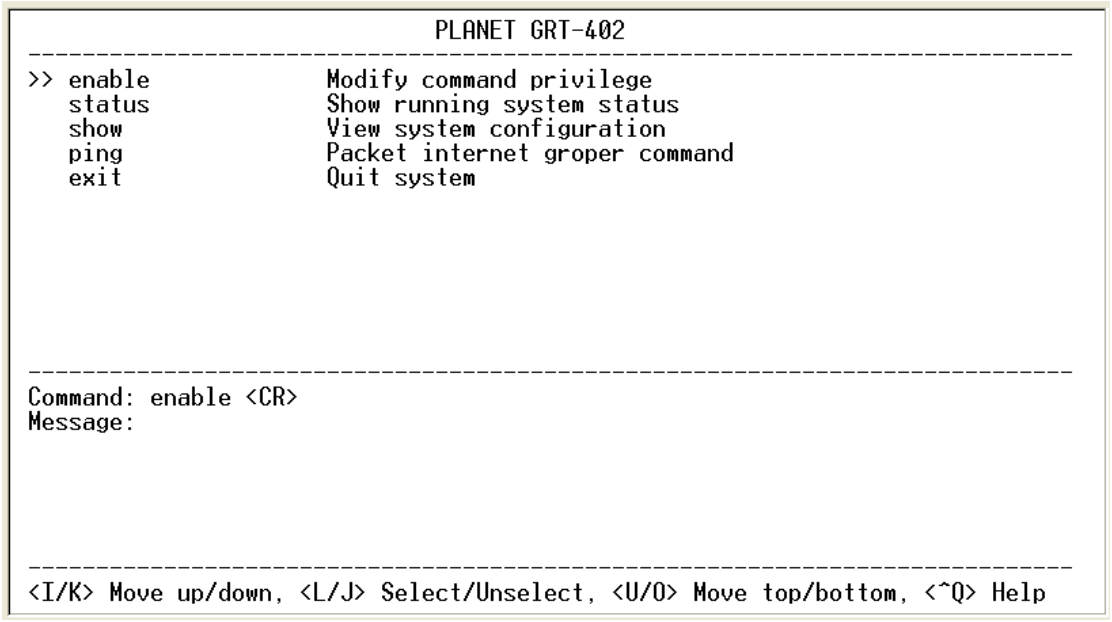
For serial console and Telnet management, the Router implements two operational interfaces: Command Line Interface (CLI) and menu driven interface. The CLI mode provides users a simple interface, which is better for working with script file. The menu driven interface is a user-friendly interface to general operations. The command syntax for CLI is the same as that of the menu driven interface. The only difference is that the menu driven interface shows you all of available commands for you to select. You don't need to remember the command syntax and save your time on typing the whole command line.

The following figure gives you an example of the menu driven interface. In the menu, you scroll up/down by pressing key **I / K**, select one command by key **L**, and go back to a higher level of menu by key **J**.

For example, to show the system information, just logon to the Router, move down the cursor by pressing key **K** twice and select "show" command by key **L**, you will see a submenu and select "system" command in this submenu, then the system will show you the general information.



10.4 Window Structure



From top to bottom, the window will be divided into four parts:

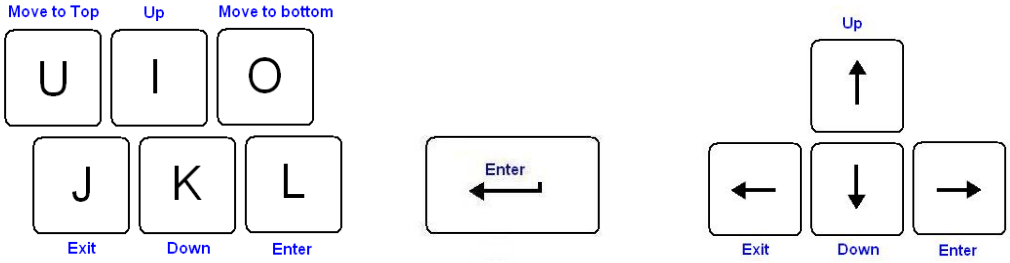
1. **Product name:** "GRT-101 / GRT-401 / GRT-402"
2. **Menu field:** Menu tree is prompted in this field. "**>>**" symbol indicates the cursor place.
3. **Configuring field:** You will configure the parameters in this field. **< parameters >** indicates the parameters you can choose and **< more…>** indicates that there have submenu in the title.
4. Operation command for help

The following table shows the parameters in the brackets.

Command	Description
<ip>	An item enclosed in brackets is required. If the item is shown in lower case bold, it represents an object with special format. For example, **<ip>** may be **192.168.0.3**.
<Route|Bridge>	Two or more items enclosed in brackets and separated by vertical bars means that you must choose exactly one of the items. If the item is shown in lower case bold with leading capital letter, it is a command parameter. For example, **Route** is a command parameter in **<Route|Bridge>**.
[1~1999]	An item enclosed in brackets is optional.
[1~65534|-t]	Two or more items enclosed in brackets and separated by vertical bars means that you can choose one or none of the items.

10.5 Menu Driven Interface Commands

Before changing the configuration, familiarize yourself with the operations list in the following table. The operation list will be shown on the window.



Menu Driven Interface Commands

Keystroke	Description
[UP] or I	Move to above field in the same level menu.
[DOWN] or K	Move to below field in the same level menu.
U	Move to top field in the same level menu
O	Move to bottom field in the same level menu
[LEFT] or J	Move back to previous menu
[RIGHT], L or [ENTER]	Move forward to submenu
[TAB]	To choose another parameter
Ctrl + C	To quit the configuring item
Ctrl + D	Disconnection
Ctrl + U	Hot-key switch to command line interface
Ctrl + Q	Display help menu

10.6 Main menu before enable

When following the menu, all of the configuration commands are placed in the subdirectories of Enable protected by supervisor password. On the other hand, unauthorized user cannot change any configurations but viewing the status and configuration of the router and using ping command to make sure the router is working.

```
>>  enable      Modify command privilege
    status      Show running system status
    show        View system configuration
    ping        Packet internet groper command
    exit        Quit system

-------------------------------------------------------------------------
```

If you need setup and manage the router, you must set **enable** command before.

10.7 Enable

To set up the router, move the cursor " **>>**" to **enable** and press enter key. While the screen appears, type the supervisor password. The default supervisor password is **root**. The password will be prompted as " ***** " symbol for system security.

```
-------------------------------------------------------------------------
Command: enable <CR>
Message: Please input the following information.

Supervisor password: ****
-------------------------------------------------------------------------
```

In this sub menu, you can set up management features and upgrade software, backup the system configuration and restore the system configuration via utility tools.

For any changes of configuration, you have to write the new configuration to EPROM and reboot the router to work with new setting.

The screen will prompt as follows:

```
>> enable      Modify command privilege
   setup       Configure system
   status      Show running system status
   show        View system configuration
   write       Update flash configuration
   reboot      Reset and boot system
   ping        Packet internet groper command
   admin       Setup management features
   utility     TFTP upgrade utility
   exit        Quit system
```

The description of the commands is:

Command	Description
enable	Modify command privilege. When you login via serial console or Telnet, the router defaults to a program execution (read-only) privileges to you.

	To change the configuration and write changes to nonvolatile RAM (NVRAM), you must work in enable mode.
setup	To configure the router, you have to use the setup command.
status	View the status of router.
show	Show the system and configuration of router.
write	Update flash configuration. After you have completed all necessary setting, make sure to write the new configuration to NVRAM by "**write**" command and reboot the system, or all of your changes will not take effect.
reboot	Reset and boot system. After you have completed all necessary setting, make sure to write the new configuration to NVRAM and reboot the system, otherwise, all of your changes will not take effect.
ping	Internet ping command.
admin	You can setup management features in this command.
utility	Upgrade software and backup and restore configuration.
exit	Quit system.

10.8 Status

You can view running system status of SHDSL.bis, WAN, route, interface, fireware, ip_qos and stp via **status** command.

Move cursor " **>>** " to **status** and press enter.

```
>> shdsl.bis        Show SHDSL.bis status
   lan              Show lan interface status
   wan              Show WAN interface status
   route            Show routing table
   interface        Show interface statistics status
   firewall         Show firewall status
   ip_qos           Show IP QoS statistics
   stp              Show STP status
   clear            Reset statistics
```

Command	Description
shdsl.bis	The SHDSL.bis status includes line rate, SNR margin, TX power, attenuation, and CRC error of the product, and SNR margin, attenuation and CRC error of remote side. The router can access remote side's information via EOC (embedded operation channel).
lan	LAN status shows all their parameters including IP address ,Net mask, Mac address and protocol information

wan	WAN status shows all their parameters including IP address ,Net mask, PVC and protocol information
route	You can see the routing table via route command.
interface	The statistic status of WAN and LAN interface can be monitor by interface command.
firewall	Show firewall status (for firewall models only)
Ip_qos	Show IP QOS status
stp	Show the STP status on all LANs and WANs
clear	Clear all statistics data

10.8.1 Shdsl.bis

Move cursor " **>>** " to **shdsl.bis** and press enter.

