4-Wire G.SHDSL.bis Firewall Router

GRT-504

User's Manual

Copyright

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.
PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.
Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.
If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

Trademarks

CE mark Warning

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

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 (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.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

WEEE Caution

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 and have to collect such WEEE separately.

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.

Customer Service

For information on customer service and support for the Multi-Homing Security Gateway, please refer to the following Website URL:

http://www.planet.com.tw

Before contacting customer service, please take a moment to gather the following information:

- The GRT-504 serial number and MAC address
- Any error messages that displayed when the problem occurred
- Any software running when the problem occurred
- Steps you took to resolve the problem on your own

Revision

User's Manual for PLANET 4-Wire G.SHDSL.bis Firewall Router

Model: GRT-504

Rev: 1.0 (Sep. 2008)

Port No. EM-GRT504v1

Table of Contents

1 Descriptions

The Planet new SHDSL family member GRT-504 is the G.SHDSL.bis router that complies with ITU-T G.991.2 standard and provides affordable, flexible, efficient Internet access solution for SOHO and Small Medium Business environment. The GRT-504 supports business-class, multi-range from 384 Kbps to 11.4 Mbps (4-wire) symmetric data rates and also can be connected as the LAN-to-LAN network connection at the distance up to 6.7km (4.2 miles) by using existing telephone copper wires.

The Planet GRT-504 is integrated high-end Bridging/Routing capabilities with advanced functions of Firewall, QoS, DMZ, Virtual Server, and VPN pass-through. And because of the network environment growing rapidly, Virtual LAN has become more and more important feature in internetworking industry. The GRT-504 supports IEEE 802.1Q and port-based VLAN over ATM network.

With the built-in Simple Network Management Protocol (SNMP) and web-based management, the GRT-504 offers an easy-to-use, platform-independent management and configuration facility. And the GRT-504 also provides Command-Line Interface; it can be accessed via Telnet and the console port. The network administrator can manage the device by proper way.

1.1 Features

- **High Speed Symmetric Data Transmission**：The GRT-504 supports the latest G.SHDSL.bis technology, provides the higher symmetric data rate up to 11.4 Mbps on 4 wires.
- **CO and CPE side Support**：Provide the back-to-back connection.
- **Firewall:** It supports Natural NAT firewall and Advanced Stateful packet Inspection (SPI) firewall functions.
- **QoS (Quality of Service):** The GRT-504 supports ATM QoS and IP QoS. The ATM QoS includes UBR (Unspecified bit rate), CBR (Constant bit rate), VBR-rt (Variable bit rate real-time), and VBR-nrt (Variable bit rate non-real-time). Also, the traffic classification based on IP, IP range, port, protocol, and precedence.
- **VLAN Support**：It supports the IEEE 802.1Q Tagged and port-based VLAN. It offers significant benefit in terms with efficient use of bandwidth, flexibility, performance, and security.
- **Bridge and Router Modes**：The GRT-504 supports two connection modes. Currently, it comes pre-configured with routing mode. Note that, routing mode and bridging mode cannot be used simultaneously.
- **Virtual Server**：This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **VPN Pass through Support**：PCs with VPN (Virtual Private Networking) software using PPTP, L2TP, and IPSec are transparently supported - no configuration is required.
- **DMZ Support**：The GRT-504 can translate public IP address to private IP address to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the most flexibility to run programs, which could be incompatible in NAT environment.
- **RIPv1/v2 Routing**：It supports RIPv1/v2 routing protocol for routing capability.

- **Simple Network Management Protocol (SNMP)**：It is an easy way to remotely manage the router via SNMPv1/v2.
- **Fully ATM protocol stack implementation over G.SHDSL.bis**
- **PPPoA and PPPoE support user authentication with PAP/CHAP/MS-CHAP**

1.2 Specification

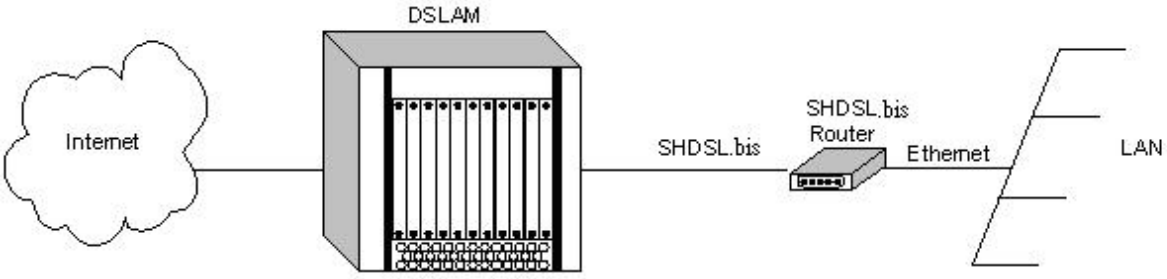
Product	4-Wire G.SHDSL.bis Firewall Router
Model	GRT-504
Hardware	
Standard	Compliant with ITU-T G.991.2 Standard Annex A/B Compliant with G.SHDSL.bis Annex A/B/F/G TC-PAM Line Code Symmetric data transmission speed up to 11.4 Mbps on 4-wire Multi-range from 384 Kbps to 11.4 Mbps
Protocol	RFC 1577 - Classical IP over ATM (RFC 1577) RFC 2364 - PPP over ATM RFC 1483/2684 - Ethernet over ATM RFC 2516 - PPP over Ethernet (fixed and dynamic IP) RFC 2364 - PPP over ATM (fixed and dynamic IP)
AAL and ATM Support	Support up to 8 PVCs ATM Forum UNI 3.1/4.0 PVC Support OAM F4 / F5 AIS/RDI and loopback VC multiplexing and SNAP/LLC Integrated ATM QoS support (UBR,CBR,VBR-rt, and VBR-nrt)
LAN Port	4 x 10Base-T/100Base-TX (Auto-Negotiation, Auto MDI/MDI-X)
Console	1 x RS-232 (DB9)
Button	1 x Reset Button
LED Indicators	PWR, WAN LNK/ACT, LAN 1/2/3/4, ALM
Software	
Maximum Concurrent Sessions	1024
Protocol and Advanced Functions	IEEE 802.1D transparent learning bridge IEEE 802.1Q VLAN Support IP/TCP/UDP/ARP/ICMP/IGMP protocols IP routing with static routing and RIPv1/RIPv2 IP multicast and IGMP proxy Network address translation (NAT/PAT) DMZ host/Multi-DMZ/Multi-NAT function Virtual Server (RFC1631) DNS relay and caching DHCP server, client and relay IP QoS
Security	Built-in NAT and SPI Firewall PPP over PAP (RFC1334) PPP over CHAP (RFC1994) Password protection for system management
VPN	VPN (PPTP/L2TP/IPSec) pass-through
Management	Web-based configuration Command-line Interpreter(CLI) via Console Command-line Interpreter(CLI) via Telnet Software upgrade via web-browser/TFTP server SNMPv1 and v2
Environment Specification	
Dimension (W x D x H)	145 x 188 x 33mm
Power	9V DC, 1A
Temperature: **Humidity**	Operating: 0~45 degree C, 0%~ 90% (non-condensing), Storage: -10~70 degree C, 0~95% (non-condensing)
Emission	FCC, CE

Package Contents

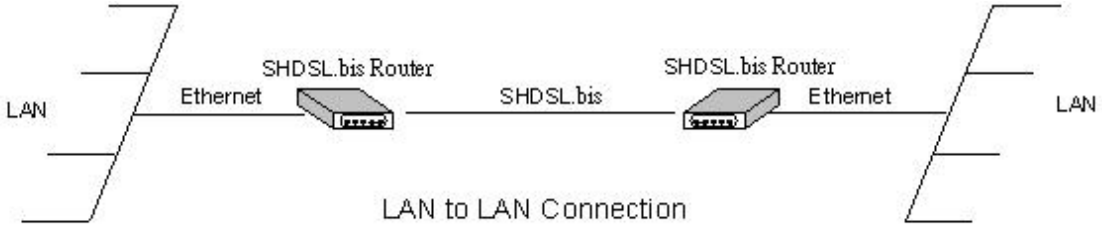
The following items should be included. If any of these items are damaged or missing, please contact your dealer immediately.

- 4-Wire G.SHDSL.bis Firewall Router x 1
- Power Adapter x 1
- Quick Installation Guide x 1
- User's manual CD x 1
- Console Cable x 1
- RJ-45 to RJ-11 Cable x 1

1.3 Applications



Connection with DSLAM



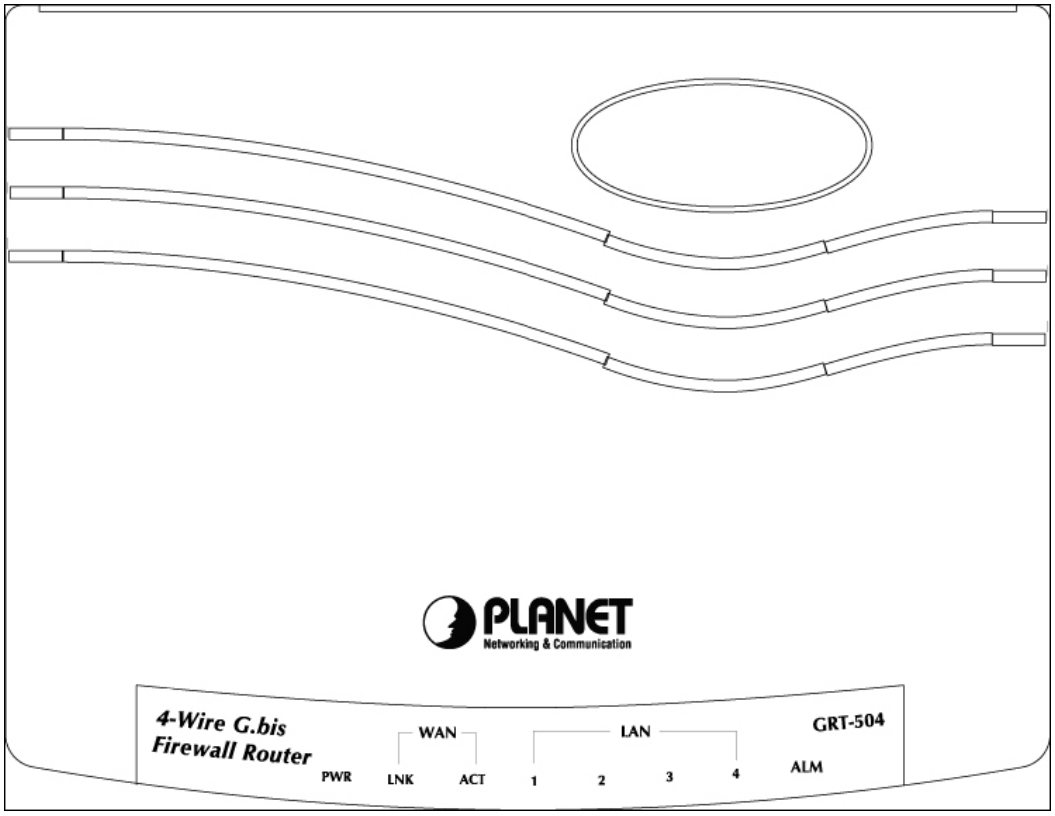
LAN to LAN Connection

2 Getting to know about the router

This section will introduce hardware of the router.

2.1 Front Panel

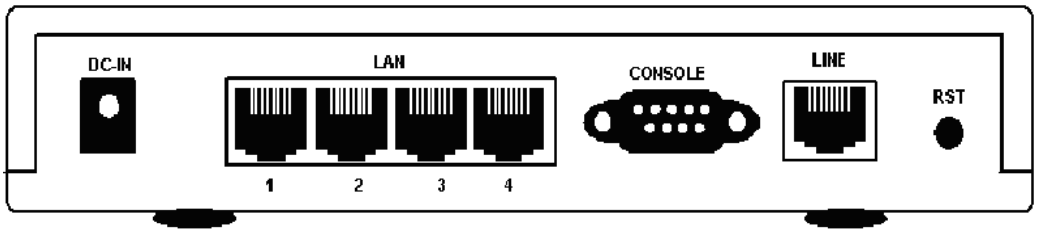
The front panel contains LEDs which show status of the router.



LEDs		Color	Active	Description
PWR		Green	ON	The power adaptor is connected to GRT-504
WAN	LNK	Green	ON	G.SHDSL.bis connection is established
		Green	Blink	G.SHDSL.bis is handshaking
	ACT	Green	Blink	Transmit data or receive data over G.SHDSL.bis link
LAN	1 / 2 / 3 / 4	Green	ON	LAN Port connect with Ethernet link
	1 / 2 / 3 / 4	Green	Blink	LAN Port Transmit or receive data
ALM		Red	ON	G.SHDSL.bis line connection is dropped
		Red	Blink	G.SHDSL.bis self test

2.2 Rear Panel

The rear panel of SHDSL.bis router is where all of the connections are made.



Port	Description
DC-IN	Power connector with 9V DC 1.0A
LAN (1 / 2 / 3 / 4)	Ethernet 10/100Base-TX for LAN port (RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	G.SHDSL.bis interface for WAN Port
RST	The reset button, the router restore the default settings when press this button until reboot.

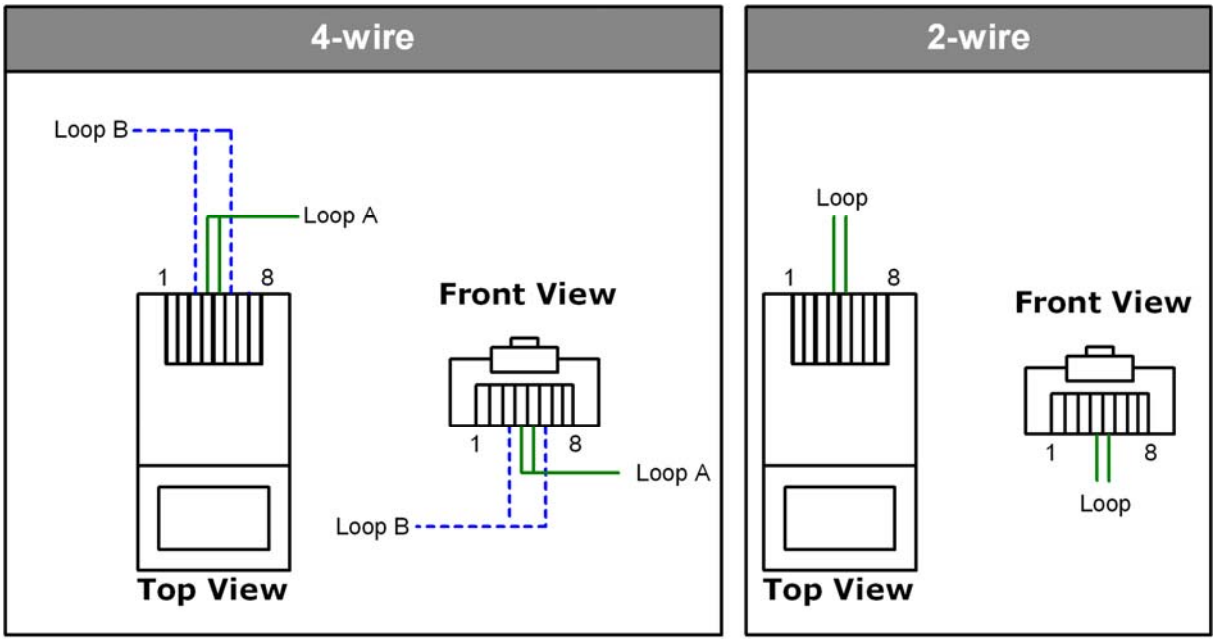
The reset button can be used only in one of two ways.

(1) Press the Reset Button for one second will cause system reboot.

(2) Pressing the Reset Button for four seconds will cause the product loading the factory default setting and losing all of yours configuration. When you want to change its configuration but forget the user name or password, or if the product is having problems connecting to the Internet and you want to configure it again clearing all configurations, press the Reset Button for four seconds with a paper clip or sharp pencil.

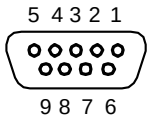
2.3 SHDSL.bis Line Connector

Below figure show the SHDSL.bis line cord plugs pin asignment:



2.4 Console Cable

Below figure show the cosole cable pins asignment:

Pin Number	Description	Figure
1	No connection	
2	RxD (O)	
3	TxD (I)	
4	No connection	
5	GND	
6	No connection	
7	CTS (O)	
8	RTS (I)	
9	No connection	

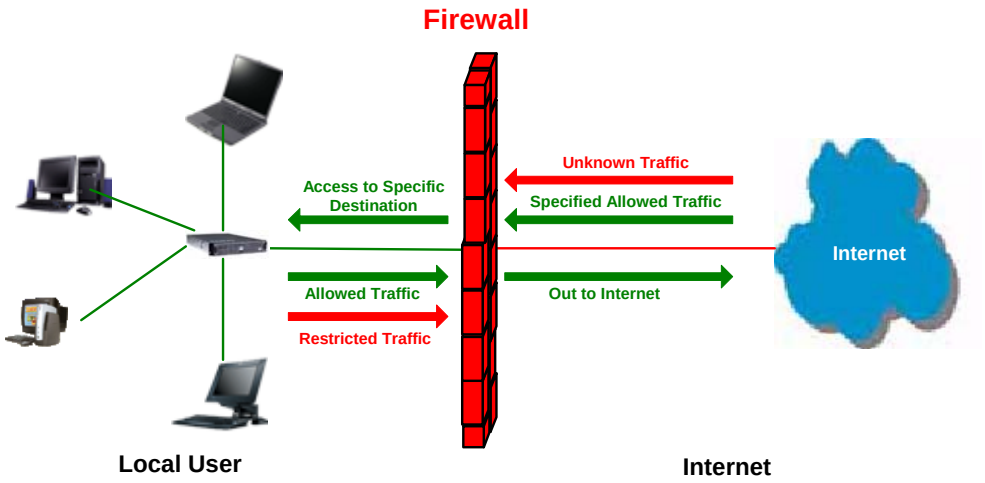
3 Getting to know Firewall feature

3.1 Introduction

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.

A firewall examines all traffic routed between the networks. The traffic is routed between the networks if it meets certain criteria; otherwise, it is filtered. A firewall filters both inbound and outbound traffic. Except managing the public access to private networked resources such as host applications, the firewall is capable of log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their IP addresses of source and destination. This is known as address filtering. Firewalls can also filter specific types of network traffic by port numbers, which is also known as protocol filtering because the decision of traffic forwarding is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

An Internet firewall cannot prevent the damage from the individual users with router dialing into or out of the network, which bypass the firewall altogether. The misconduct or carelessness of employee is not in the control of firewalls either. Authentication Policies, which is involved in the use and misuse of passwords and user accounts, must be strictly enforced. The above management issues need to be settled during the planning of security policy, but cannot be solved with Internet firewalls alone.

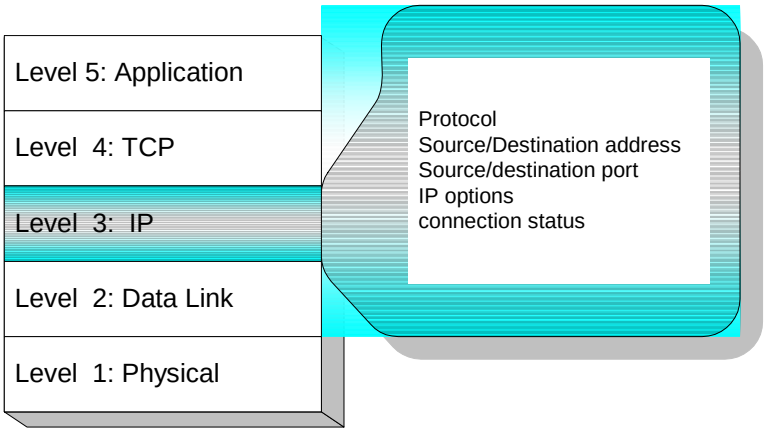


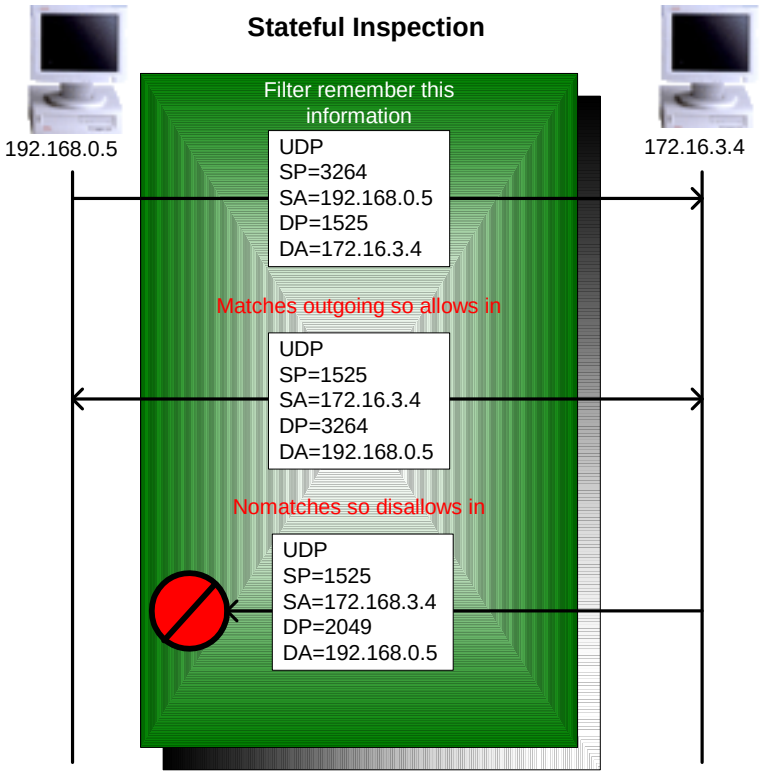
3.2 Types of Firewall

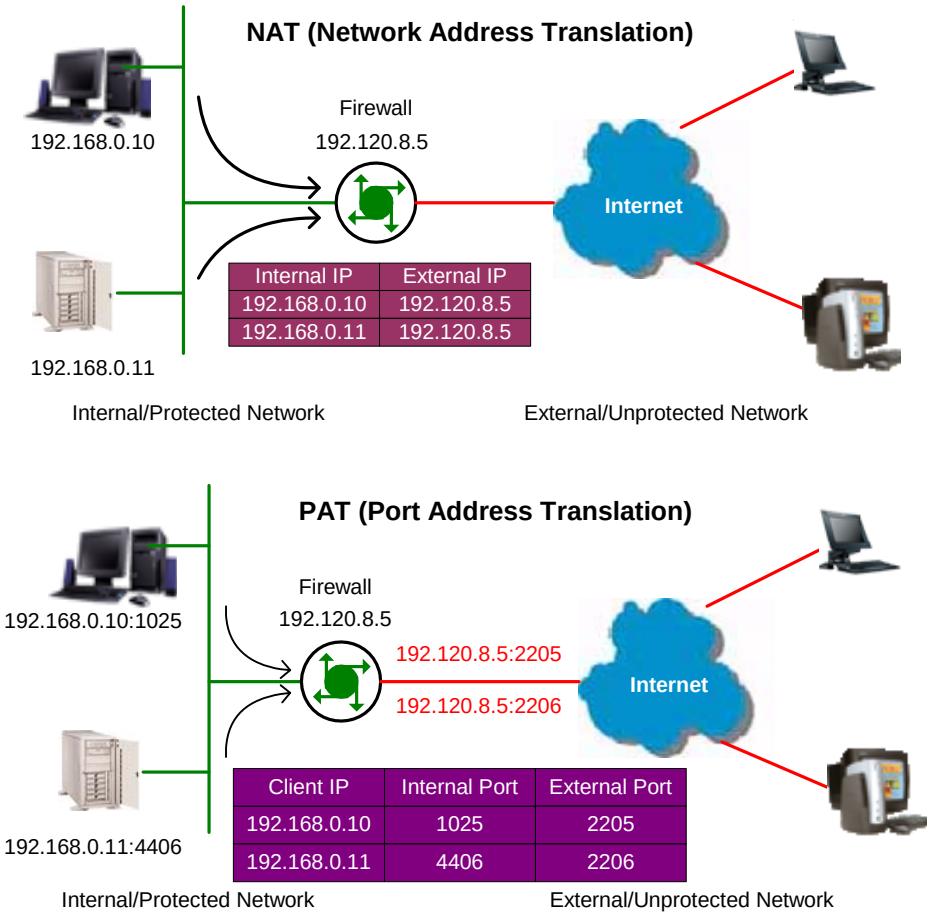
There are three types of firewall:

3.2.1 Packet Filtering

In packet filtering, firewall will examine the protocol and the address information in the header of each packet and ignore its contents and context (its relation to other packets and to the intended application). The firewall pays no attention to applications on the host or local network and it "knows" nothing about the sources of incoming data. Filtering includes the examining on incoming and outgoing packets, and determines the packet dropping or not by a set of configurable rules. Network Address Translation (NAT) routers offer the advantages of packet filtering firewalls but can also hide the IP addresses of computers behind the firewall, and offer a level of circuit-based filtering.

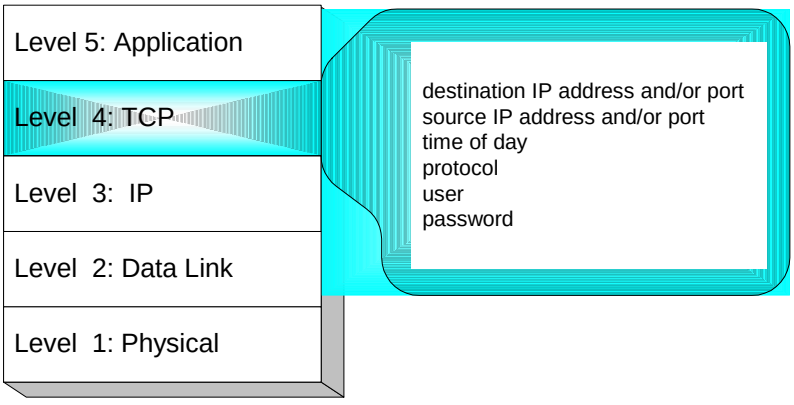






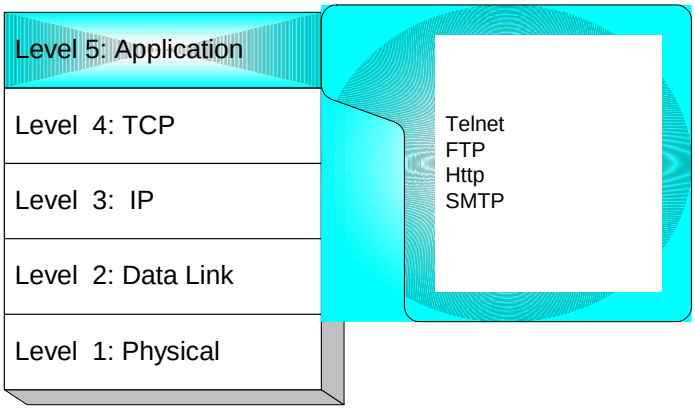
3.2.2 Circuit Gateway

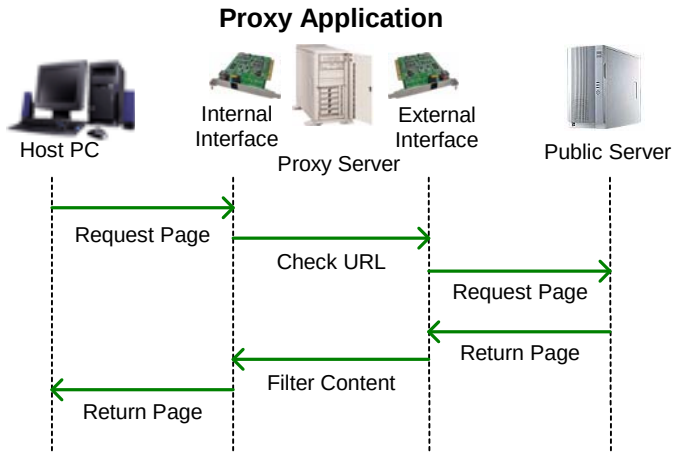
Also called a "Circuit Level Gateway," this is a firewall approach, which validates connections before allowing data to be exchanged. What this means is that the firewall doesn't simply allow or disallow packets but also determines whether the connection between both ends is valid according to configurable rules, then opens a session and permits traffic only from the allowed source and possibly only for a limited period of time.



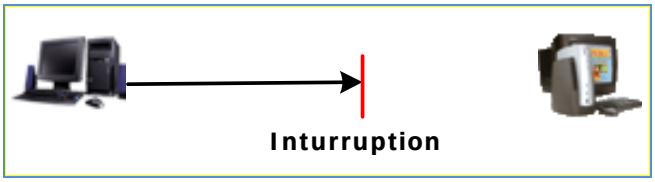
3.2.3 Application Gateway

The Application Level Gateway acts as a proxy for applications, performing all data exchanges with the remote system in their behalf. This can render a computer behind the firewall invisible to the remote system. It can allow or disallow traffic according to very specific rules, for instance permitting some commands to a server but not others, limiting file access to certain types, varying rules according to authenticated users and so forth. This type of firewall may also perform very detailed logging of traffic and monitoring of events on the host system; furthermore can often be instructed to sound alarms or notify an operator under defined conditions. Application-level gateways are generally regarded as the most secure type of firewall. They certainly have the most sophisticated capabilities.



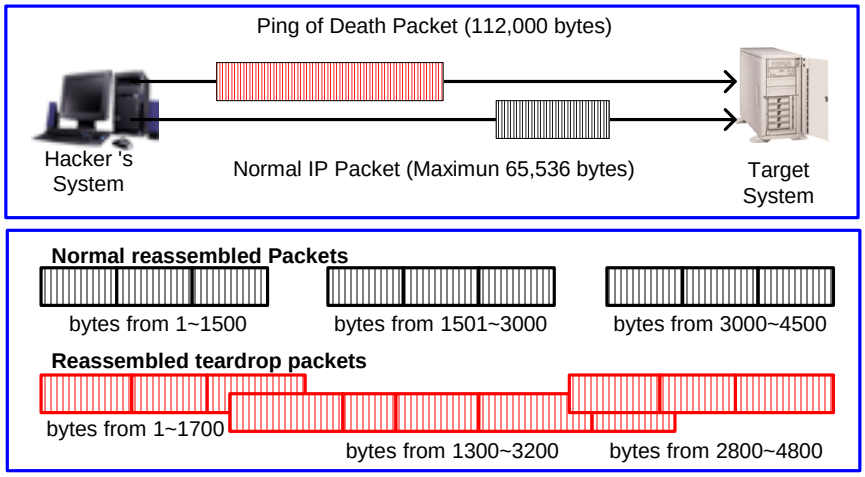


3.3 Denial of Service Attack

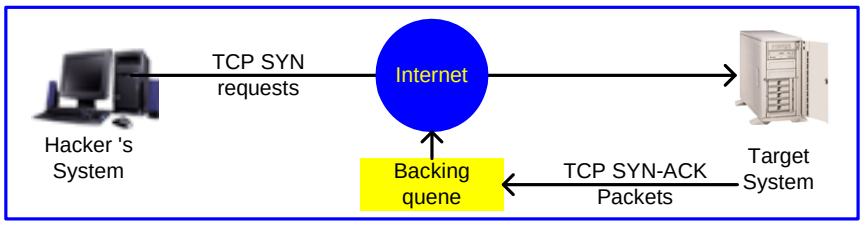


Typically, Denial of Service (DoS) attacks result in two flavors: resource starvation and system overloading. DoS attacks happen usually when a legitimate resource demanding is greater than the supplying (ex. too many web requests to an already overloaded web server). Software weakness or system incorrect configurations induce DoS situations also. The difference between a malicious denial of service and simple system overload is the requirement of an individual with malicious intent (attacker) using or attempting to use resources specifically to deny those resources to other users.