If the Router is 4-wire model, it will show two channels' status as follows:

Monitoring Window...

<SHDSL.bis Status>

Channel	:	A /	B
SHDSL.bis Mode	: CPE Side / CPE Side		
Line Rate(n*64)	:	0kbps /	0kbps
Current SNR Margin	:	0dB /	0dB
Attenuation	:	0dB /	0dB
CRC Error Count	:	0 /	0

SHDSL Remote Side Status

Channel	:	A /	B
Current SNR Margin	:	0dB /	0dB
Attenuation	:	0dB /	0dB
CRC Error Count	:	0 /	0

If the Router is a 2-wire model, it will show one channel's status as follows:

Monitoring Window...

<SHDSL.bis Status>

SHDSL.bis Mode
Line Rate(n*64) :CPE Side
Current SNR Margin :0kbps
Attenuation :0dB
CRC Error Count :0dB
:0
SHDSL Remote Side Status
Current SNR Margin :0dB
Attenuation :0dB
CRC Error Count :0

Show SHDSL.bis status includes the Mode, Line Rate, Current SNR Margin, Attenuation and CRC error count on both side. They are real time status, and the screen may refresh anytime. You can press the "c" key to clear CRC error counter. Press Ctrl-C can quit this screen.

10.8.2 Wan

Move cursor " **>>** " to **wan** and press enter.

Monitoring Window...

WAN	IP address	/	NetMask	VPI/ VCI	Encap	Protocol	Active
WAN1	192.168.	1.	1/255.255.255.	0 0/ 32	LLC	IPoA	No
WAN2	192.168.	2.	1/255.255.255.	0 0/ 34	LLC	Ethernet	No
WAN3	192.168.	3.	1/255.255.255.	0 0/ 34	LLC	Ethernet	No
WAN4	192.168.	4.	1/255.255.255.	0 0/ 35	LLC	IPoA	No
WAN5	192.168.	5.	1/255.255.255.	0 0/ 36	LLC	PPPoA	No
WAN6	192.168.	6.	1/255.255.255.	0 0/ 37	LLC	Ethernet	No
WAN7	192.168.	7.	1/255.255.255.	0 0/ 38	LLC	Ethernet	No
WAN8	192.168.	8.	1/255.255.255.	0 0/ 39	LLC	Ethernet	No

Show WAN status include IP address, Net Mask, VPI/VCI, encapsulation type, protocol on each WAN ports

10.8.3 Route

Move cursor " **>>** " to **Route** and press enter.

Monitoring Window...

```
Flag    Destination     /       Netmask     /       Gateway         Interface       Portname
---- ---------------------------------------- ---------- -------
 C          192.168.0.0/    255.255.255.0/      directly        192.168.0.1       LAN
 C            127.0.0.1/255.255.255.255/      directly          127.0.0.1 Loopback

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

You can view the routing table on here.

10.8.4 Interface

Move cursor " **>>** " to **Interface** and press enter.

```
------------------------------------------------------------------------------
Monitoring Window...
<Interface Statistics>
```

Port	InOctets	InPackets	OutOctets	OutPackets	InDiscards	OutDiscards
LAN	0	0	512	8	0	0
WAN1	0	0	0	0	0	0
WAN2	0	0	0	0	0	0
WAN3	0	0	0	0	0	0
WAN4	0	0	0	0	0	0
WAN5	0	0	0	0	0	0
WAN6	0	0	0	0	0	0
WAN7	0	0	0	0	0	0
WAN8	0	0	0	0	0	0

```
------------------------------------------------------------------------------
```

You can view interface statistics data on one LAN port and maximum eight WAN ports.

10.8.5 Firewall

Move cursor " **>>** " to **firewall** and press enter.

```
------------------------------------------------------------------------------
Monitoring Window...


<Current Firewall Status>
        Attack Type         Current Status History Status
---------------------- -------------- --------------
        All DoS protects are disabled!
---------------------- -------------- --------------
Packets dropped by DoS protect function: 0
```

Packets dropped by SPI filter function: 0

Packets dropped by packet filter function: 0

You can view firewall statistics. (Only for firewall models)

10.8.6 IP_qos

Move cursor " **>>** " to **Ip_qos** and press enter.

Command: status ip_qos <0~8>

Message: Please input the following information.

Interface number <0~8>:

You can view IP QoS statistics data on one LAN port.

Monitoring Window...

<Current IP QoS Statistics - LAN Interface>

Preced.	InBytes	InPackets	OutBytes	OutPackets	OutDropByts	OutDropPkts
0	0	0	0	0	0	0
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0

10.8.7 STP

Move cursor " **>>** " to **STP** and press enter.

<STP Status>
Bridge ID / Designated ROOT ID : 8000-000379-572002 / 8000-000379-572002
ROOT Port / ROOT Path Cost : None / 0
Max Age/Forward Delay/Hello Time: 20 / 15 / 2(secs)

	LAN	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
State	F	D	D	D	D	D	D	D	D
Priority	128	128	128	128	128	128	128	128	128
Path Cost	100	500	500	500	500	500	500	500	500

<Hint> D-Disable, B-Blocking, LS-Listening, LN-Learning, F-Forwarding.

You can view all STP status on all LAN and WANs ports.

The STP state per LANs and WANs are as following:

Blocking - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.

Listening - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.

Learning - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)

Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

Disabled - Not strictly part of STP, a network administrator can manually disable a port.

10.8.8 Clear

Move cursor " **>>** " to **Clear** and press enter.
You can clear all statistics by this command.

Command: status clear <CR>
Message: Clear OK!

10.9 Show

You can view the system information, configuration and configuration in command script by **show** command.

Move cursor " **>>** " to **show** and press enter.

```
>> system          Show general information
   config          Show all configuration
   script          Show all configuration in command script
```

Command	Description
system	The general information of the system will show in system command.
config	Config command can display detailed configuration information.
script	Configuration information will prompt in command script.

10.9.1 System information

Move cursor to " **>>** " to **system** and press enter.

Status Window...

General system information

MCSV	:14A1-0000-5221D8B0
Software Version	:148D-0000-4101606C
Chipset	:PEF24628V1.2
Firmware Version	:1.1-1.5.7__004
Hostname	:SOHO
System Up Time	:0DAY/0HR/50MIN

From this screen, you can know more about the general information of this router.

10.9.2. Configuration information

Move cursor to " **>>** " to **config** and press enter.

You can view all setting using table format.

10.9.3 Configuration with Script format

Move cursor to " **>>** " to **script** and press enter.

You can view all setting using script format.

10.10 Write

For any changes of configuration, you must write the new configuration to EPROM using **write** command and reboot the router to take affect.

Move cursor to " **>>** " to **write** and press enter.

Command: write <CR>
Message: Please input the following information.

Are you sure? (y/n): **y**

Press "y" to confirm the write operation.

10.11 Reboot

To reboot the router, please use "**reboot**" command. Move cursor to " **>>** " to **reboot** and press enter.

Command: reboot <CR>
Message: Please input the following information.

Do you want to reboot? (y/n): **y**

Press "y" to confirm the reboot operation.

10.12 Ping

Ping command will be used to test the Ethernet connection of router or Internet linking condition. Move cursor " **>>** " to **ping** and press enter.

Command: ping <ip> [1~65534|-t] [1~1999]
Message: Please input the following information.

IP address <IP> : **10.0.0.1**
Number of ping request packets to send (TAB select): **-t**
Data size [1~1999]: **32**

There are 3 parameters for ping command:

<ip> [1~65534|-t] [1~1999]

IP address: The IP address which you want to ping.

Number of ping request packed to send, key TAB for further selection:

- Default: It will send 4 packets only
- 1~65534: Set the number of ping request packets from 1 to 65534
- -t : It will continuous until you key Ctrl+C to stop

Data Size: From 1 to 1999

10.13 Administration

You can modify the user profile, security, SNMP (Sample Network Management Protocol), supervisor information and SNTP (Simple Network Time Protocol) in **admin**.

For configuration the parameters, move the cursor " **>>** " to **admin** and press enter.

```
>> user          Manage user profile
   security      Setup system security
   snmp          Configure SNMP parameter
   passwd        Change supervisor password
   id            Change supervisor ID
   sntp          Configure time synchronization
```

10.13.1 User Profile

You can use **user** command to clear, modify and list the user profile. You can set up at most five users to access the router via console port or telnet in user profile table however users who have the supervisor password can change the configuration of the router. Move the cursor " **>>** " to **user** and press enter key.

```
>> clear         Clear user profile
   modify        Modify the user profile
   list          List the user profile
```

You can delete the user by number using **clear** command. If you do not make sure the number of user, you can use **list** command to check it. **Modify** command is to modify an old user information or add a new user to user profile.

To modify or add a new user, move the cursor to **modify** and press enter.

```
---------------------------------------------------------------------
Command: admin user modify <1~5> <more...>
Message: Please input the following information.

Legal access user profile number <1~5> : 2
---------------------------------------------------------------------
```

The screen will prompt as follows:

```
>> Attrib        UI mode
   Profile       User name and password
```

There are two UI modes, **command** and **menu** mode, to set up the router. We will not discuss command mode in this manual.

Move the cursor to **Attrib** to change the UI mode on this profile
Move the cursor to **Profile** and press enter, you can change the username and their password on this profile.

The screen will prompt as follows:

```
---------------------------------------------------------------------------
 Command: admin user modify 5 profile <name> <pass_conf>
 Message: Please input the following information.

 Legal user name (ENTER for default) <admin>: superman
 Input the old Access password: ****
 Input the new Access password: ****
 Re-type Access password: ****
 ---------------------------------------------------------------------------
```

For example, set up the legal user name is "superman" and access password is"1234",and use write command to store on NVRAM.

Finally, you can use **list** command to check the listing of five profiles including on user name and their UI mode. Next time when you re-enter this system, you can use this set of username and password. You can set up a maximum of five profiles, i.e five sets of usernames and passwords.

User: superman
Password: ****

User Profile

User profile	User name	Password	Attrib
1			□Menu □Command
2			□Menu □Command
3			□Menu □Command
4			□Menu □Command
5			□Menu □Command

For example, when using the command **list**, the screen will prompt as follows:

```
---------------------------------------------------------------------------
Legal Access User Profile
   No          User    Name            UI Mode
 ---- ------------------ -----------
    1                       test          Menu
    2                     test-1          Menu
    3                     test-2       Command
    4                     test-3       Command
    5                   superman          Menu

---------------------------------------------------------------------------
```

10.13.2 Security

Security command can be configured as sixteen legal IP addresses for telnet access and telnet port number.

Move the cursor " **>>** " to **security** and press enter. The default legal address is 0.0.0.0. It means that there is no restriction of IP to access the router via telnet.

```
>> port          Configure telent TCP port
   ip_pool       Legal address IP address pool
   list          Show security profile
```

Telnet TCP Port:

Telnet TCP Port	

Legal client IP Address pool:

	Legal client IP Address pool
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Move the cursor to **port** and press enter. You can set up port number from 1 to 65534.

Move the cursor to **IP Pool** and press enter, there are sixteen legal IP addresses for telnet access. The default legal address is 0.0.0.0. It means that there is no restriction of IP to access the router via telnet. There are two sub-menus: **modify** and **clear** for easy to set up each one.

Move the cursor to **list** and press enter, you can view full listing on security profile including the Telnet listing TCP port and 16 host IP address.

10.13.3 SNMP

Simple Network Management Protocol (SNMP) is the protocol not only governing network management, but also the monitoring of network devices and their functions.

The router can generate SNMP traps to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security. This router supports MIB I & II.

Move the cursor " **>>** " to **snmp** and press enter.

```
>> community     Configure community parameter
   trap          Configure trap host parameter
```

10.13.4 Community

There are 5 entries of SNMP community that can be configured in this system.

Move the cursor to **community** and press enter.

```
------------------------------------------------------------------------------
--
Command: admin snmp community <1~5> <more...>
Message: Please input the following information.

Community entry number <1~5> : 2
------------------------------------------------------------------------------
--
```

The screen will prompt as follow:

```
>> edit              Edit community entry
   list              Show community configuration
```

Move the cursor to **edit** and press enter. You can setup the following:

Validate : Set **Enable** or **Disable**
Community : Key in the string
Access right : Set **Read only**, **Read Write** or **Denied**

Move the cursor to **list** and press enter, you can view full listing on SNMP Community Pool.
5 entries of SNMP trap are allowed to be configured in this system.

SNMP Community:

SNMP entry(1~5)	
Validate	☐Enable ☐Disable
Community	
Access Right :	☐Read only ☐Read Write ☐Denied

10.13.4.1 Trap Host

Move the cursor to **trap** and press enter.

```
                    ------------------------------------------------------------------------
Command: admin snmp trap <1~5> <more...>
Message: Please input the following information.

Trap host entry number <1~5> : 2
------------------------------------------------------------------------
```

The screen will prompt as follow:

```
>> edit              Edit trap host parameter
   list              Show trap configuration
```

Move the cursor to **edit** and press enter, you can setup the following:

Version : **Disable**, **1** or **2**
Trap host IP address : Key in the IP address
Community : Key in the string

SNMP Trap Host:

Trap Host entry(1~5)	
Version	□Disable □Ver.1 □Ver.2
IP Address	

Community	

Move the cursor to **list** and press enter, you can view full listing on SNMP Trap Host Pool.

10.13.5 Supervisor Password and ID

The supervisor password and ID is the last door for security but the most important. Users who access the router via web browser have to use the ID and password to configure the router and users who access the router via telnet or console mode have to use the password to configure the router. Suggest changing the ID and password after the first time of configuration, and save it. At next time when you access to the router, you have to use the new password.

	Factory default
User name	admin
Password	admin
Supervisor ID	root
Supervisor Password	root

Command: admin passwd <pass_conf>
Message: Please input the following information.

Input old Supervisor password: ****
Input new Supervisor password: ********
Re-type Supervisor password: ********

Command: admin id <pass_conf>
Message: Please input the following information.

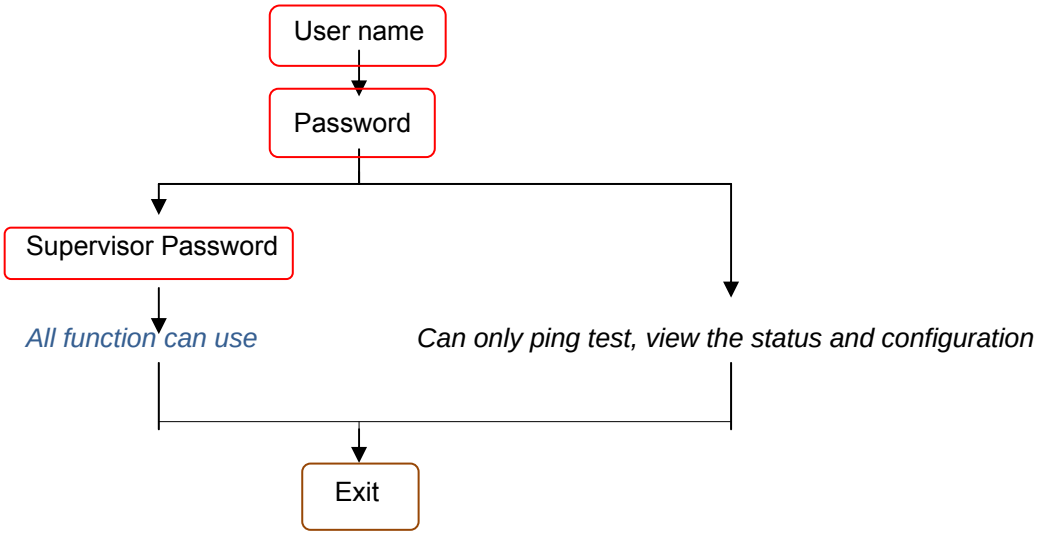
Legal user name (Enter for default) <root> : **test**

The default admin ID is "root".

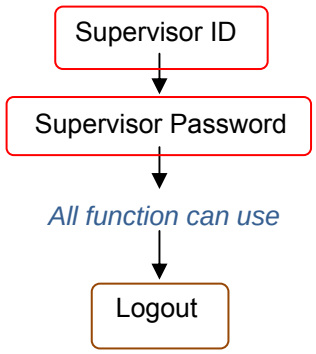
Supervisor ID and Password:

Supervisor ID	
Supervisor Password	

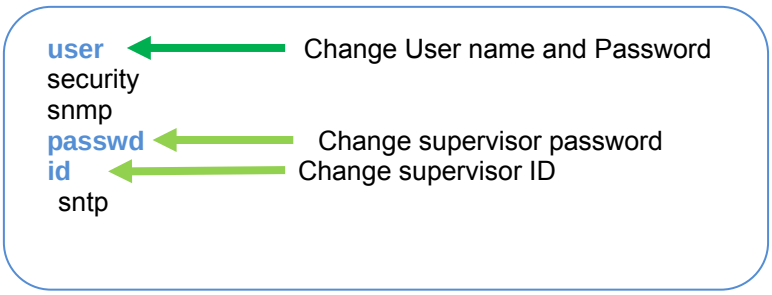
Telnet Console mode:



Web Brower mode:



Administration:



10.13.6 SNTP

Time synchronization is an essential element for any business that relies on an IT system. The reason for this is that these systems all have clocks that are the source of time for files or operations they handle. Without time synchronization, time on these systems varies with each other or with the correct time and this can cause- virtual server schedule processes to fail and system log exposures with wrong data.

There are two methods to synchronize time, synchronize with PC or SNTPv4. If you choose

synchronize with PC, the router will synchronize with PC. If you choose SNTPv4, the router will use the protocol to synchronize with the time server. Synchronization with time server, SNTP v4, needs to configure service, time_server and time_zone. Synchronization with PC does not need to configure the above parameters.

Move the cursor " **>>** " to **sntp** and press enter.