Ping of death- On the Internet, ping of death is a kind of denial of service (DoS) attack caused by deliberately sending an IP packet which size is larger than the 65,536 bytes allowed in the IP protocol. One of the features of TCP/IP is fragmentation, which allows a single IP packet to be broken down into smaller segments. Attackers began to take advantage of that feature when they found that fragmented packets could be added up to the size more than the allowed 65,536 bytes. Many operating systems don't know what to do once if they received an oversized packet, then they freeze, crash, or reboot. Other known variants of the ping of death include teardrop, bonk and nestea.



SYN Flood- The attacker sends TCP SYN packets, which start connections very fast, leaving the victim waiting to complete a huge number of connections, causing it to run out of resources and dropping legitimate connections. A new defense against this is the "SYN cookies". Each side of a connection has its own sequence number. In response to a SYN, the attacked machine creates a special sequence number that is a "cookie" of the connection then forgets everything it knows about the connection. It can then recreate the forgotten information about the connection where the next packets come in from a legitimate connection.



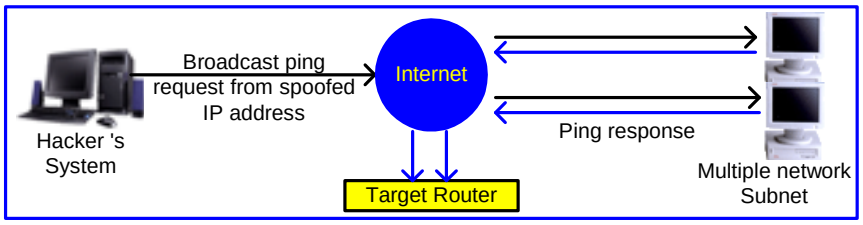
ICMP Flood- The attacker transmits a volume of ICMP request packets to cause all CPU resources to be consumed serving the phony requests.

UDP Flood- The attacker transmits a volume of requests for UDP diagnostic services, which cause all CPU resources to be consumed serving the phony requests.

Land attack- The attacker attempts 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 source address of the intended victim is forged in a broadcast ping so that a huge number of ICMP echo reply back to victim indicated by the address, overloading it.



Fraggle Attack- A perpetrator sends a large amount of UDP echo packets at IP broadcast addresses, all of it having a fake source address.

4 Getting to know VLAN feature

Virtual Local Area Network (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.

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. VLAN architecture benefits include:

1. Increased performance
2. Improved manageability
3. Network tuning and simplification of software configurations
4. Physical topology independence
5. Increased security options

As DSL (over ATM) links are deployed more and more extensively and popularly, it is rising progressively to implement VLAN (VLAN-to-PVC) over DSL links and, hence, it is possible to be a requirement of ISPs.

We discuss 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.

4.1 Specification

1. The unit supports up to 8 active VLANs with shared VLAN learning (SVL) bridge out of 4096 possible VLANs specified in IEEE 802.1Q.
2. Each port always belongs to a default VLAN with its port VID (PVID) as an untagged member. Also, a port can belong to multiple VLANs and be tagged members of these VLANs.
3. A port must not be a tagged member of its default VLAN.
4. If a non-tagged or null-VID tagged packet is received, it will be assigned with the default PVID of the ingress port.
5. If the packet is tagged with non-null VID, the VID in the tag will be used.
6. The look up process starts with VLAN look up to determine whether the VID is valid. If the VID is not valid, the packet will be dropped and its address will not be learned. If the VID is valid, the VID, destination address, and source address lookups are performed.
7. The VID and destination address lookup determines the forwarding ports. If it fails, the packet will be broadcasted to all members of the VLAN, except the ingress port.
8. Frames are sent out tagged or untagged depend on if the egress port is a tagged or untagged member of the VLAN that frames belong.
9. If VID and source address look up fails, the source address will be learned.

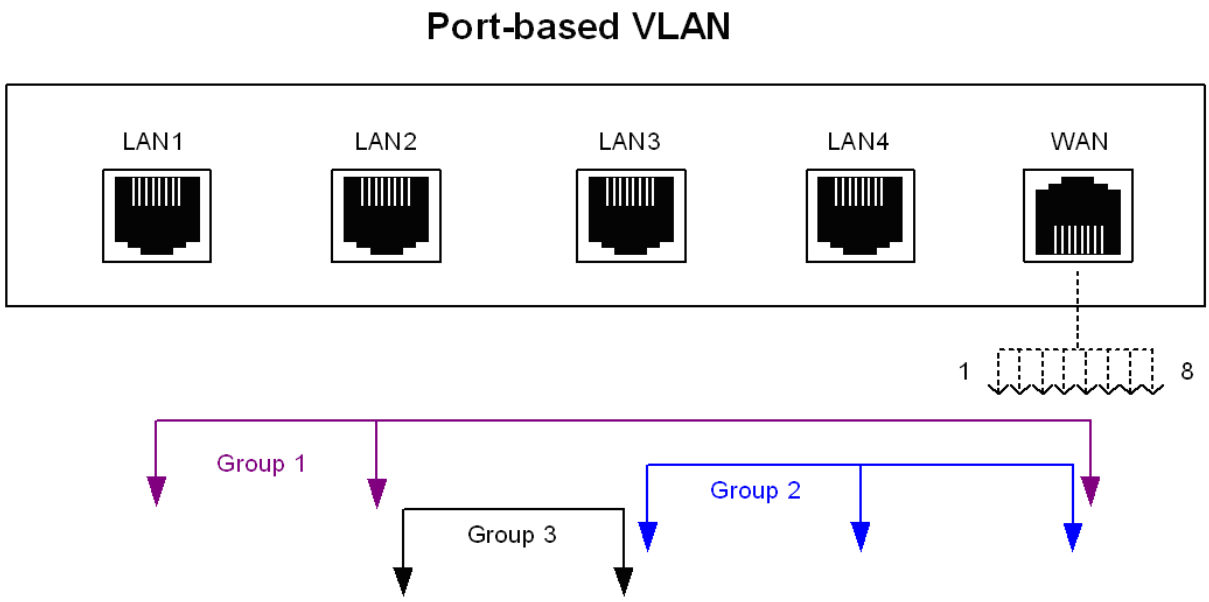
4.2 Frame Specification

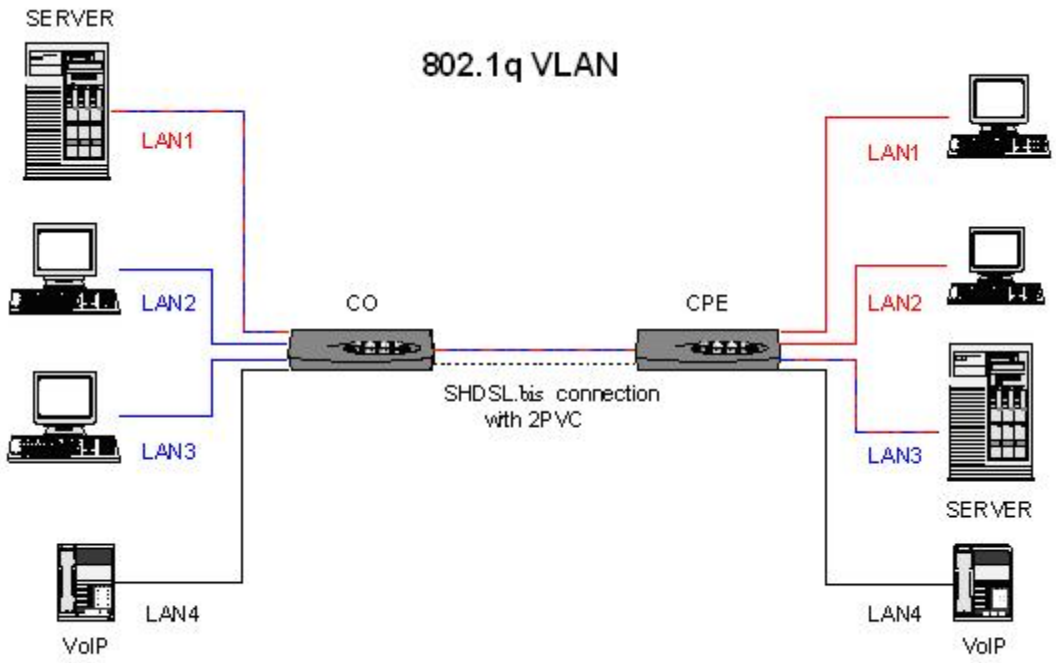
An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. Such frames are classified as belonging to a particular VLAN based on parameters associated with the receiving port. Also, priority tagged frames, which, by definition, carry no VLAN identification information, are treated the same as untagged frames.
A VLAN-tagged frame carries an explicit identification of the VLAN to which it belongs; i.e., it carries a tag header that carries a non-null VID. This results in a minimum tagged frame length of

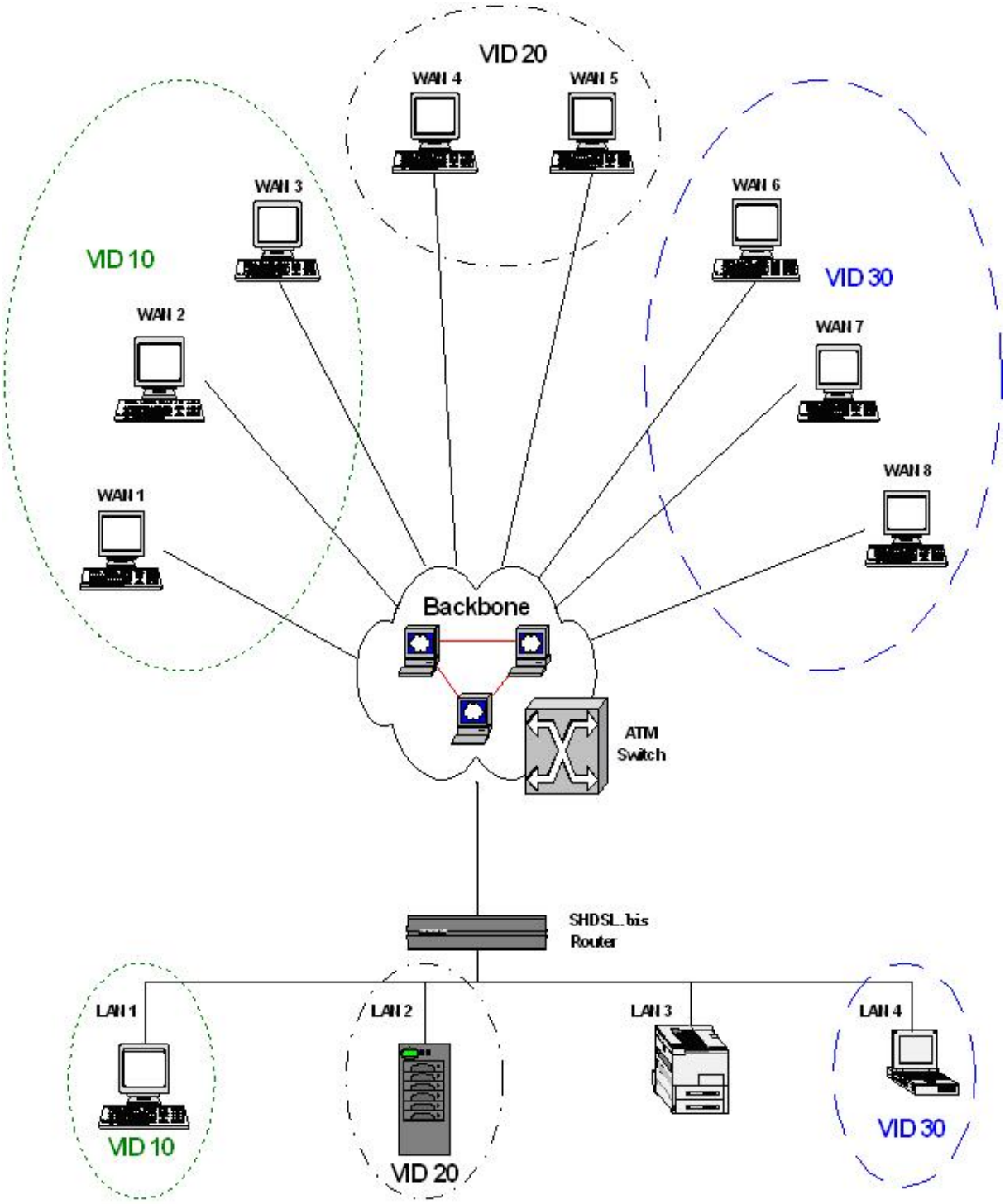
68 octets. Such a frame is classified as belonging to a particular VLAN based on the value of the VID that is included in the tag header. The presence of the tag header carrying a non-null VID means that some other device, either the originator of the frame or a VLAN-aware bridge, has mapped this frame into a VLAN and has inserted the appropriate VID.

The following figure shows the difference between a untagged frame and VLAN tagged frame, where the Tag Protocol Identifier (TPID) is of 0x8100 and it identifies the frame as a tagged frame. The Tag Control Information (TCI) consists of the following elements: 1) User priority allows the tagged frame to carry user priority information across bridged LANs in which individual LAN segments may be unable to signal priority information (e.g., 802.3/Ethernet segments). 2) The Canonical Format Indicator (CFI) is used to signal the presence or absence of a Routing Information Field (RIF) field, and, in combination with the Non-canonical Format Indicator (NCFI) carried in the RIF, to signal the bit order of address information carried in the encapsulated frame. 3) The VID uniquely identifies the VLAN to which the frame belongs.

4.3 Applications




SERVER
802.1q VLAN
LAN1
LAN2
LAN3
LAN4
VoIP
CO
CPE
SHDSL.bis connection
with 2PVC
LAN1
LAN2
LAN3
SERVER
LAN4
VoIP


VID 20
WAN 4
WAN 5
WAN 3
VID 10
WAN 2
WAN 1
WAN 6
VID 30
WAN 7
WAN 8
Backbone
ATM
Switch
SHDSL.bis
Router
LAN 1
LAN 2
LAN 3
LAN 4
VID 10
VID 20
VID 30

5 Configuration to the Router

This guide is designed to let users through Web Configuration or serial console with G.shdsl.bis Router in the easiest and quickest way possible. Please follow the instructions carefully.

Note: There are three methods to configure the router: serial console, Telnet and Web Browser. Only one configuration application is used to setup the Router at any given time. Users have to choose one method to configure it.
For Web configuration, you can skip item 3.
For Serial Console Configuration, you can skip item 1 and 2.

5.1 Check List

(1) Check the Ethernet Adapter in PC or NB

Make sure that Ethernet Adapter had been installed in PC or NB used for configuration of the router. TCP/IP protocol is necessary for web configuration, so please check the TCP/IP protocol whether it has been installed.

(2) Check the Web Browser in PC or NB

According to the Web Configuration, the PC or NB need to install Web Browser, IE or Netscape. Note: Suggest to use IE5.0, Netscape 6.0 or above and 800x600 resolutions or above.

(3) Check the Terminal Access Program

For Serial Console and Telnet Configuration, users need to setup the terminal access program with VT100 terminal emulation.

(4) Determine Connection Setting

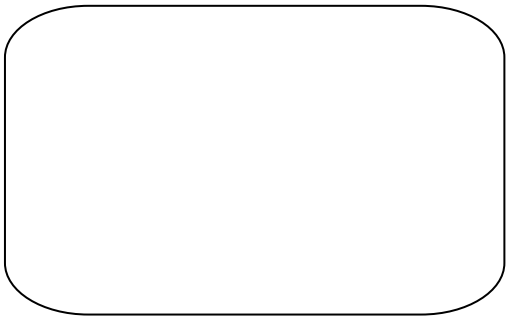
Users need to know the Internet Protocol supplied by your Service Provider and determine the mode of setting.