```
>> method          Select time synchronization method
   service          Tigger SNTP v4.0 service
   time_server1     Configure time server 1
   time_server2     Configure time server 2
   time_server3     Configure time server 3
   updaterate       Configure update period
   time_zone        Configure GMT time zone offset
   list                          Show SNTP configuration
```

To configure SNTP v4 time synchronization, follow the below procedures.

move the cursor to method and press enter.

```
---------------------------------------------------------------------
Command: admin sntp method <SNTPv4|SyncWithPC>
Message: Please input the following information.

SYNC method (Enter for default) <SyncWithPC> : SNTPv4
---------------------------------------------------------------------
```

Move the cursor to service and press enter.

```
---------------------------------------------------------------------
Command: admin sntp service <Disable|Enable>
Message: Please input the following information.

Active SNTP v4.0 service (Tab Select) <Enable> : Enable
---------------------------------------------------------------------
```

Move the cursor to time_server1 and press enter.

```
---------------------------------------------------------------------
Command: admin sntp time_server1 <string>
Message: Please input the following information.

Time server address (Enter for default) <ntp-2.vt.edu> : ntp-2.vt.edu
---------------------------------------------------------------------
```

You can configure three time servers in this system with time_server1, time_server2 and time_server3.
The default time servers are the following:

- time_server1 : ntp-2.vt.edu
- time_server2 : ntp.drydog.com
- time_server3 : ntp1.cs.wisc.edu

Move the cursor to **update_rate** and press enter.

```
---------------------------------------------------------------------
Command: admin sntp update_rate <10~268435455>
Message: Please input the following information.
```

Update period (secs) (Enter for default) <3600> : **86400**

Move the cursor to **time_zone** and configure where your router is placed. The easiest way to know the time zone offset hour is from your PC clock. Double click the clock at the right corner of monitor and check the time zone of your country. It will show (GMT+XX:XX) or (GMT-XX.XX) information.

Command: admin sntp time_zone <-12~12>
Message: Please input the following information.

GMT time zone offset (hours) (Enter for default) : **-8**

Time synchronization:

Method	□Sync with PC □SNTP V4.0
SNTP V4.0 Service	□Enable □Disable
Time Server 1	
Time Server 2	
Time Server 3	
Update Rate	
Time Zone	

Move the cursor to **list** for review the SNTP setting.

Status Window...

Time Synchronization Parameters
Method : SNTP v4.0
Service : Enable
Time Server 1 : ntp-2.vt.edu
Time Server 2 : ntp.drydog.com
Time Server 3 : ntp1.cs.wisc.edu
Update Period : 3600 secs
GMT Time Zone Offset : 8 hours

10.14 Utility

There are three utility tools, upgrade, backup and restore, embedded in the firmware. You can update the new firmware via TFTP upgrade tools and backup the configuration via TFTP backup tool and restore the configuration via TFTP restore tool. For upgrade, TFTP server with the new firmware will be supported by supplier but for backup and restore, you must have your own TFTP server to backup and restore the file.

Move the cursor " **>>** " to **utility** and press enter.

>> upgrade Upgrade main software
backup Backup system configuration
Restore Restore system configuration

10.14.1 Upgrade

Move the cursor " **>>** " to **upgrade** and press enter.

```
---------------------------------------------------------------------------
 Command: utility upgrade <ip> <file>
 Message: Please input the following information.

 TFTP server IP address (ENTER for default) <192.168.0.2>: 192.168.0.100
 Upgrade filename (ENTER for default) <default.bin>: K5890000.bin

---------------------------------------------------------------------------
```

Type TFTP server IP address and upgrade filename of the software.

10.14.2 Backup

Move the cursor " **>>** " to **backup** and press enter.

```
---------------------------------------------------------------------------
 Command: utility backup <ip> <file>
 Message: Please input the following information.

 TFTP server IP address (ENTER for default) <192.168.0.2>: 192.168.0.120
 Upgrade filename (ENTER for default) <default.bin>: backup001.bin


---------------------------------------------------------------------------
```

Type TFTP server IP address and backup filename of system configuration.

10.14.3 Restore

Move the cursor " **>>** " to **restore** and press enter.

```
---------------------------------------------------------------------------
 Command: utility restore <ip> <file>
 Message: Please input the following information.

 TFTP server IP address (ENTER for default) <192.168.0.2>: 192.168.0.150
 Upgrade filename (ENTER for default) <default.bin>: backup002.bin

 ---------------------------------------------------------------------------
```

Type TFTP server IP address and restore filename of system configuration.

10.15 Exit

If you want to exit the system without saving, use **exit** command to quit system.

```
---------------------------------------------------------------------------
 Command: exit <CR>
 Message: Please input the following information.

 Do you want to disconnect? (y/n):

---------------------------------------------------------------------------
```

Press "y" to confirm the exit operation.

10.16 Setup

All of the setup parameters are located in the subdirectories of setup. Move the cursor " **>>** " to **setup** and press enter.

```
>> mode          Switch system operation mode
   Shdsl.bis     Configure SHDSL parameters
   wan           Configure WAN interface profile
   bridge        Configure transparent bridging
   vlan          Configure virtual LAN parameters
   stp           Configure bridge STP parameters
   route         Configure routing paramters
   lan           Configure LAN interface profile
   ip_share      Configure NAT/PAT parameters
   firewall      Configure Firewall parameters
   ip_ qos       Configure IP QoS paramters
   dhcp          Configure DHCP parameters
   dns_proxy     Configure DNS proxy parameters
   hostname      Configure local host name
   default       Restore factory default setting
```

10.16.1 Operation Mode

The product can act as routing mode or bridging mode. The default setting is routing mode. You can change the system operation mode by using mode command. Move the cursor " **>>** " to **mode** and press enter.

```
---------------------------------------------------------------------
Command: setup mode <Route|Bridge>
Message: Please input the following information.

System operation mode (TAB select) <Route>: Route
---------------------------------------------------------------------
```

Operation Mode:

Operation Mode	☐Route ☐Bridge

10.16.2 SHDSL.bis

You can set up the SHDSL parameters by the command **shdsl**. Move the cursor " **>>** " to shdsl and press enter.

```
`>> mode          Configure SHDSL.bis mode
   link          Configure shdsl.bis link
   n*64          Configure SHDSL.bis data rate
   type          Configure SHDSL.bis annex type
   margin        Configure SHDSL.bis SNR margin
   tcpam         Configure shdsl.bis TCPAM type
   probe         Configure shdsl.bis line probe
   tclayer       Configure shdsl.bis TC Layer
   clear         Clear current CRC error count
```

SHDSL.bis:

Mode	□STU-C □STU-R
Link	□2-Wire □M-Pair □M-Pair(Conexant) □Auto_Fall_Back □Standby □Multi-link
Line rate (Nx64)	
Annex Type	□A □B □AF □BG
SNR Margin	
TCPAM	□Auto □TCPAM-16 □TCPAM-32
Probe	□Disable □Enable
TC Layer	□ATM □EFM

10.16.2.1 Mode

There are two types of SHDSL.bis mode, STU-C and STU-R. STU-C means the terminal of central office and STU-R means customer premise equipment.

10.16.2.2 Link

This link item is only for 4-wire model.

2-wire mode

For 4-wire model, it can use only the first one pair for the single pair DSL wire application.

M – Pair Mode

In this mode, each wire pair of SHDSL.bis router must be configured with the same line rate. If one pair fails then the entire line must be restarted. It also has the Conexant M-pair standard used with connection to other router with Conexant chip set solution.

Auto Fall Back Mode

Two DSL pairs are working simultaneously. When one pair of both is disconnected, the other pair will keep working.

Standby Mode

Only one of two pairs is working; the other pair is standby. If the working pair fails, the standby pair will start up to continue.

Multi–Link Mode

For 4-wire model, each pair will connect to two different remote devices, which may or may not be in the same location.

10.16.2.3 N*64

You can set up the data rate by the multiple of 64Kbps where n is from 3 to 89.
If the router is 4 wire model and doesn't use on 2-wire mode, the line rate will double from 2-wire model's setting.

		2-wire model	4-wire model
Annex A/B	TCPAM-16	192~2304 kbps(n=3~36)	384~4608 kbps(n=6~72)
Annex AF/BG	TCPAM-16	192~3840 kpbs (n=3~60)	384~7680 kbps(n=6~120)
	TCPAM-32	768~5696 kpbs(n=12~89)	1536~11392 kbps(n=24~178)

10.16.2.4 Type

There are four types of SHDSL.bis Annex type, **Annex-A**, **Annex-B**, **Annex-AF**, and **Annex-BG**.

10.16.2.5 Margin

Generally, you cannot need to change SNR margin, which ranges from -10 to 21. SNR margin is an index of line connection. You can see the actual SNR margin in STATUS SHDSL.bis. The larger SNR margin is, the better the line connection quality is. If you set SNR margin in the field as 3, the SHDSL.bis connection will drop and reconnect when the SNR margin is lower than 3. On the other hand, the device will reduce the line rate and reconnect for better line connection.

10.16.2.6 TCPAM

There are two TCPAM settings on SHDSL.bis: TCPAM-16 or TCPAM-32. In most cases, you can set Auto. It can use TCPAM-16 or TCPAM-32 for Annex A/F or B/G. If using Annex A or B, only TCPAM-16 can be used.

10.16.2.7 Probe

For adaptive mode, you have to Enable. The router will adapt the data rate according to the line status.

10.16.2.8 TC Layer

There are two TC layer settings on this router: EFM layer and ATM layer. According to the network connected: ATM based access networks or Ethernet based access networks

10.16.2.9 Clear

Clear command can clear CRC error count.

10.16.3 WAN

The router supports 8 PVC, private virtual circuit, and so you can set up eight WAN, such as WAN1 to WAN8. Move the cursor " **>>** " to **wan** and press enter.

For example, to set up WAN1, type **1** on interface number.

```
---------------------------------------------------------------------
Command: setup wan <1~8>
Message: Please input the following information.

Interface number <1~8>: 1
---------------------------------------------------------------------

---------------------------------------------------------------------------------------
>> protocol          Link type protocol
   address           IP address and subnet mask
   vpi_vci           Configure VPI/VCI value
   encap             Configure encapsulation type
   qos               Configure VC QoS
   isp               Configure account name, password and idle time
   ip_type           Configure IP type in PPPoA and PPPoE
   list              WAN interface configuration
---------------------------------------------------------------------------------------
```

WAN parameter:

WAN interface number(1~8)		
Protocol	☐Disable ☐Ethernet ☐PPPoA ☐IPoA ☐PPPoE	
Address	IP	
	Mask	
VC	VPI	
	VCI	
Encap	☐VC-Mux ☐LLC	
QoS	☐UBR ☐CBR ☐rt-VBR ☐nrt-VBR	
	PCR	
	SCR	
	MBS	
ISP	Name	
	Password	
	Idle Timeout	
IP Type (PPPoA or PPPoE)	☐Dynamic ☐Fixed ☐Unnumbered	

10.16.3.1 Protocols
There are four types of protocols, IPoA, EoA, PPPoA and PPPoE, which you can set up.
.

10.16.3.2 IP Address
For dynamic IP of PPPoA and PPPoE, you do not need to set up IP address and subnet mask.

10.16.3.3 VPI / VCI
There are unique VPI value and VCI value for Internet connection supported by ISP. The range of VIP is from 0 to 255 and VCI from 0 to 65535.

***VPI** (Virtual Path Identifier) : for set up ATM Permanent Virtual Channels(PVC).*
***VCI** (Virtual Channel Identifier) : for set up ATM Permanent Virtual Channels(PVC).*

10.16.3.4 Ecapsulation
There are two types of encapsulation, **VC-Mux** and **LLC**.

10.16.3.5 VC QoS

You can set up virtual circuit quality of service, VC QoS, using **qos** command. The router supports **UBR**, **CBR**, **VBR-rt** and **VBR-nrt**. Move the cursor to **qos** and press enter.

```
>> class        Configure QoS class
   pcr          Configure peak cell rate (kbps)
   scr          Configure sustainable cell rate (kbps)
   mbs          Configure max. burst size (cell)
```

UBR (Unspecified Bit Rate) is the simplest service provided by ATM networks. There is no guarantee of anything. It is a primary service used for transferring Internet traffic over the ATM network.

CBR (Constant Bit Rate) is used by connections that requires a static amount of bandwidth that is avilable during the connection life time. This bandwidth is characterized by Peak Cell Rate (PCR). Based on the PCR of the CBR traffic, specific cell slots are assigned for the VC in the schedule table. The ATM always sends a signle cell during the CBR connection's assigned cell slot.

VBR-rt (Varible Bit Rate real-time) is intended for real-time applications, such as compressed voice over IP and video comferencing, that require tightly constrained delays and delay variation. VBR-rt is characterized by a peak cell rate (PCR), substained cell rate (SCR), and maximun burst rate (MBR).

VBR-nrt (Varible Bit Rate non-real-time) is intended for non-real-time applications, such as FTP, e-mail and browsing.

PCR (Peak Cell Rate) in kbps: The maximum rate at which you expect to transmit data, voice and video. Consider PCR and MBS as a menas of reducing lantency, not increasing bandwidth. The range of PCR is 384kbps to 11392kbps

SCR (Substained Cell Rate): The sustained rate at which you expect to transmit data, voice and video. Consider SCR to be the true bandwidth of a VC and not the lone-term average traffic rate. The range of SCR is 384kbps to 11392kbps.

MBS (Maximum Burst Size): The amount of time or the duration at which the router sends at PCR. The range of MBS is 1 cell to 255 cells.

10.16.3.6 ISP

ISP command can configure account name, password and idle time. Idle time is from 0 minute to 300 minutes.

10.16.3.7 IP Type

Most of the ISPs use dynamic IP for PPP connection but some of the ISPs use static IP. You can configure the IP type: **Dynamic**, **Fixed** and **Unnumbered**. The setting is via **ip_type** command.

The **ip unnumbered** configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The ip unnumbered interface can "borrow" the IP address of another interface already configured on this router, which conserves network and address space.

10.16.3.8 List

You can review the WAN interface configuration via **list** command.

10.16.4 Bridge

You can set up the bridge parameters in bridge command. If the product is configured as a router, you do not want to set up the bridge parameters. Move the cursor " **>>** " to bridge and press enter.

```
>> gateway          Default gateway
   static           Static bridging table
```

10.16.4.1 Gateway

You can set up default gateway IP via gateway command.

10.16.4.2 Static Bridging Table

You can set up 20 sets of static bridge in static command. After entering **static** menu, the screen will prompt as below:

```
>> Deby_PCs         Deny PCs to access Internet
   add              Add static MAC entry
   delete           Delete static MAC entry
   modify           Modify static MAC entry
   list             Show static bridging table
```

You can deny PCs to access Internet for security purpose use **deny_PCs** command
After enter add menu, the screen will prompt as follows:

```
>> mac              Configure MAC address
   lan_port         Configure LAN interface bridging type
   wan1_port        Configure WAN1 interface bridging type
   wan2_port        Configure WAN2 interface bridging type
   wan3_port        Configure WAN3 interface bridging type
   wan4_port        Configure WAN4 interface bridging type
   wan5_port        Configure WAN5 interface bridging type
   wan6_port        Configure WAN6 interface bridging type
   wan7_port        Configure WAN7 interface bridging type
   wan8_port        Configure WAN8 interface bridging type
```

Deny PCs to access interface:

Deny PCs to access Interface	☐Disable ☐Enable

Static MAC Address:

MAC entry number (1~20)			
MAC Address			
LAN	☐Filter	☐Forward	☐Dynamic
WAN1	☐Filter	☐Forward	☐Dynamic
WAN2	☐Filter	☐Forward	☐Dynamic
WAN3	☐Filter	☐Forward	☐Dynamic
WAN4	☐Filter	☐Forward	☐Dynamic
WAN5	☐Filter	☐Forward	☐Dynamic
WAN6	☐Filter	☐Forward	☐Dynamic
WAN7	☐Filter	☐Forward	☐Dynamic
WAN8	☐Filter	☐Forward	☐Dynamic

10.16.5 VLAN

Virtual LAN (VLAN) is defined as a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLAN is based on logical instead of physical connections, it is extremely flexible.

You can setup the Virtual LAN (VLAN) parameters in vlan command. The router support the implementation of VLAN-to-PVC only for bridge mode operation, i.e., the VLAN spreads over both the COE and CPE sides, where there is no layer 3 routing involved. The unit supports up to 8 active VLANs with shared VLAN learning (SVL) bridge out of 4096 possible VLANs specified in IEEE 802.1Q.

Move the cursor " >> " to **vlan** and press enter.

```
>> mode        Trigger virtual LAN function
   modify      Modify virtual LAN rule
   pvid        Modify port default ID
   link_mode   Modify port link type
   list        Show VLAN configuration
```

To activate the VLAN function, move the cursor " **>>** " to **mode** and press enter. The products support two types of VLAN: **802.11q** and **Port-Based**.

```
---------------------------------------------------------------------
Command: setup vlan active <Disable|8021Q|Port>
Message: Please input the following information.