Protocol Selection

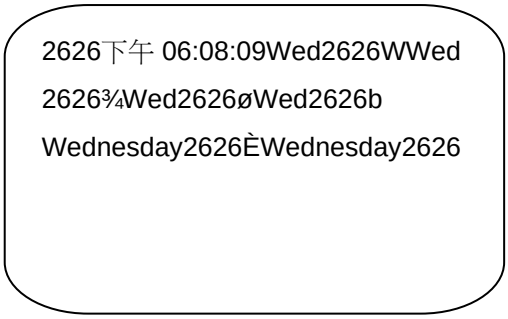
RFC1483	Ethernet over ATM
RFC1577	Classical Internet Protocol over ATM
RFC2364	Point-to-Point Protocol over ATM
RFC2516	Point-to-Point Protocol over Ethernet

The difference Protocols need to setup difference WAN parameters. After knowing the Protocol provided by ISP, you have to ask the necessary WAN parameters to setup it.

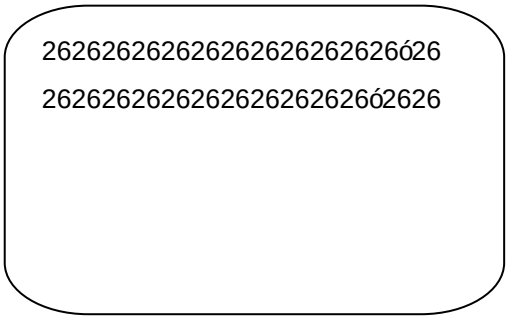
Bridge EoA



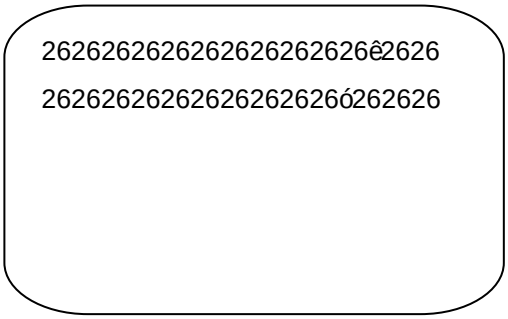
Route EoA



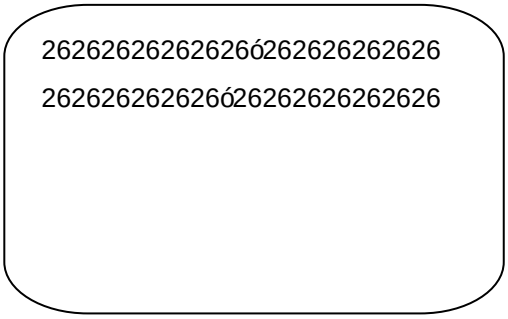
IPoA



PPPoA



PPPoE

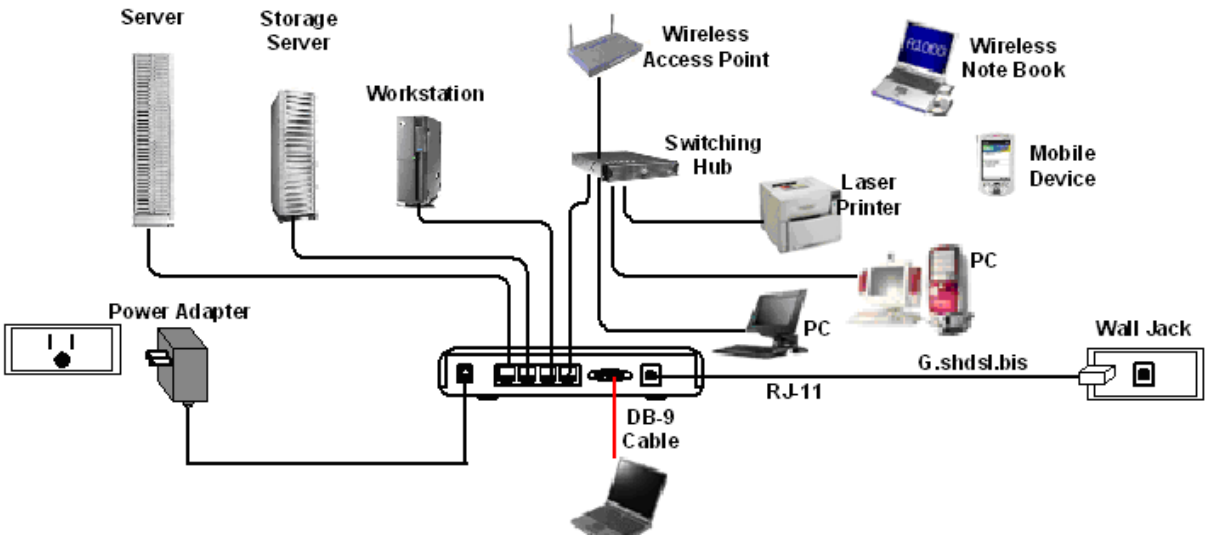


5.2 Install the SHDSL.bis Router

To avoid possible damage to this Router, do not turn on the router before Hardware Installation.

- Connect the power adapter to the port labeled DC-IN on the rear panel of the product.
- Connect the Ethernet cable.

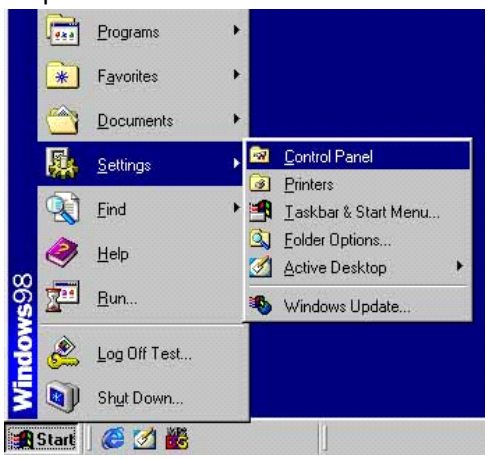
  Note: This router supports auto-MDIX switching so both straight through and cross-over Ethernet cable can be used.
- Connect the phone cable to the router and the other side of phone cable to wall jack.
- Connect the power adapter to power source inlet.
- Turn on the PC or NB, which is used for configuration the Router.



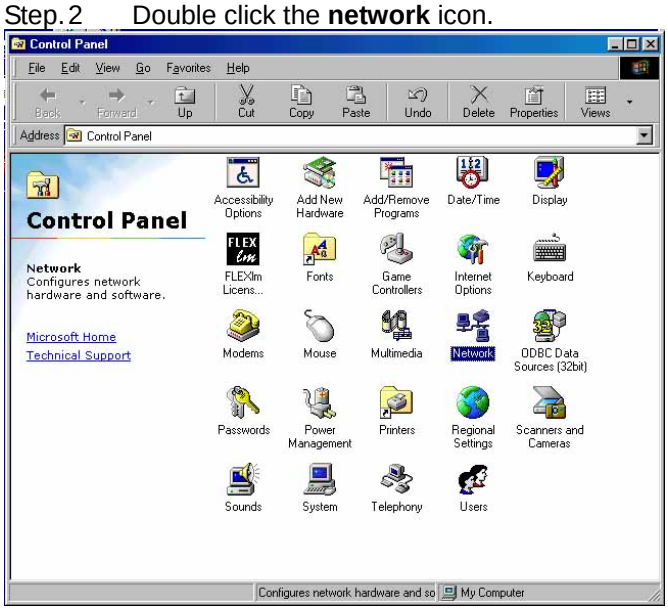
4-port router with complex network topology

6 Configuration via Web Browser

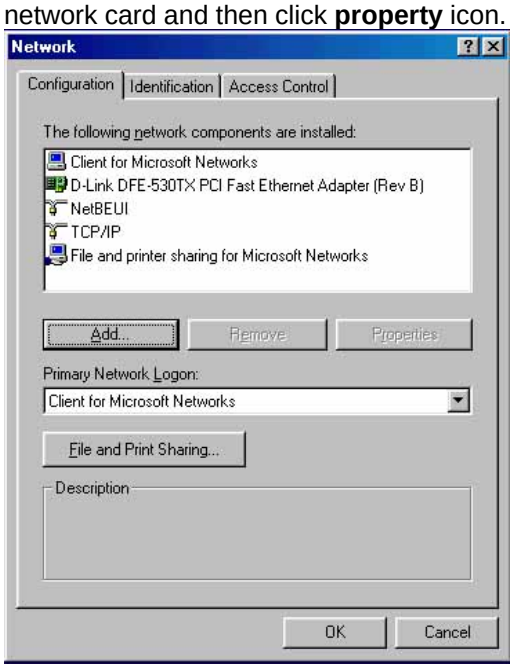
Step. 1 Click the **start** button. Select **setting** and **control panel**.



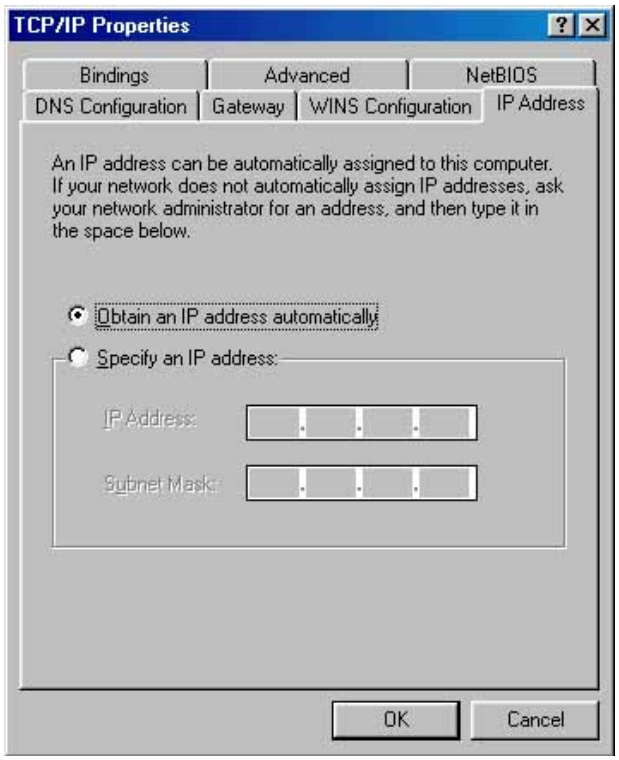
Step. 2 Double click the **network** icon.



In the Configuration window, select the **TCP/IP** protocol line that has been associated with your network card and then click **property** icon.



Choose IP address tab.
Select **Obtain IP address automatically**.
Click **OK** button.



The window will ask you to restart the PC. Click **Yes** button.

After rebooting your PC, open IE or Netscape Browser to connect the Router. Type

http://192.168.0.1

The default IP address and sub net-mask of the Router is 192.168.0.1 and 255.255.255.0. Because the router acts as DHCP server in your network, the router will automatically assign IP address for PC or NB in the network.

Type User Name root and Password root and then click OK.
The default user name and password both is *root*. For the system security, suggest changing them after configuration.

Note: After changing the User Name and Password, strongly recommend you to save them because another time when you login, the User Name and Password have to be used the new one you changed.

Function Listing

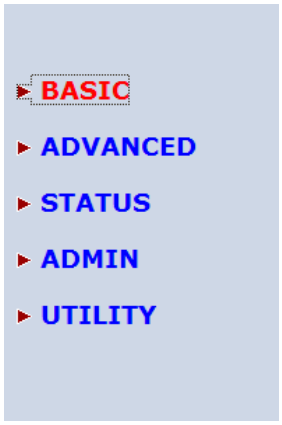
Following is the G.SHDSL.bis router full function listing.

- **BASIC (Quick Setup)**
- **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - STP
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- **STATUS**
  - SHDSL.bis
  - LAN
  - WAN
  - ROUTE
  - INTERFACE
  - FIREWALL
  - IP QoS
  - STP
- **ADMIN**
  - SECURITY
  - SNMP
  - TIME SYNC
- **UTILITY**
  - SYSTEM INFO
  - CONFIG TOOL
  - FIRMWARE UPGRADE
  - LOGOUT
  - RESTART

6.1 Basic Setup

The Basic Setup contains Bridge or Route operation mode. User can use it to completely setup the router. After successfully completing it, you can access Internet or as LAN extension. This is the easiest and possible way to setup the router.

Note: The advanced functions are only for advanced users to setup advanced functions. The incorrect setting of advanced function will affect the performance or system error, even disconnection.



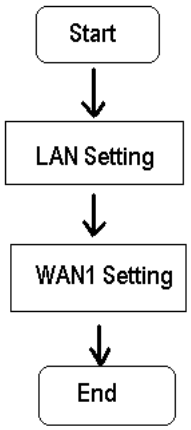
Click Basic for basic installation.

6.1.1 Bridge Mode

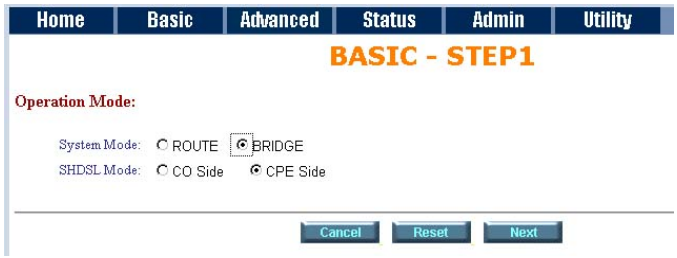
Parameter Table:

System mode	Bridge	
SHDSL	☐CO side ☐CPE side	
LAN	IP address	
	Subnet Mast	
	Gateway	
	Host Name	
WAN1	VPI	
	VCI	
	Encapsulation	☐VC-mux ☐LLC

The flow chart of bridge mode setup:

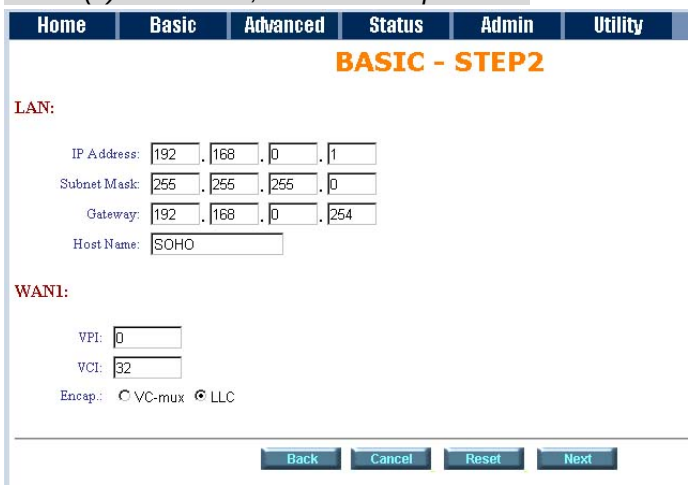


Setup up system mode and SHDSL mode



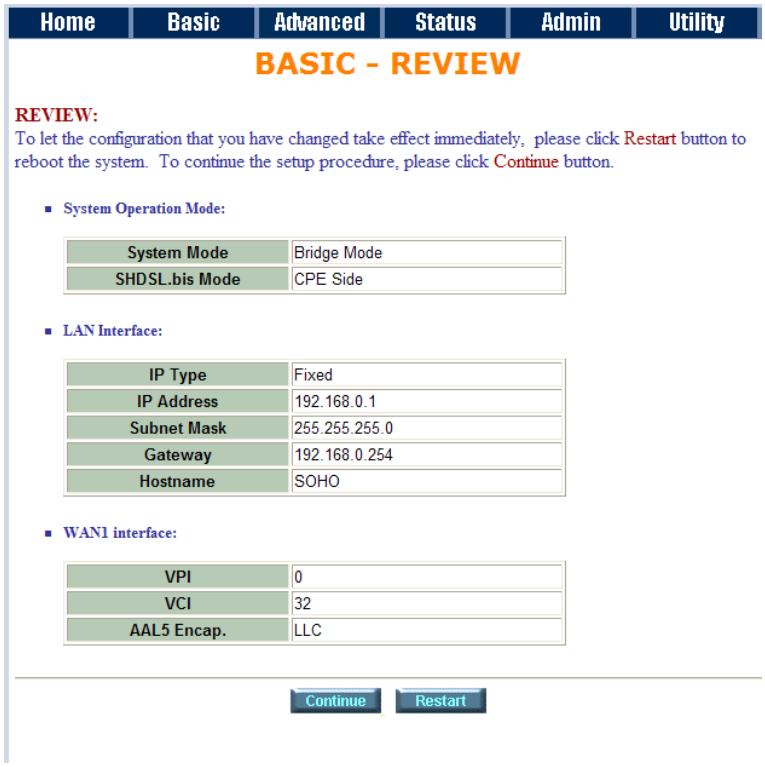
Click Bridge and CPE Side to setup Bridging mode and then click Next for the next setting. This router can be setup as one of two SHDSL.bis working mode: CO (Central Office) and CPE (Customer Premises Equipment). For connection with DSLAM, the SHDSL.bis router working mode is CPE. For "LAN to LAN" connection, one side must be CO and the other side must be CPE.