Tigger VLAN function (Tab select) <Disable>: 8021Q
---------------------------------------------------------------------
```

VLAN Mode:

VLAN Mode	□Disable	□802.1Q Tag VLAN	□Port Based VLAN

The IEEE 802.1Q defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure. Port-Based VLANs are VLANs where the packet forwarding decision is based on the associated ports. If you don't use VLAN ,set to **Disbale**.

10.16.5.1 802.11Q VLAN

To modify the VLAN rule, move the cursor " **>>** " to modify and press enter.

Command: setup vlan modify <1~8> <1~4094> <string>
Message: Please input the following information.

Rule entry index <1~8>: **1**
VLAN ID (ENTER for default) <1>: **10**
VLAN port status (ENTER for default)<111111111>:111111111

For each VLAN, VID(VLAN ID) and PVID is a unique number among 1~4094.

		1	2	3	4	5	6	7	8	9
No.	VID	LAN	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1										
2										
3										
4										
5										
6										
7										
8										
PVID										
Link Type		□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk	□Access □Trunk

To assign PVID (Port VID), move the cursor ">>" to **pvid** and press enter. The port index 1 represents LAN and ports index 2 to 9 represents WAN1 to WAN8 respectively. VID value is the group at which you want to assign the PVID of the port.

Command: setup vlan pvid <1~9> <1~4094>
Message: Please input the following information.

Port index <1~9>: **1**
VID Value (Enter for default) <10>: **10**

VLAN port status is a 9-digit binary number whose bit-1 location indicates the VLAN port membership in which 1MSB and 8MSBs represents one LAN port and eight WAN ports, respectively. For example, the setting "vlan modify 1 20 111000000" means that the VID 20 member ports includes LAN, WAN1 and WAN. The member ports are tagged members. Use PVID command to change the member port to untagged members

To modify the link type of the port, move the cursor to **link_mod**e and press enter. There are two types of link: **access** and **trunk**. **Trunk** link will send the tagged packet from the port and **Access** link will send un-tagged packet from the port. The port index 1 represents LAN and ports index 2 to 9 represents WAN1 to WAN8 respectively. According to the operation mode of the device, link type of WAN port is automatically configured. If the product operates in bridge mode, the WAN link type will be trunk, and in routing mode, access.

Command: setup vlan link_mode <1~12> <Access|Trunk>
Message: Please input the following information.

Port index <1~12>: **1**
Port link type (Tab select) <Trunk>: **Access**

10.16.5.2 Port Base VLAN

With port-based VLAN, the port is assigned to a specific VLAN independent of the user or system attached to the port. This means all users attached to the port should be members in the same VLAN. The port based setting performs the VLAN assignment. The port configuration is static and cannot be automatically changed to another VLAN without manual reconfiguration.

For Port-based VLAN, user must set up the table using 802.11Q methods. But don't care the value of VID , PVID or link type.

Port-based VLAN:

No.	LAN1	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1									
2									
3									
4									
5									
6									
7									
8									

To view the VLAN table, move the cursor to **list** and press enter.

10.16.5.3 STP

Spanning-Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations

The default is disable.

>> active Trigger Bridge STP function

STP:

STP Function	□Disable □Enable

Once you enable the STP feature, you can see the STP status follow IEEE 802.1d standard to work. The working steps are Blocking, Listening, Learning and forwarding.

10.16.6 Route

You can set up the routing parameters in route command. If the product is configured as a bridge, you do not want to set up the route parameters. Move the cursor " **>>** " to **route** and press enter.

```
>> static          Configure static routing table
   rip             Configure RIP protocol
```

10.16.6.1 Static

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

With Dynamic Routing, you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

You can set up 20 sets of static route in static command. After entering **static** menu, the screen will show as follows:

```
>> add             Add static route entry
   delete          Delete static route entry
   List            Show static routing table
```

You can add 20 sets of static route entry by using **add** command. Type the IP information of the static route including IP address, subnet mask and gateway.

Static Route Table:

	IP Address	Subnet Mask	Gateway
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

You can delete the static route information via **delete** command.

You can review the static route entry by using **list** command.

10.16.6.2 Rip

To configure Routing Information Protocol (RIP), you can use **rip** command to set up the parameters. Move the cursor "**>>**" to **rip** and press enter.

```
>> generic      Configure operation and auto summery mode
   lan          Configure LAN interface RIP parameters
   wan          Configure WAN interface RIP parameters
   list         Show RIP configuration
```

Generic RIP Parameters

Generic command can set up RIP mode and auto summary mode.

Generic RIP Parameter:

Rip Mode	□Disable □Enable
Auto Summary	□Disable □Enable

Interface RIP Parameters

[LAN]

If there are other routers in your LAN, you can configure LAN interface RIP parameters via **lan** command.

```
Command: setup route rip lan <1~1> <more...>
Message: Please input the following information.

Active interface number <1~1>:
```

The screen will prompt as follows:

```
>> attrib       Operation, authentication and Poison reverse mode
   version      RIP protocol version
   authe        Authentication code
```

[WAN1 ~ WAN8]
The product supports 8 PVCs and you can configure the RIP parameters of each WAN via **wan** command. Move the cursor "**>>**" to **wan** and press enter.

Command: setup route rip wan <1~8> <more...>
Message: Please input the following information.

Active interface number <1~8>: **1**

The screen will prompt as follows:

>>	attrib	Operation, authentication and Poison reverse mode
	version	RIP protocol version
	authe	Authentication code

Attrib command can configure RIP mode, authentication type and Poison reverse mode.
Version command can configure RIP protocol version.
Authe command can configure authentication code.

Interface RIP Parameter:

Interface	(LAN, WAN1~8)
RIP Mode	□Disable □Enable □Silent
Authentication type	□None □Password □MD5
Poison reverse mode	□Disable □Enable
RIP protocol version	□Ver.1 □Ver.2
Authentication code	

You can review the list of RIP parameters via **list** command.

10.16.7 LAN

LAN interface parameters can be configured LAN IP address, subnet mask and NAT network type.

Command: setup lan <1~1> <more...>
Message: Please input the following information.

Interface number <1~1>:1

There is only one LAN port, so type 1 and press ENTER.

>>	ip_type	IP type
	address	LAN IP address and subnet mask
	attrib	NAT network type
	Ethernet	Media type

Ip_type can set up this IP is **Fixed** or **Dynamic**.
Address can set up **IP address** and **subnet mask**.
Attrib can set up NAT network type: **Global** or **Virtual**.
Ethernet item can set up the PHY parameters on this LAN port: **Auto**, **100M-Full**, **100M-Half**, **10M-Full** and **10M-Half**.

LAN Port parameter:

IP Type	□Fixed □Dynamic
LAN IP Address	
LAN Subnet Mask	
NAT Network type	□Global □Virtual
Ethernet Media Type	□Auto □100M-Full □100M-Half □10M- Full □10M-Half

10.16.8 IP share

You can configure Network Address Translation (NAT), Port Address Translation (PAT) and Demilitarized Zone (DMZ) parameters in **ip_share** menu.

10.16.8.1 NAT

NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and reverse the global IP addresses of incoming packets back into local IP addresses. This ensure security since each outgoing or incoming request must go through a translation process, that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and lets the company to use a single IP address of its communication in the Internet world.

To configure Network Address Translation (NAT), Move the cursor "**>>**" to **ip_share** then press enter.

```
>> nat          Configure network address translation
   pat          Configure port address translation
   dmz          Configure DMZ host function
```

Virtual IP address pool

You can configure NAT parameters in **nat** menu.

```
>> virtual      Virtual IP address pool
   global       Global IP address pool
   Fixed        Fixed IP address mapping
```

The **virtual** menu contains a range of virtual IP addresses, delete virtual IP addresses, and show virtual IP addresses.

```
>> range        Edit virtual IP address pool
   delete       Delete virtual IP address pool
   List         Show virtual IP address pool
```

You can create five virtual IP address pool range in **range** command.

```
---------------------------------------------------------------------
Command: setup ip_share nat virtual range <1~5> <ip> <1~253>
Message: Please input the following information.

NAT local address range entry number <1~5>: 1
Base address: 192.168.0.2
Number of address: 49
---------------------------------------------------------------------
```

NAT (Virtual IP address and range)

	Base Address	Number of Address
1		
2		
3		
4		
5		

You can delete virtual IP address range from 1 to 5 by using **delete** command.

You can view the virtual IP address range via **list** command.

Global IP address pool

To set up global IP address pool, move the cursor "**>>**" to **global** command and press enter.

```
>> range          Edit global IP address pool
   interface      Bind address pool to specific interface
   delete         Delete global IP address pool
   list           Show global IP address pool
```

You can create five global IP address pool range via **range** command.

```
---------------------------------------------------------------------
Command: setup ip_share nat global range <1~5> <ip> <1~253>
Message: Please input the following information.

NAT global IP address range entry number <1~5>: 1
Base address: 122.22.22.2
Number of address: 3
---------------------------------------------------------------------
```

After configuration global IP address range, you can bind address pool to specific interface via **interface** command.

NAT (Global IP Address and range):

	Base Address	Number of Address	Active Interface Numbe(1~8)
1			
2			
3			
4			
5			

```
---------------------------------------------------------------------
Command: setup ip_share nat global interface <1~5> <1~8>
Message: Please input the following information.

NAT global ddress range entry number <1~5>: 1
Active interface number <1~8>: 1
---------------------------------------------------------------------
```

You can delete global IP address range from 1 to 5 by using **delete** command.

You can view the global IP address range via **list** command.

Fixed IP address mapping

To modify fixed IP address mapping, move the cursor "**>>**" to **fixed** command and press enter.

```
    virtual          Virtual IP address pool
    global           Global IP address pool
>>  Fixed            Fixed IP address mapping
```

```
>>  modify          Modify fixed NAT mapping
    interface       Bind address pair to specific interface
    delete          Delete fixed NAT mapping
    list            Show fixed IP address mapping
```

You can create up to 10 fixed NAT mapping entry via **modify** command.

```
---------------------------------------------------------------------
Command: setup ip_share nat fixed modify <1~10> <ip> <ip>
Message: Please input the following information.

Fixed NAT mapping entry number <1~10>: 1
Local address: 192.168.0.250
Global address: 122.22.22.2
---------------------------------------------------------------------
```

Fixed Address Mapping:

	Local Address	Global Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

After configuration fixed IP address entry, you can bind the entry to specific interface via **interface** command.

```
---------------------------------------------------------------------
Command: setup ip_share nat fixed interface <1~10> <1~8>
Message: Please input the following information.

Fixed NAT mapping entry number <1~10>: 1
Active interface number (Enter for default) <1~8>: 1
---------------------------------------------------------------------
```

Fixed NAT Mapping:

Mapping entry number	Active Interface number(1~8)
1	
2	
3	
4	
5	
6	
7	

8	
9	
10	

You can delete fixed NAT mapping entry from 1 to 10 by using **delete** command.

You can view the fixed NAT mapping entry via **list** command.

10.16.8.2 PAT

Port Address Translation (PAT) is a feature of a device that translates TCP or UDP communications made between hosts on a private network and hosts on a public network. It allows a single public IP address to be used by many hosts on the private network, which is usually called a Local Area Network or LAN.

A PAT device transparently modifies IP packets as they pass through it. The modifications make all the packets which it sends to the public network from the multiple hosts on the private network appear to originate from a single host - the PAT device - on the public network.
In PAT, both the sender's private IP and port number are modified; the PAT device chooses the port numbers which will be seen by hosts on the public network.

In PAT, generally there is only one publicly exposed IP address and incoming packets from the public network are routed to their destinations on the private network by reference to a table held within the PAT device which keeps track of public and private port pairs. This is often called connection tracking.

To configure Port Address Translation, move the cursor "**>>**" to **pat** and press enter.

```
>> clear          Clear virtual server mapping
   modify         Modify virtual server mapping
   list           Show virtual server mapping pool
```

You can delete virtual server mapping entry, from 1 to 10, by using **clear** command.

You can create up to 10 virtual server mapping entry via **modify** command.

```
---------------------------------------------------------------------
Command: setup ip_share pat modify <1~10> <more...>
Message: Please input the following information.

Virtual server entry number <1~10>: 1
---------------------------------------------------------------------
```

After keying in enter, the screen will prompt as follows:.

```
>> interface      Active interface
   port           TCP/UDP port number
   server         Host IP address and port number
   protocol       Transport protocol
   name           Service name
   begin          The schedule of beginning time
   end            The schedule of ending time
```

Set the active interface number via **interface** command.

You can configure the global port number by using **port** command.

The local server, host, IP address and port number are configured via **server** command.

The authorized access protocol is set up via **protocol** command.

Name command can be used to configure the service name of the host server.

Begin and **end** command is used to set up the local server schedule to access.

Virtual Server:

Virtual Server entry number(1~10)	
Interface(1~8)	
ICP/UDP Port Number(1~65534)	
Host IP Address	
Host Port Number	
Protocol	□TCP □UDP
Service Name	
Beginning Time	
Ending Time	

You can view the fixed NAT mapping entry via **list** command.

10.16.8.3 DMZ

DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company private network and the outside public network. It prevents outside users from getting direct access to a server that has company private data.

To set up demilitarized zone, move the cursor ">>" to **dmz** and press enter.

```
>> active          Tigger DMZ host function
   address          Configure virtual IP address and interface
```

You can enable the demilitarized zone via **active** command.

After enabling the DMZ, shift the cursor to **address** and press enter.

```
---------------------------------------------------------------------
Command: setup ip_share dmz address <ip> <1~8>
Message: Please input the following information.

Virtual IP address: 192.168.0.251
Active interface number (Enter for default) <1>: 1
---------------------------------------------------------------------
```

DMZ Host:

DMZ Host Function	□Disable □Enable
IP Address	Active interface number
	1
	2

	3
	4
	5
	6
	7
	8

10.16.9 Firewall

This item is only for firewall models.
To configure Firewall, move the cursor " >> " to **firewall** and press enter.

```
-------------------------------------------------------------------
>> level                Configure firewall security level
   pkt_filter           Configure packet filter
   dos_protect          Configure DoS protect
-------------------------------------------------------------------
```

10.16.9.1 Firewall security level

There are three levels of firewall, which you can setup in this product.

Level one, **basic**, only enables the NAT firewall and the remote management security. The NAT firewall will take effect if NAT function is enabled. The remote management security is default to block any WAN side connection to the device. Non-empty legal IP pool in ADMIN will block all remote management connection except those IPs specified in the pool.

Level two, **automatic**, enables basic firewall security and all DoS protection.

Level three, **advanced**, is an advanced level of firewall where user can determine the security level for special purpose, environment, and applications by configuring the DoS protection and defining an extra packet filter with higher priority . Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

The firewall security level can configure via **level** command.

Firewall Security Level:

Level	□Basic □Automatic □Advanced

10.16.9.2 Packet Filtering

Packet filtering function can be configured by **pkt_filter** command. Move the cursor to **pkt_filter** and press enter.

```
>> active          Tigger packet filtering function
   drop_flag        Drop fragment packets
   add              Add packet filtering rule
   delete           Delete packet filtering rule
   modify           Modify packet filtering rule
   exchange         Exchange the filtering rule
   list             Show packet filtering table
```

To enable the packet filtering function, you can use **active** command.
To enable the drop fragmented packets, you can use **drop_frag** command.

Function enable:

Packet filtering function	☐Disable ☐Enable
Drop fragmented packet	☐Disable ☐Enable

Add the packet filtering rule via **add** command.
You can set up maximum 32 numbers packet filtering rules, Anytime you can modify and exchange their rules by using **modify** and **exchange** command.

>> protocol	Configure protocol type
direction	Configure direction mode
src_ip	Configure source IP parameter
dest_ip	Configure destination IP parameter
port	Configure port parameter (TCP and UDP only)
tcp_flag	Configure TCP flag (TCP only)
icmp_type	Configure ICMP flag (ICMP only)
description	Packet filtering rule description
enable	Enable the packet filtering rule
begin	The schedule of beginning time
end	The schedule of ending time
action	Configure action mode

Packet filtering:

Protocol	☐ANY ☐TCP ☐UDP ☐ICMP ☐GRE ☐RSVP ☐ESP ☐AH
Direction	☐Inbound ☐Outbound
Source IP	
Destination IP	
Source Port	(TCP/UDP only)
Destination Port	(TCP/UDP only)
TCP flag	(TCP only) ☐ANY ☐SYN ☐ACK
ICMP flag	(ICMP only) ☐Echo_Reply ☐Dest_Unreach ☐Src_Quench ☐Redirect ☐Echo_Request ☐R_Advertise ☐R_Solicit ☐T_Exceed ☐Param_Problem ☐T_Stamp

	☐T_Stamp_Reply ☐Info_Request ☐Info_Reply ☐□Addr_Mask_Request ☐Addr_Mask_Reply
Description	
Enable	☐ON ☐OFF
Begin Time	
End Time	
Action	☐ENY ☐PERMIT

10.16.9.3 DOS Protection

DoS protection parameters can be configured in dos_protection menu.
Move the cursor to **dos_protection** and press enter.

```
>> syn_flood        Enable protection SYN flood attack
   icmp_flood       Enable protection ICMP flood attack
   udp_flood        Enable protection UDP flood attack
   ping_death       Enable protection PING of death attack
   land_attack      Enable protection land attack
   ip_spoff         Enable protection IP spoofing attack
   smurf_attack     Enable protection smurf attack
   fraggle_attack   Enable protection fraggle attack
```

SYN flood: A SYN flood is a form of denial-of-service attack, attempts to slow your network by requesting new connections but not completing the process to open the connection. Once the buffer for these pending connections is full a server will not accept any more connections and will be unresponsive.

ICMP flood: A sender transmits a volume of ICMP request packets to cause all CPU resources to be consumed serving the phony requests.

UDP Flood: A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol(UDP). A sender transmits a volume of requests for UDP diagnostic services which cause all CPU resources to be consumed serving the phony requests.

Ping of Death: A ping of death (POD) attack attempts to crash your system by sending a fragmented packet, when reconstructed is larger than the maximum allowable size.

Land attack: A land attack is an attempt to slow your network down by sending a packet with

identical source and destination addresses originating from your network.

IP Spoofing: IP Spoofing is a method of masking the identity of an intrusion by making it appeared that the traffic came from a different computer. This is used by intruders to keep their anonymity and can be used in a Denial of Service attack.

Smurf attack: The Smurf attack is a way of generating a lot of computer network traffic to a victim host. That is a type of denial-of-service attack. A Smurf attack involves two systems. The attacker sends a packet containing a ICMP echo request (ping) to the network address of one system. This system is known as the amplifier. The return address of the ping has been faked (spoofed) to appear to come from a machine on another network (the victim). The victim is then flooded with responses to the ping. As many responses are generated for only one attack, the attacker is able use many amplifiers on the same victim.

Fraggle attack: A Fraggle attack is a type of denial-of-service attack where an attacker sends a large amount of UDP echo traffic to IP broadcast addresses, all of it having a fake source address. This is a simple rewrite of the smurf attack code.

DoS Protection

SYN flood	☐Disable	☐Enable	Packets per sec. 0~700	
ICMP flood	☐Disable	☐Enable	Packets per sec. 0~700	
UDP flood	☐Disable	☐Enable	Packets per sec. 0~700	
PING of death	☐Disable	☐Enable		
Land	☐Disable	☐Enable		
IP_spoofing	☐Disable	☐Enable		
Smurf	☐Disable	☐Enable		
Fraggle	☐Disable	☐Enable		

10.16.10 IP QoS

The Internet has worked so far with a best effort traffic model: every packet is treated (forwarded or discarded) equally. This is very simple and efficient model and several arguments have been stated against any need for a more complicated system.

To configure IP QoS , move the cursor " >> " to **ip_qos** and press enter.