Set up (a) LAN IP address , Subnet Mask, Gateway and Host Name
(b) WAN1 VPI,VCI and Encapsulation



LAN:
IP: 192.168.0.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.254 (The Gateway IP is provided by ISP)
Host Name: SOHO
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.
WAN1:
VPI: 0
VCI: 32
Encap: Click LLC and than Click Next to review

Review



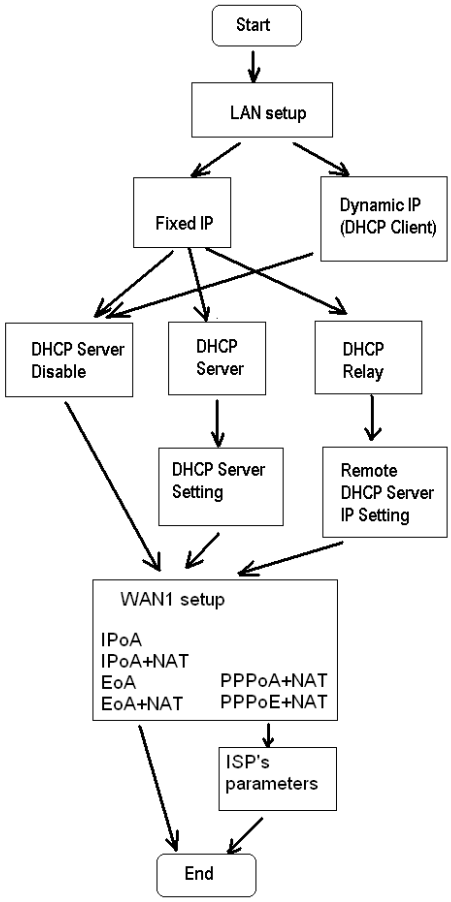
The screen will prompt the new configured parameters. Checking the parameters and Click Restart The router will reboot with the new setting or Continue to configure another parameters.

6.1.2 Routing Mode

Parameter Table:

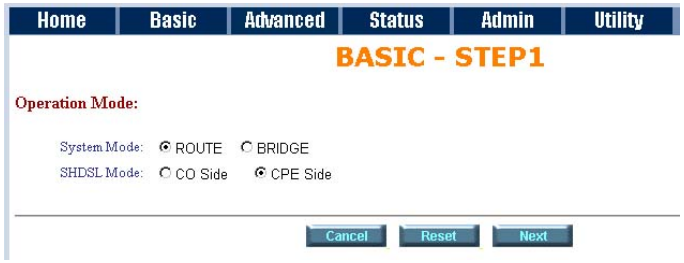
System mode	Route			
SHDSL	☐CO side ☐CPE side			
LAN	IP type		☐Fixed ☐Dynamic(DHCP Client)	
	IP address			
	Subnet Mast			
	Host Name			
	Trigger DHCP service		☐Disable ☐Server ☐Relay	
WAN1	VPI			
	VCI			
	Encapsulation		☐VC-mux ☐LLC	
	Protocol		☐IPoA ☐IPoA + NAT ☐EoA ☐EoA + NAT ☐PPPoA + NAT ☐PPPoE + NAT	
DHCP Server	Default gateway			
	Subnet Mast			
	Start IP address			
	End IP address			
	DNS Server 1			
	DNS Server 2			
	DNS Server 3			
	Lease time			
	Host Entries	1	MAC :	IP:
		2	MAC :	IP:
		3	MAC :	IP:
		4	MAC :	IP:
		5	MAC :	IP:
		6	MAC :	IP:
		7	MAC :	IP:
		8	MAC :	IP:
		9	MAC :	IP:
		10	MAC :	IP:
DHCP Relay	IP address			

The flow chart of route mode setup:



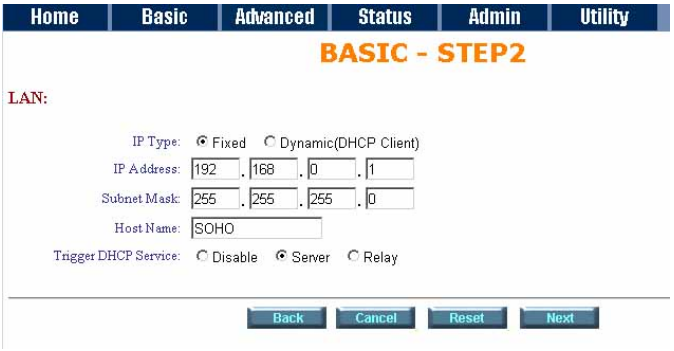
Routing mode contains DHCP server, DHCP client, DHCP relay, Point-to-Point Protocol over ATM and Ethernet and IP over ATM and Ethernet over ATM. You have to clarify which Internet protocol is provided by ISP.

Setup up system mode and SHDSL mode



click ROUTE and CPE Side then press Next.

Set up the LAN IP address , Subnet Mask, Gateway, Host Name and Trigger DHCP Service with fixed IP type.



IP type: Fixed
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
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.

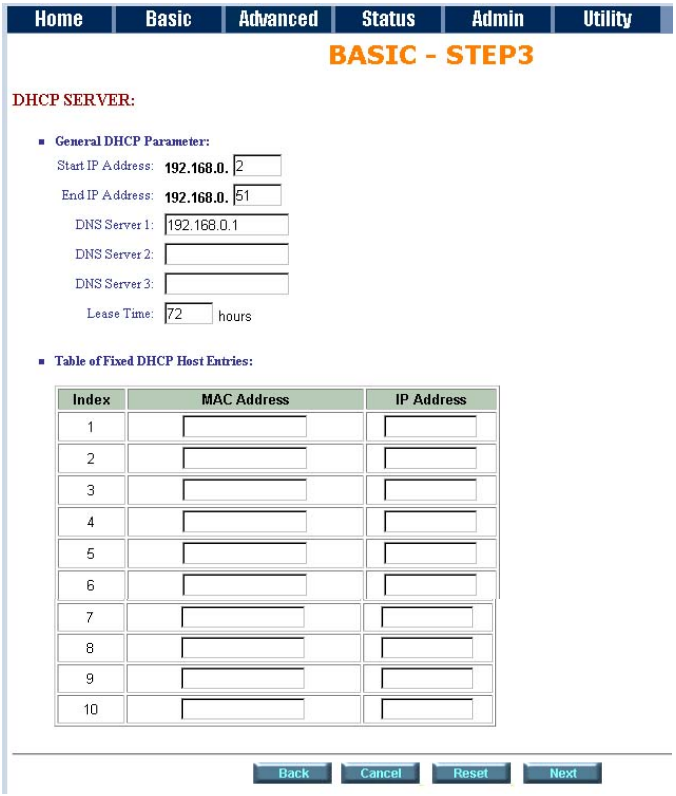
Trigger DHCP Service: Server
The default setup is Enable DHCP server. If you want to turn off the DHCP service, choose Disable.

If set DHCP server to Relay, the router acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.

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 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.

If the DHCP server is "Enable", you have to setup the following parameters for processing it as DHCP server.
The embedded DHCP server assigns network configuration information at most 253 users accessing the Internet in the same time.

Set up the DHCP Server parameters and fixed DHCP host table



Start IP Address: This field specifies the first of the contiguous addresses in the IP address pool.
End IP Address: The field specifies the last of the contiguous addresses in the IP address pool.

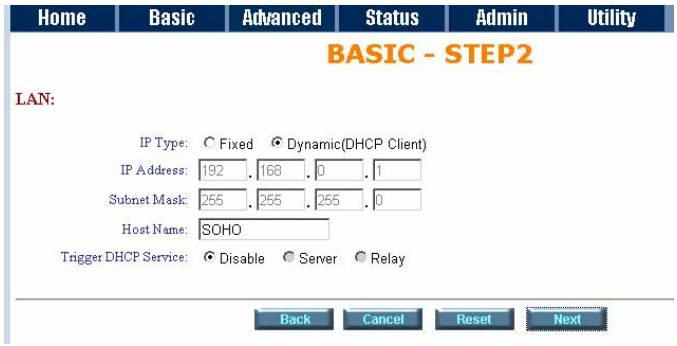
For example: If the LAN IP address is 192.168.0.1, the IP range of LAN is 192.168.0.2 to 192.168.0.51. The DHCP server assigns the IP form Start IP Address to End IP Address. The legal IP address range is form 0 to 255, but 0 are reserved as network name and 255 are reserved for broadcast. It implies the legal IP address range is from 1 to 254. That means you cannot assign an IP greater than 254 or less then 1. **Lease time** 72 hours indicates that the DHCP server will reassign IP information in every 72 hours.

DNS Server1, **DNS Server2,** and **DNS Server3**: 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. There have three DNS server can use.
You may assign a fixed IP address to some device while using DHCP, you have to put this device's MAC address in the **Table of Fixed DHCP Host Entries**. There have ten fixed IP address location can use.
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at factory and consists of six pairs of hexadecimal characters, for example, 00:30:4F:0A:02:4F

Press Next to setup WAN1 parameters.

Some of the ISP provides DHCP server service by which the PC in LAN can access IP information automatically. To setup the DHCP client mode, follow the procedure.

Set up IP address, Subnet Mask, Host Name with DHCP Client mode



LAN IP Type: Dynamic(DHCP Client)
Click Next to setup WAN1 parameters.

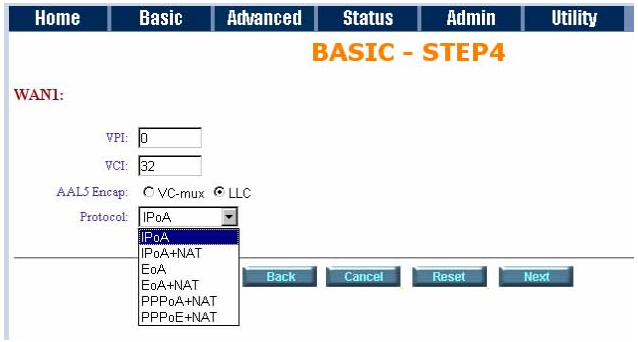
DHCP relay
If you have a DHCP server in LAN and you want to use it for DHCP services, the product provides DHCP relay function to meet yours need.

IP Type: Fixed
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
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.
Trigger DHCP Service: Relay

Set up the DHCP Server
Press Next to setup **Remote DHCP server parameter**.

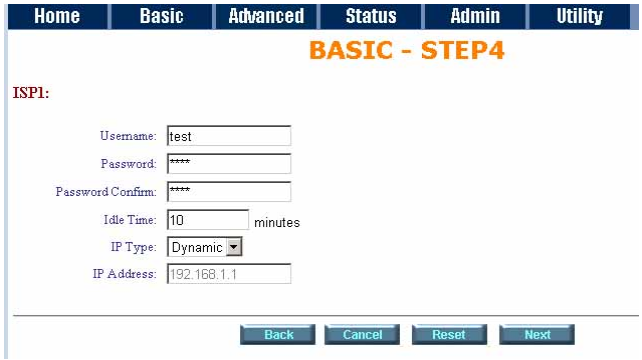
If using DHCP relay service, there must set up the remote DHCP server IP address
Enter DHCP server IP address in IP address field.
Press Next

Set up the WAN1 VPI, VCI Encap. and Protocol



VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: PPPoA + NAT or PPPoE + NAT
Click Next to setup User name and password.
For more understanding about NAT, review NAT/DMZ chapter.

If the Protocol using PPPoA+NAT or PPPoE+NAT, you must setup the ISP's parameters on the following:



Type the ISP1 parameters.
Username: test
Password: test
Password Confirm: test
Your ISP will provide the user name and password.
Idle Time: 10

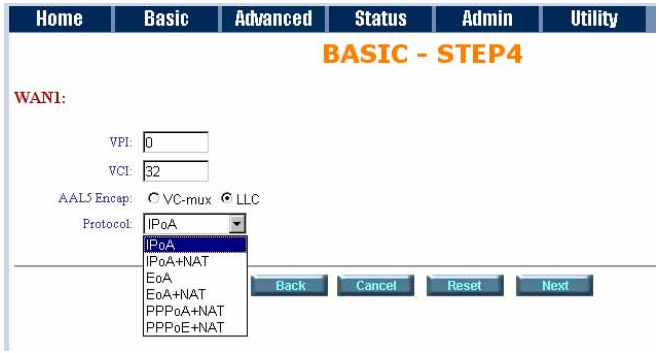
You want your Internet connection to remain on at all time, enter "0" in the Idle Time field.
IP Type: Dynamics.
The default IP type is Dynamic. It means that ISP PPP server will provide IP information including dynamic IP address when SHDSL.bis connection is established. On the other hand, you do not need to type the IP address of WAN1. Some of the ISP will provide fixed IP address over PPP. For fixed IP address:
IP Type: Fixed
IP Address: 192.168.1.1
Click Next.
Note: For safety, the password will be prompt as star symbol.

***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**: When you don't want the connection up all the time and specify an idle time on this field.*
***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 on each time you connect to the Internet.*

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 to continue setting another parameter.

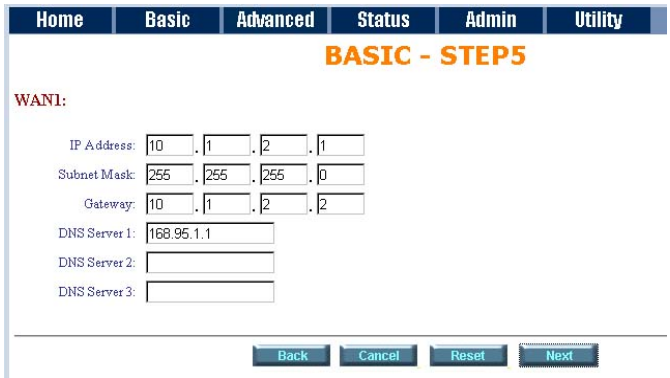
Set up : WAN1 VPI, VCI, Encap. and Protocol



WAN:
VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT
Click Next to setup the IP parameters.

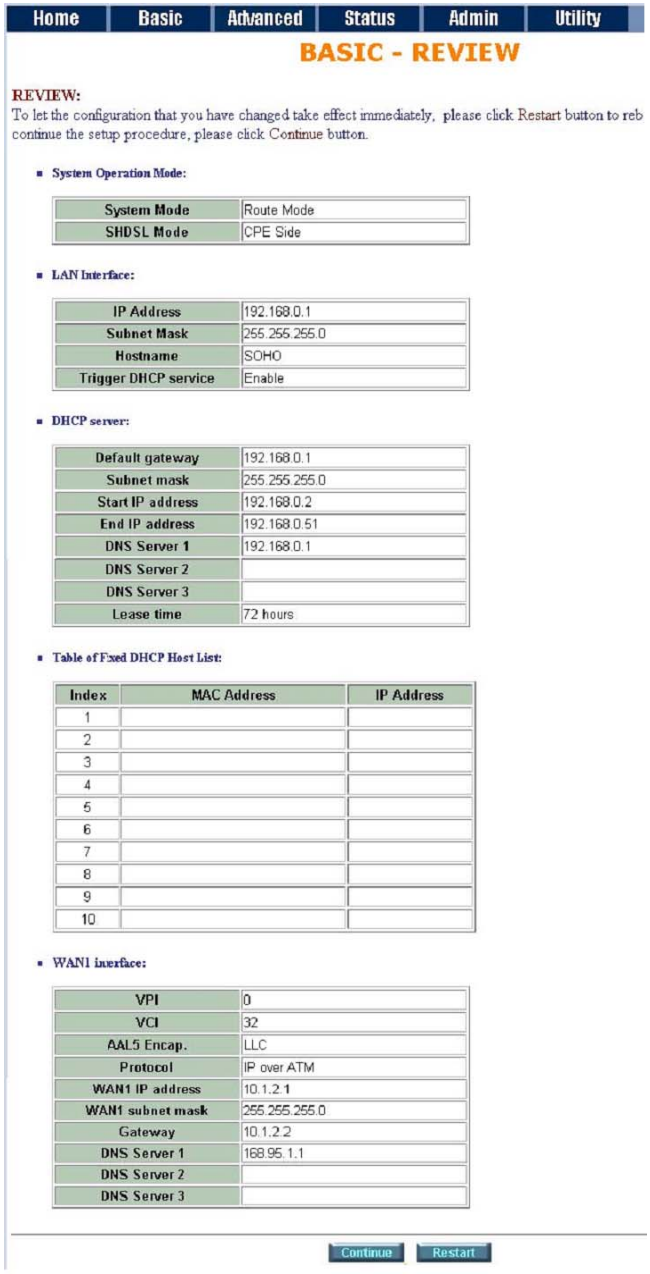
For more understanding about NAT, review NAT/DMZ chapter.

Set up the WAN1 IP address, Subnet Mask, gateway and DNS Server



IP Address: 10.1.2.1
It is router IP address like 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 the default gateway.
DNS Server 1: 168.95.1.1
Your ISP will provide at least one DNS (Domain Name System) Server IP address.
Click Next to review.

Review



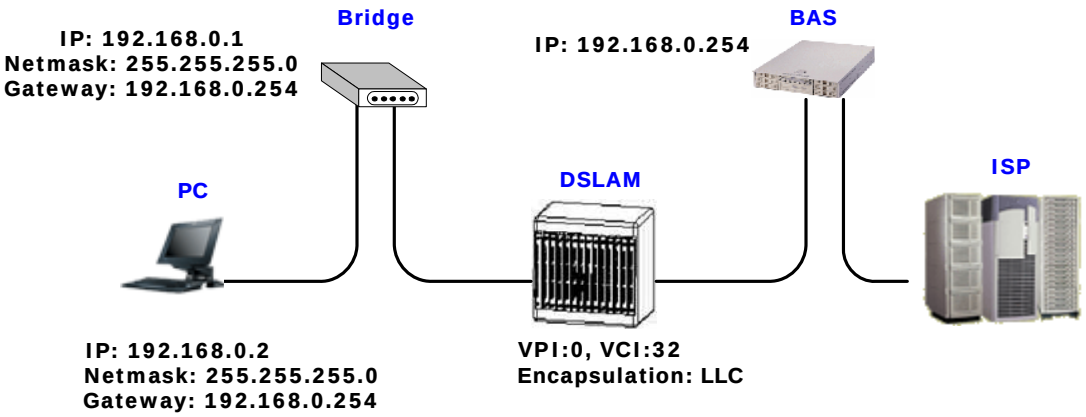
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

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

6.1.3 Reference diagram

Bridge mode

When configured in Bridge Mode, the router will act as a pass-through device and allow the workstations on your LAN to have public addresses directly on the internet.

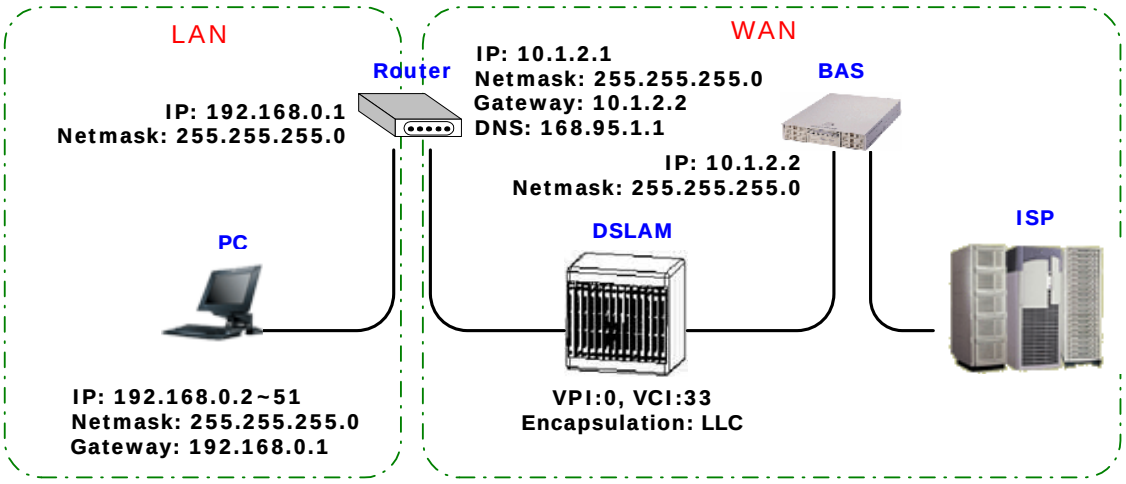


IPoA or EoA

IPoA (Dynamic IP over ATM) interfaces carries IP packets over AAL5. AAL5 provides the IP hosts on the same network with the data link layer for communications. In addition, to allow these hosts to communicate on the same ATM networks, IP packets must be tuned somewhat. AS the bearer network of IP services, ATM provides high speed point-to-point connections which considerably improve the bandwidth performance of IP network. On the other hand, ATM provides excellent network performance and perfect QoS.

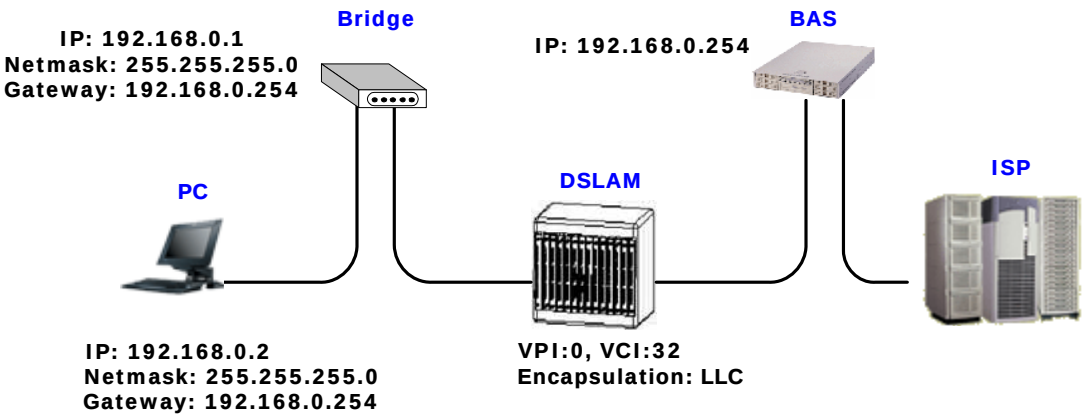
EoA (Ethernet-over-ATM) protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EoA protocol for data transfer with their customers' DSL modems.

EoA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EoA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.



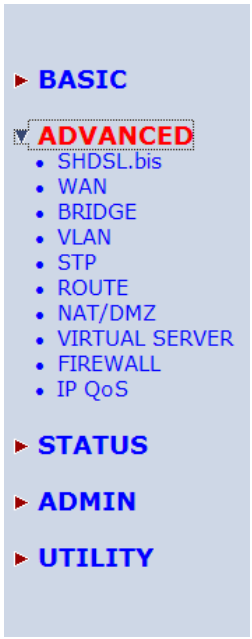
PPPoE or PPPoA

PPPoA (point-to-point protocol over ATM) and PPPoE (point-to-point protocol over Ethernet) 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.



6.2 Advanced Setup

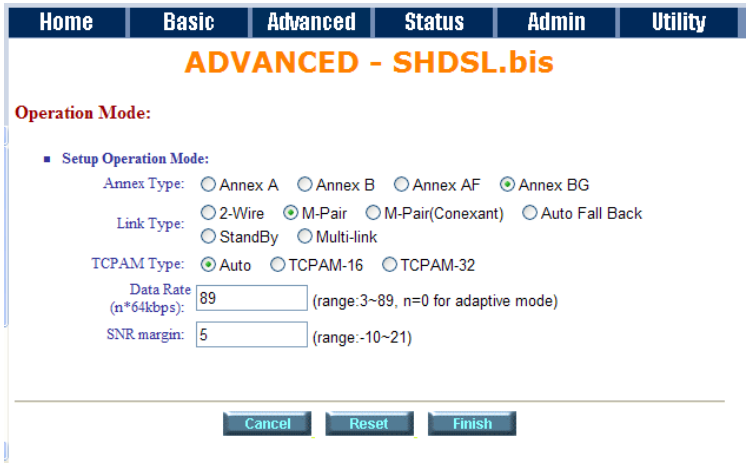
Advanced setup contains **SHDSL.bis, WAN, Bridge, VLAN, Ethernet, Route, NAT/DMZ, Virtual SERVER, FIREWALL and IP QoS** parameters.



6.2.1 SHDSL.bis

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

Enter Parameters in SHDSL.bis



6.2.1.1 Annex Type

There are four Annex types: **Annex A** (ANSI), **Annex B** (ETSI), **AnnexAF** and **Annex BG** . It the router must connect to your ISP, please check them about it. If your routers configed to point to point application, you must choose one of the four types according to which line rate you need.

6.2.1.2 Line Type

There are six type of line type for you choose: **2-wire**, **M-Pair**, **M-Pair(Conexant)**, **Auto Fall Back**, **StandBy** and **Multi-link.**

2-wire mode

For 4-wires 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 disconnect, the other pair will keep working.

Stanby Mode

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

Multi–Link Mode

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

6.2.1.3 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 click the caption TPCAM-16 or TPCAM-32.

6.2.1.4 Data Rate

For 2-wire model **(n*64kbps)**

You can setup 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 768Kbps ~ 5696Kbps (Nx64kbps, N=12~89)
TCPAM16 ; data rate is 192Kbps ~ 3840Kbps (Nx64kbps, N=3~60)
For uning Annex A or B
TCPAM16 ; 192Kbps ~ 2304Kbps (Nx 64kbps, N=3~36)

For 4-wire model **(n*128kbps)**

You can setup 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 1536Kbps ~ 11392Kbps (Nx128kbps, N=12~ 89)
TCPAM16 ; data rate is 384Kbps ~ 7680Kbps (Nx128kbps, N=3~60)
For using Annex A or B
TCPAM16 ; 384Kbps ~ 4608Kbps (Nx 128kbps, N=3~36)

For adaptive mode, you have to setup n=0. The router will adapt the data rate according to the line status.

		2-wire model	4-wire model
Annex A/B	TCPAM-16	192~2304 kbps	384~4608 kbps
Annex AF/BG	TCPAM-16	192~3840 kpbs	384~7680 kbps
	TCPAM-32	768~5696 kpbs	1536~11392 kbps

6.2.1.5 SNR Margin

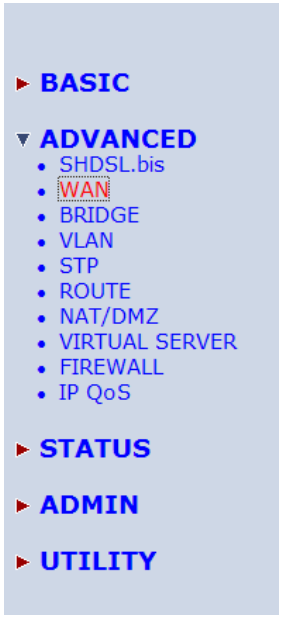
This is an index of line connection quality. You can see the actual SNR margin in STATUS SHDSL.bis. The larger is SNR margin, the better is line connection quality.

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.

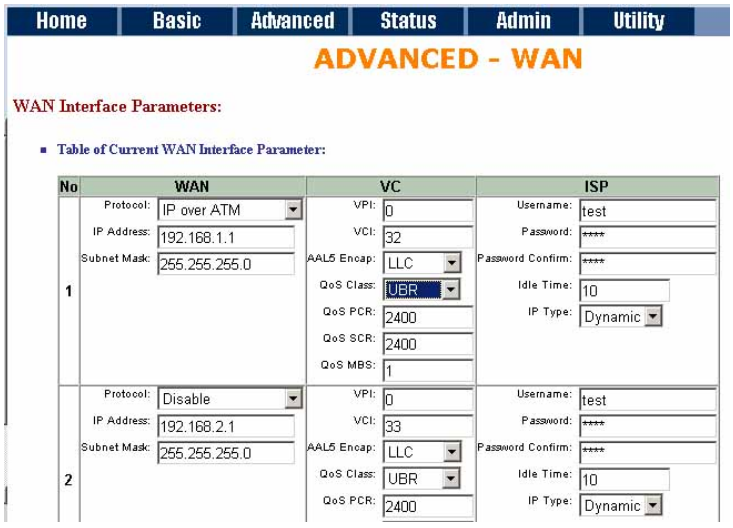
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.
Press Restart to restart the router working with new parameters or press continue to setup another parameter.

6.2.2 WAN

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



The parameters in WAN Number 1 has been setup in Basic Setup. If you want to setup another PVC, 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 erasion or blank 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 erasion or blank 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. Deapite 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 need to provide for that traffic. There have four class four choice: UBR, CBR, rt-VBR and nrt-VBR. Select CBR to specify fixed bandwidth for voice or data traffic. Select UBR for applications that are non-time sensitive, such as e-mail. Slect 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 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) 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 lone-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: When you don't want the connection up all the time and specify an idle time on this field.

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 on each time you connect to the Internet.

Press Finish to finish setting.

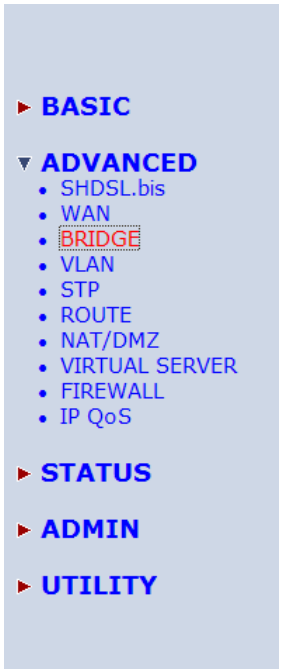
The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

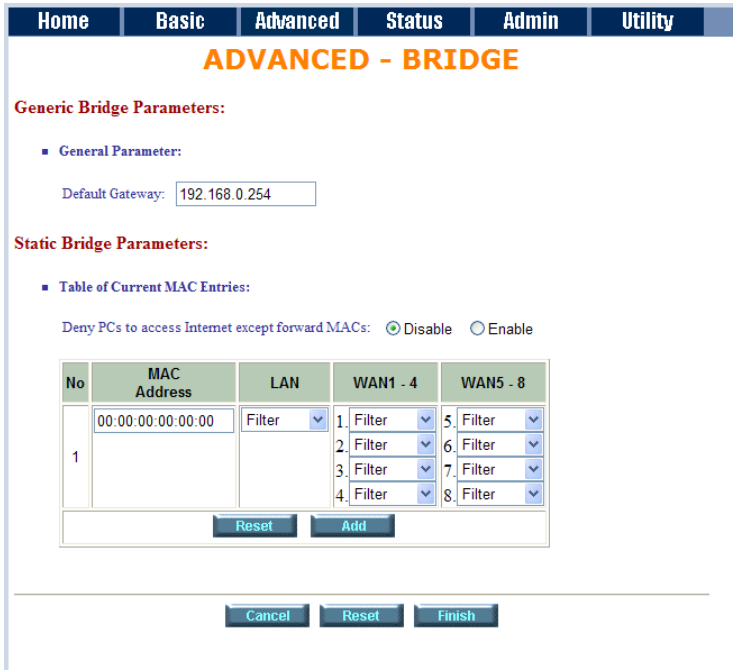
Press Restart to restart the router working with new parameters or press continue to setup another parameter.