```
>> active              Trigger IP QoS function
   add                 Add IP QoS policy
   delete              Delete IP QoS policy
   modify              Modify IP QoS policy
   list                Show IP QoS policy table
-------------------------------------------------------------------------
```

You can enable the IP QoS function via **active** command.

The add parameters of IP QoS can be configured via **add** command

To delete the policy is configured by **delete** command.

To modify the policy is configured by **modify** command.

You can view the IP QoS configuration via **list** command.

When use the **add** command, it will show the following:

```
-------------------------------------------------------------------------------------------------
>> Protocol          Configure protocol
   local_ip          Configure local IP parameter
   remote_ip         Configure remote IP parameter
   Port              Configure port parameter
   description       Policy description
   Enable            Enable the policy
   Precedence        Configure precedence parameter
-------------------------------------------------------------------------------------------------
```

Protocol identifier: One can differentiate IP from other network level protocols using link level information - TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Source port number: The only way to identify applications run over TCP or UDP is to look for port numbers and compare them to the list of well-known port numbers. While in most cases the mapping is correct, there are cases when some services or clients use a port reserved for another application.

Destination port number: The destination port identifies traffic originating from the client to the server.

Source host address: It can identify the end system sending data and based on that classify traffic

Destination host address: It can identify the end system receiving data.

Command	Description
Protocol	Set up the port protocol type (ANY, TCP or UDP)
Local_ip	Configure the local IP address
Remote_ip	Configure the remote IP address
Port	Configure the local port and remote port range
Description	Define the description of policy
Enable	Enable the policy
Precedence	Define the priority of the policy

IP QoS:

Protocol	☐ANY ☐TCP ☐UDP
Local IP	
Remote IP	
Local Port	
Remote Port	
Description	
Enable	☐ON ☐OFF
Precedence	(0 ~ 5)

10.16.11 DHCP

Dynamic Host Configuration Protocol (DHCP) is a communication protocol that lets network administrators to manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer. If computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator to supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

To configure DHCP server, move the cursor " >> " to **dhcp** and press enter.

```
>> generic          DHCP server generic parameters
   fixed            DHCP server fixed host IP list
   relay            DHCP relay parameter
   list             Show DHCP configuration
```

10.16.11.1 DHCP Server generic

The generic DHCP parameters can be configured via **generic** command.

```
>> active           Trigger DHCP server function
   gateway          Default gateway for DHCP client
   netmask          Subnet mask for DHCP client
   ip_range         Dynamic assigned IP address range
   lease_time       Configure max lease time
   name_server1     Domain name server1
   name_server2     Domain name server2
   name_server3     Domain name server3
```

Command	Description
Active	Trigger DHCP server function

Gateway	Configure default gateway for DHCP client
Net mask	Configure subnet mask for DHCP client
IP range	Configure dynamic assigned IP address range.
Lease time	Set up dynamic IP maximum lease time
Name server 1	Set up the IP address of name server #1
Name server 2	Set up the IP address of name server #2
Name server 3	Set up the IP address of name server #3

DHCP Server:

DHCP Server	☐Disable ☐Enable
DHCL Client gateway	
DHCP Client Netmask	
Start IP address	
Address Range	
Lease Time	
Name Server 1 IP	
Name Server 2 IP	
Name Server 3 IP	

10.16.11.2 DHCP Server Fixed Host

Fixed Host IP Address list are setup via **fixed** command.

```
>> add              Add a fixed host entry
   delete           Delete a fixed host entry
```

When use the fixed host entry, you must enter the MAC address and IP address at the same time. Up to 10 maximum fixed host IP addresses can be configured.

DHCP Server with Fixed Host:

	Mac Address	IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

10.16.11.3 DHCP Relay

Active the DHCP relay and remote server IP address via **relay** command

```
Command: setup dhcp relay <Disable|Enable> <ip>
Message: Please input the following information.

Parameter of command 'relay' (TAB Select) <Disable>: Enable
IP address (ENTER for default) <192.168.0.124>:
```

DHCP Relay:

DHCP Relay	□Disable □Enable
IP Address	

You can view the full DHCP configuration via **list** command.

10.16.11.4 DNS Proxy

The Domain Name Service (DNS) is a system designed to allow the identification of Internet servers to be based on names rather than IP addresses. Because Internet communication is based on IP addresses, all names must be translated into an IP address. This is the purpose of a Domain Name Server.
Enter the IP address of DNS proxy use DNS proxy command. Move cursor " >> " to **dns_proxy** and press enter.

```
------------------------------------------------------------------------
Command: setup dns_proxy <IP> [IP] [IP]
Message: Please input the following information.

DNS server 1 (ENTER for default) <168.95.1.1>: 10.0.10.1
DNS server 2: 10.10.10.1
DNS server 3:
------------------------------------------------------------------------
```

You can setup three DNS servers in the router. The number 2 and 3 DNS servers are option.

DNS Server IP:

DNS Server 1 IP	
DNS Server 2 IP	
DNS Server 3 IP	

10.16.12 Host name

A Host Name is the unique name by which a network-attached. The hostname is used to identify a particular host in various forms of electronic communication.

Enter local host name via hostname command. Move cursor " **>>** " to **hostname** and press enter.

```
------------------------------------------------------------------------
Command: setup hostname <name>
Message: Please input the following information.

Local hostname (ENTER for default) <SOHO>: test
------------------------------------------------------------------------
```

The host name can't use more than 15 characters and don't use space character.

Some of the ISP requires the Host Name as identification. You may check with ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

Host Name:

Host Name	

10.16.13 Default

If you want to restore factory default, first move the cursor " >> " to **default** and then press enter.

```
------------------------------------------------------------------------
Command: setup default <name>
```

Message: Please input the following information.

Are you sure? (Y/N): **y**

Press "y" to confirm the restore factory setting operation.

EC Declaration of Conformity

For the following equipment:

*Type of Product : G.shdsl Bridge Router
*Model Number : GRT-101, GRT-401
* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address : 11F, No. 96, Min Chuan Road, Hsin Tien
Taipei, Taiwan , R. O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (89/336/EEC).
For the evaluation regarding the EMC, the following standards were applied:

Emission	EN 55022	(1994 /A1:1995 /A2:1997)
Harmonic	EN 61000-3-2	(1995 /A1:1998 /A2:1998 / A14: 2000)
Flicker	EN 61000-3-3	(1995)
Immunity	EN 55024	(1998)
ESD	IEC 61000-4-2	(1995/A1:1998)
RS	IEC 61000-4-3	(1996/A1:1998)
EFT/ Burst	IEC 61000-4-4	(1995)
Surge	IEC 61000-4-5	(1995)
CS	IEC 61000-4-6	(1996)
Magnetic Field	IEC 61000-4-8	(1993)
Voltage Disp	IEC 61000-4-11	(1994)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Tom Shih**

Position / Title : **Product Manager**

Taiwan	**18, Nov., 2002**	
Place	*Date*	*Legal Signature*

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw
11F, No. 96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528

EC Declaration of Conformity

For the following equipment:

*Type of Product : G..SHDSL Router
*Model Number : GRT-402

* Produced by:
Manufacturer's Name: **Planet Technology Corp.**
Manufacturer's Address: 11F, No. 96, Min Chuan. Road, Hsin Tien
Taipei, Taiwan , R.O.C.

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/336/EEC, Amended by 92/31/EEC, 93/68/EEC & 98/12/EC).
For the evaluation regarding the Electromagnetic Compatibility, the following standards were applied:

Emission	EN 55022	(1994 + A1:1995 + A2:1997 Class A)
Harmonic	EN 61000-3-2	(2000)
Flicker	EN 61000-3-3	(1995 + A1:2001)
Immunity	EN 55024	(1998 + A1:2001 + A2:2003)
ESD	EN 61000-4-2	(2001)
RS	EN 61000-4-3	(2002)
EFT/ Burst	EN 61000-4-4	(1995 + A1:2000 + A2:2001)
Surge	EN 61000-4-5	(2001)
CS	EN 61000-4-6	(2001)
Magnetic Field	IEC 61000-4-8	(2001)
Voltage Disp	EN 61000-4-11	(2001)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Tom shih**

Position / Title : **Product Manager**

Taiwan	**11th Mar., 2004**	
Place	*Date*	*Legal Signature*

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw
11F, No. 96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528