6.2.3 Bridge

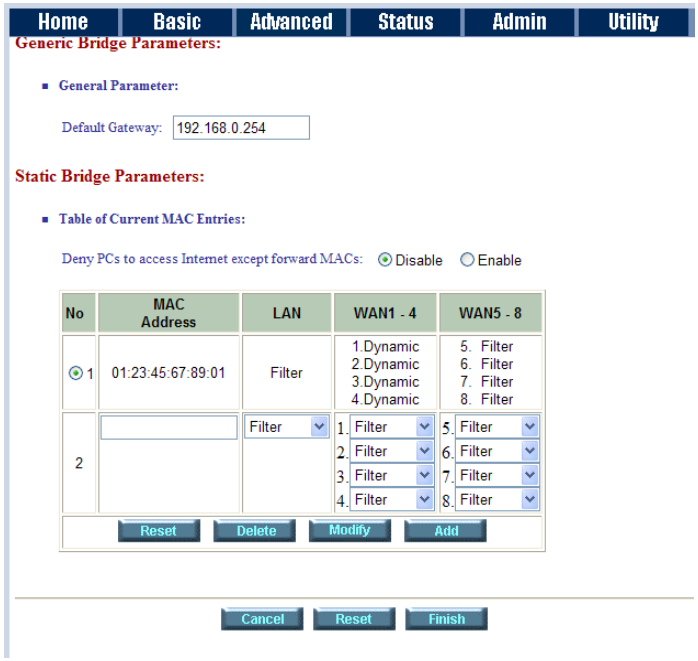
If you want to setup advanced filter function while router is working in bridge mode, you can use **BRIDGE** menu to setup the filter function, blocking function.

Click Bridge to setup.





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

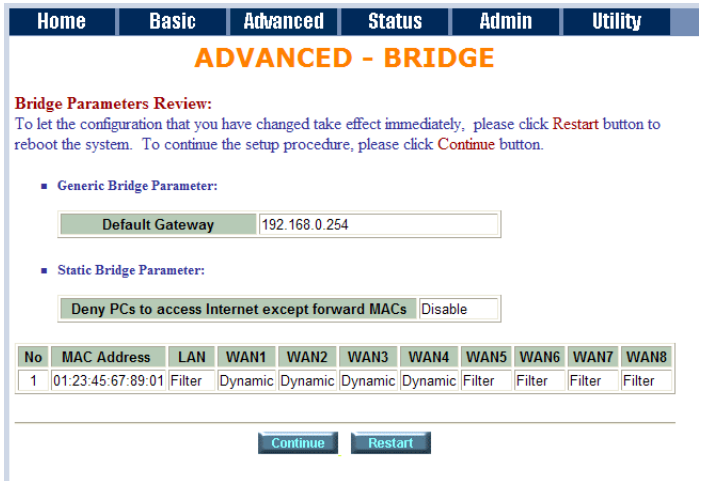


If you want to filter the designated MAC address of LAN PC to access Internet, press Add to establish the filtering table. Put the MAC address in **MAC Address** field and select Filter in **LAN** field.

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 in the bottom of web page to review the bridge parameters.

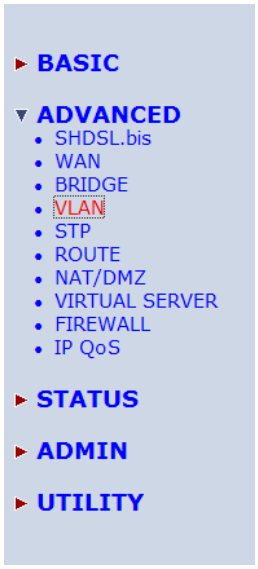


The screen will prompt the parameters that will be written in NVRAM. Check the parameters before writing in NVRAM.

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

6.2.4 VLAN

Click VLAN to configure VLAN.

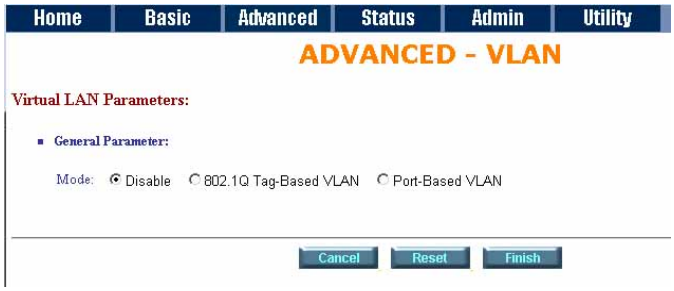


VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group.

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 every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

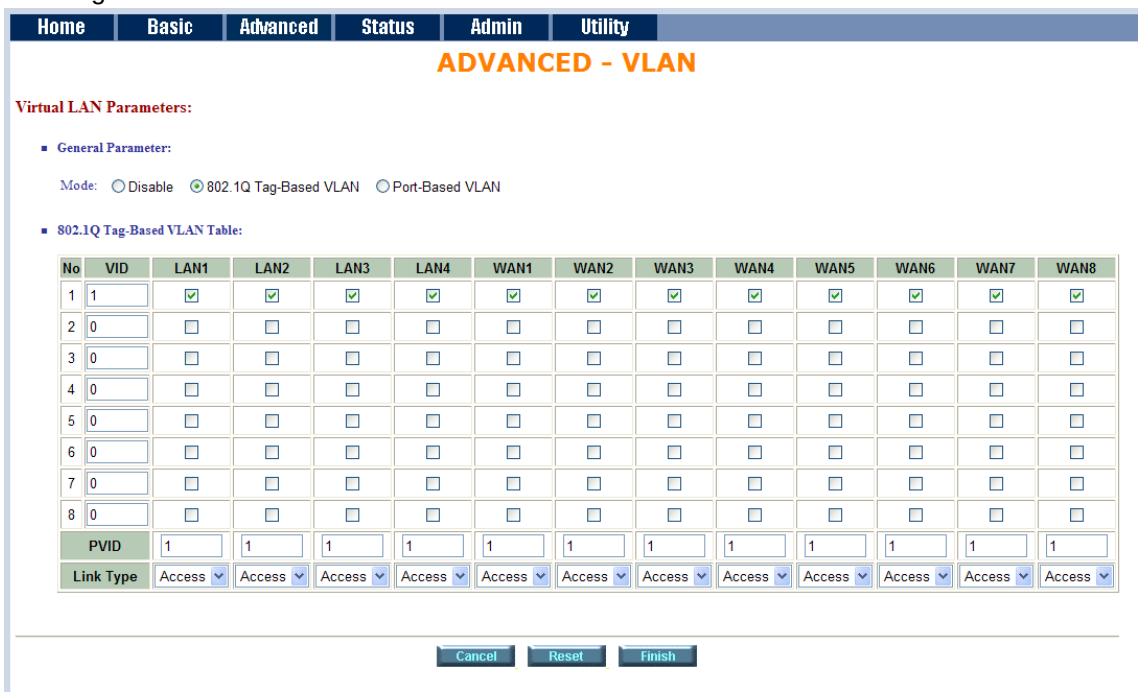
The IEEE 802.1Q defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure.



The router supports two types of VLAN: **802.1Q Tag-Based VLAN** and **Port-Based VLAN**. User can configure one of them to the router.

6.2.4.1 802.1Q Tag-Based VLAN

For setting 802.1Q VLAN click the 802.1Q Tagt-Based VLAN. The screem will prompt as following.



VID: (Virtual LAN ID) It is an definite number of ID which number is 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 prot can receive or send tagged packets.

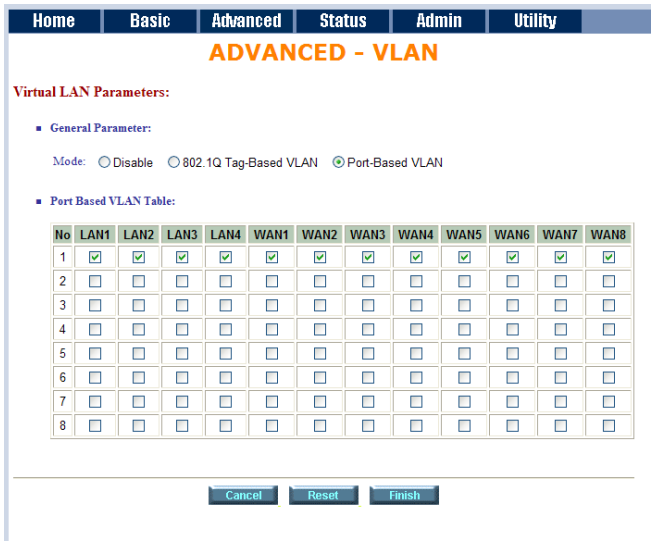
The Router initially default configures one VLAN , VID=1.
A port such as LAN1 to LAN4 and WAN1 to WAN8 can have only one PVID, but can have as many VID as the router has memory in its VLAN table to store them.

Ports in the same VLAN group share the same frame broadcast domin thus increase network performance through reduced boardcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

6.2.4.2 Port-Based VLAN

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

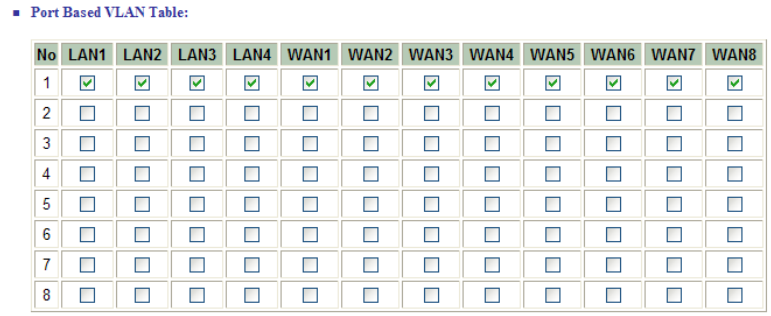
For setting Port-Based VLAN, Click Port-Based VLAN, The screem will prompt as following:



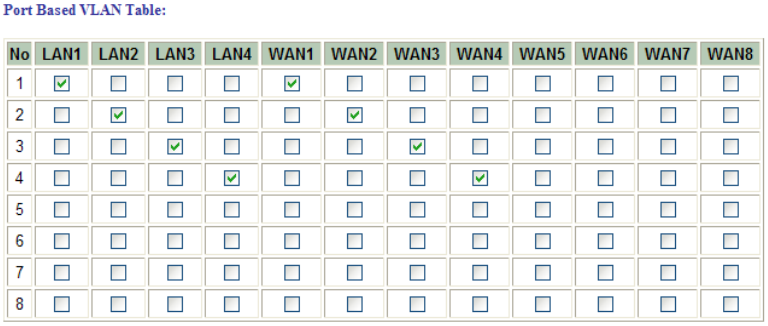
Port-Based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

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.

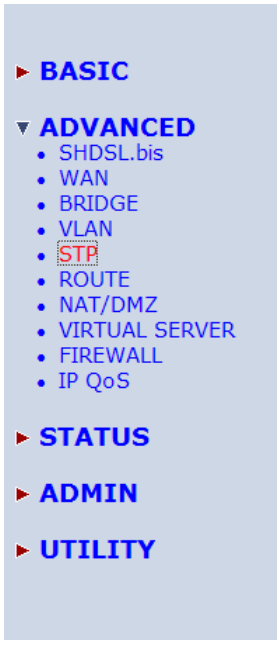
As with other VLAN approaches, the packets forwarded using this method do not leak into other VLAN domains on the network. After a port has been assigned to a VLAN, the port cannot send to or receive from devices in another VLAN.



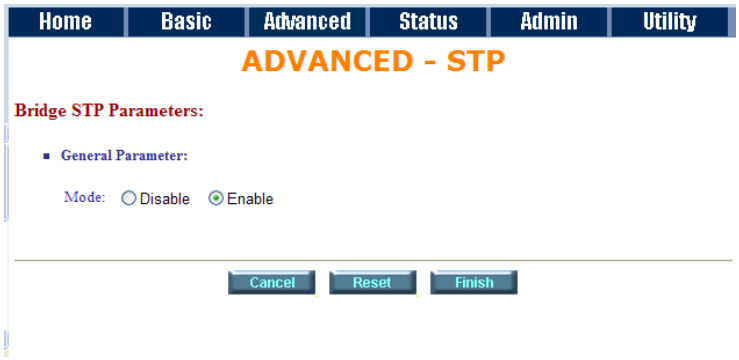
The default setting is all ports (LAN1 to LAN4 and WAN1 to WAN8) connected together which means all ports can communicate with each other. That is, there are no virtual LANs. The option is the most flexible but the least secure.



6.2.5 STP



Click STP can disable or enable the bridge STP mode.

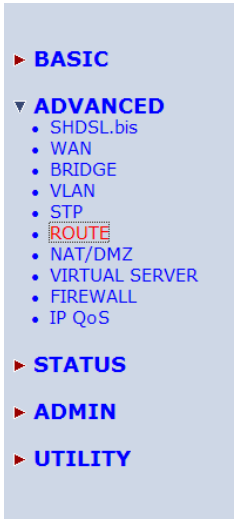


STP (Spanning-Tree Protocol) defined in the IEEE 802.1D, is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.
Multiple active paths between stations 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.

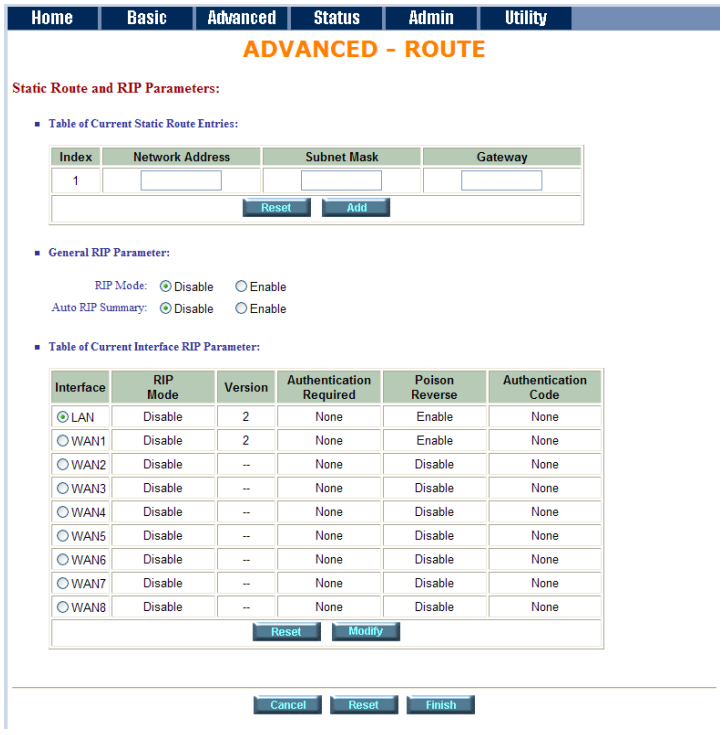
6.2.6 Route

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.

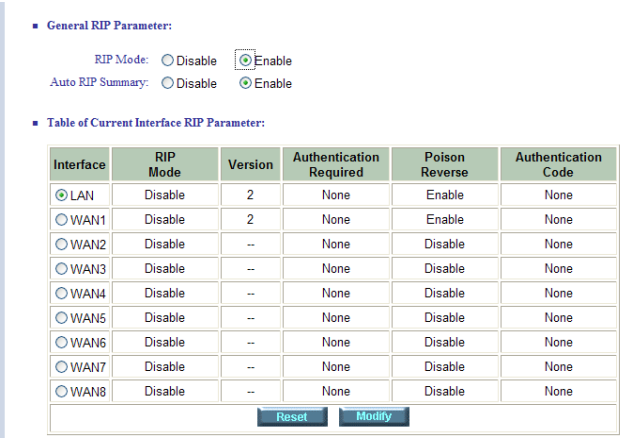
With Dynamic Routing, you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts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



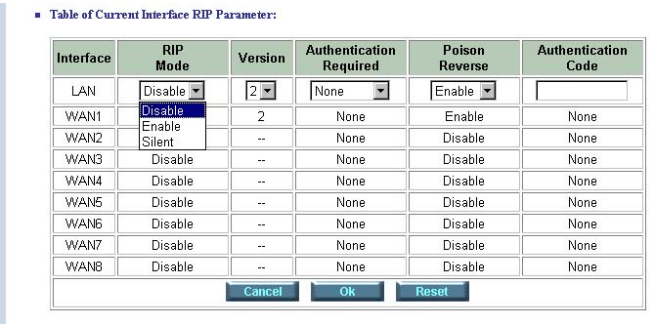
Click Route to modify the routing information.



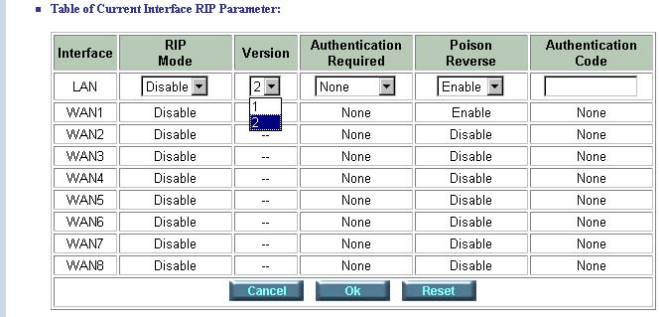
To modify the RIP (Routing information protocol) Parameters:
RIP Mode: Enable
Auto RIP Summary: Enable
Press Modify



RIP Mode:
This parameter determines how the router handle RIP (Routing information protocol). RIP allows it to exchange routing information with other router. If set to Disable, the gateway does not participate in any RIP exchange with other router. If set 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. If set 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.

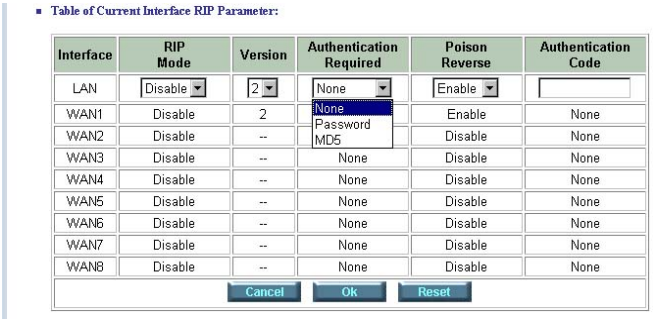


Authentication required:

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 than protected by password, authentication code.

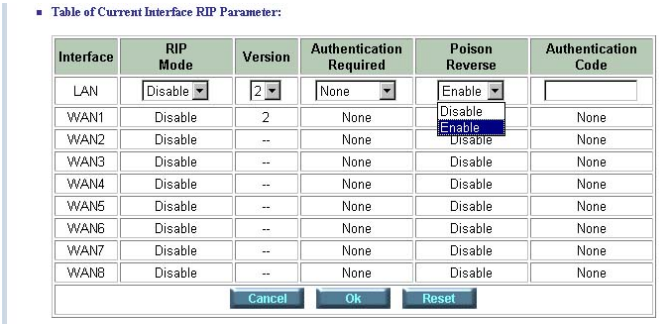


Poison Reserve:

Poison Reserve is for the purpose of promptly broadcast or multicast the RIP while the route is changed. (ex shuting 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.



After modifying the RIP parameters, press finish.

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

6.2.7 NAT/DMZ

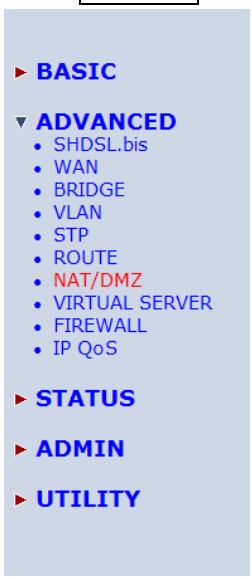
NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network 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.

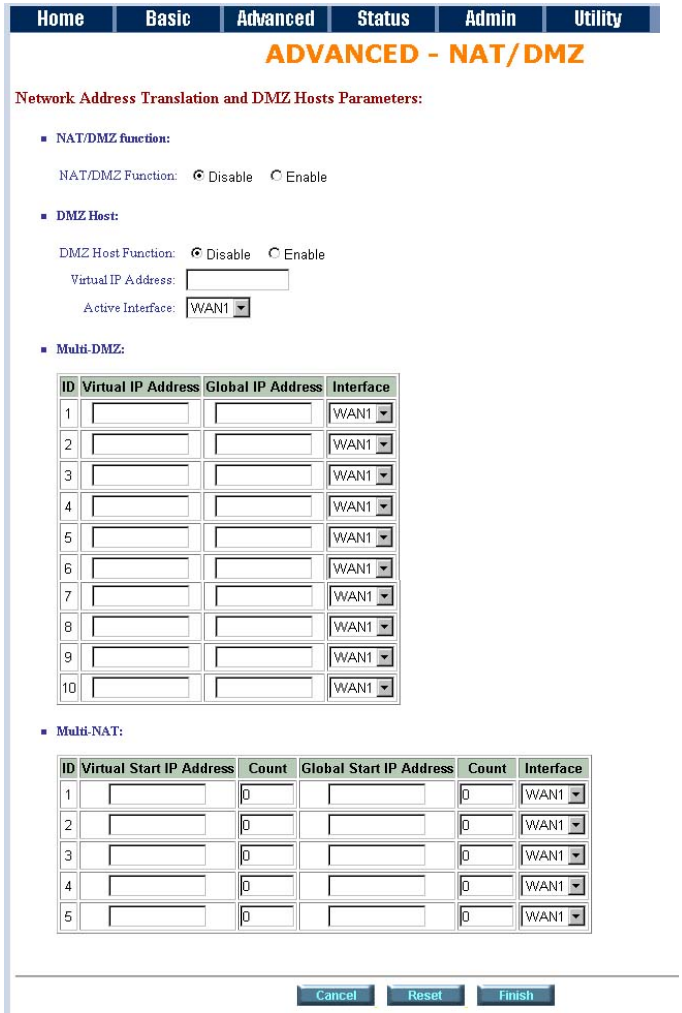
DMZ (Demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company private network and the outside public network. It prevents outside users from getting direct access to a server that has company private data.

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/DMZ to setup the parameters.





If you want to enable the NAT/DMZ functions, click Enable. Enable the DMZ host Function is used the IP address assigned to the WAN for enabling DMZ function for the virtual IP address.

6.2.7.1 Multi-DMZ

Some users who have two or more global IP addresses assigned by ISP can be used the multi DMZ. The table is for the mapping of global IP address and virtual IP address.

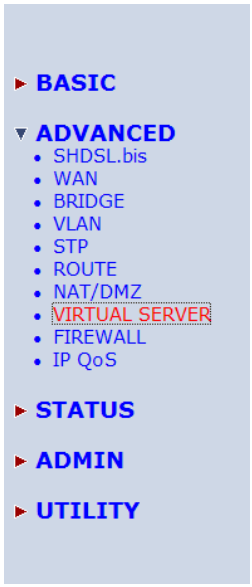
6.2.7.2 Mutli-NAT

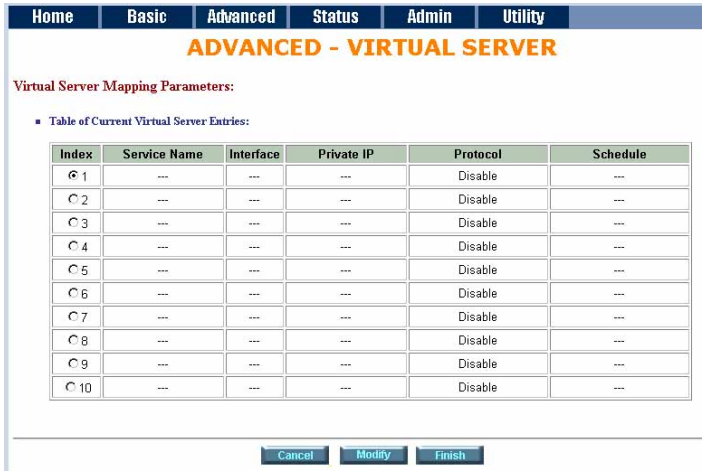
Some of the virtual IP addresses (eg: 192.168.0.10 ~ 192.168.0.50) collectively use two of the global IP addresses (eg: 69.210.1.9 and 69.210.1.10). The Multi-NAT table will be setup as;
Virtual Start IP Address: 192.168.0.10
Count: 40
Global Start IP Address: 69.210.1.9
Count: 2
Press Finish to continue 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.

6.2.8 Virtual Server

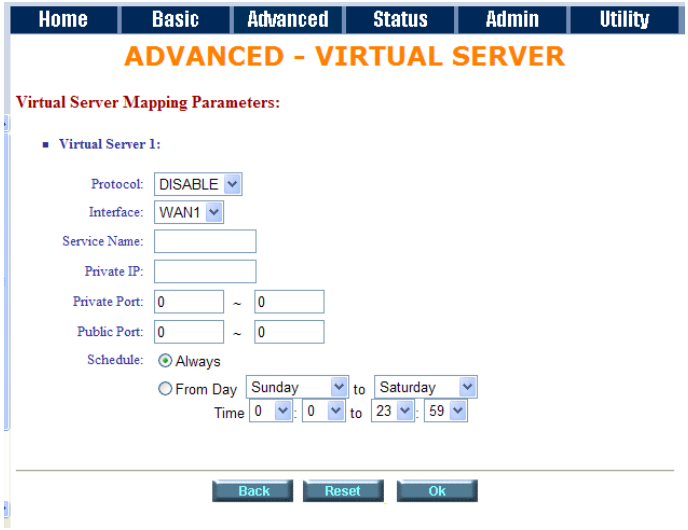
Click Virtual Server to configure the parameters.





There have ten virtual server index form 1 to 10 can been set up.

Press Modify for modify index 1.



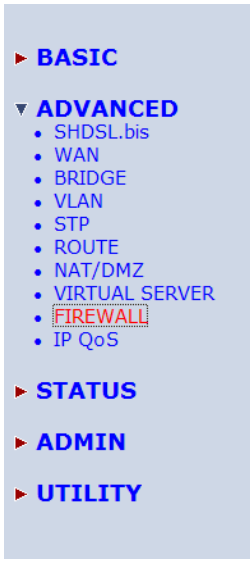
Type the necessary parameters and then click OK.

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

For example: Specific ports on the WAN interface are re-mapped to services inside the LAN. As only 69.210.1.8 (e.g., assigned to WAN from ISP) is visible to the Internet, but does not actually have any services (other than NAT of course) running on gateway, it is said to be a virtual server. Request with TCP made to 69.210.1.8:80 are remapped to the server 1 on 192.168.0.2:80 for working days from Monday to Friday 8 AM to 6PM, other requests with UDP made to 69.210.1.8:25 are remapped to server 2 on 192.168.0.3:25 and always on.

You can setup 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 Day Monday to Friday and time 8:0 to 16:0 and index 2, protocol UDP, interface WAN1, service name test2, private IP 192.168.0.3, private port 25, public port 25, schedule always.

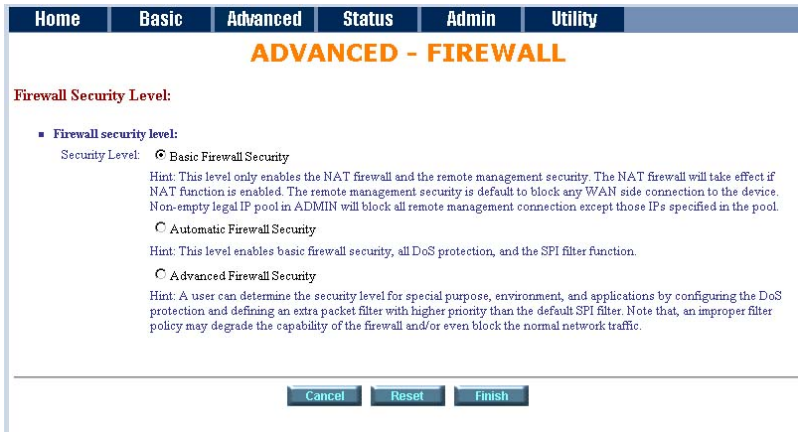
6.2.9 Firewall



A firewall is a set of related programs that protects the resources of a private network from other networks. It is helpful to users that allow preventing hackers to access its own private data resource accidentally.

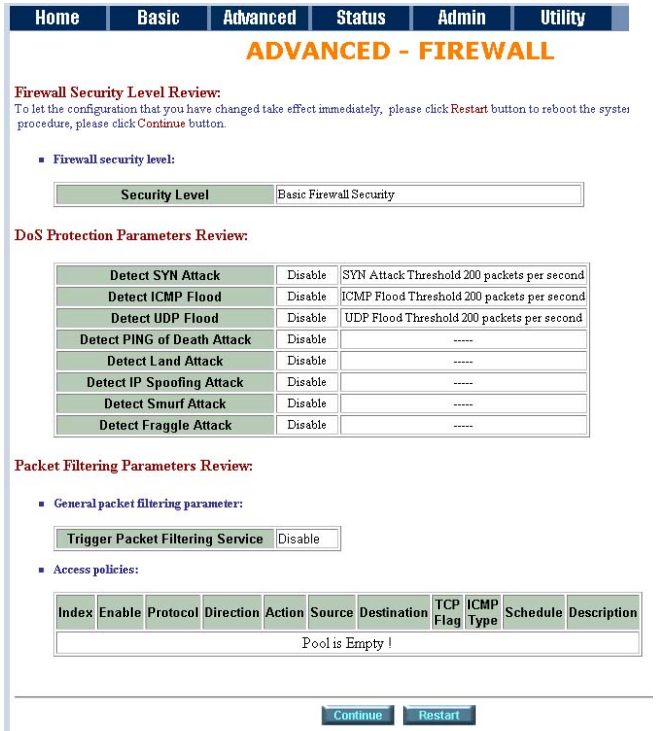
There have three security levels for setting: **Basic firewall security**, **Automatic firewall security** and **advanced firewall security**.

6.2.9.1 Basic Firewall Security



Click Basic Firewall Security.

This level 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.
Press Finish to finish setting of firewall and can review the parameters.

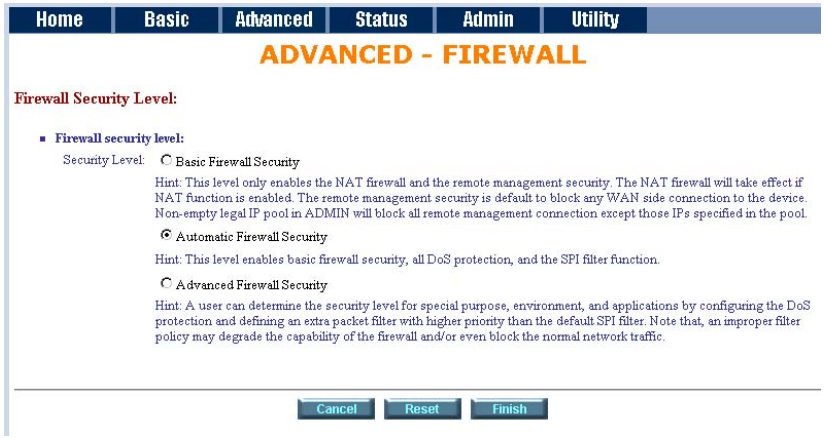


The screen will prompt the parameters, which router will record in NVRAM. Check the parameters.

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

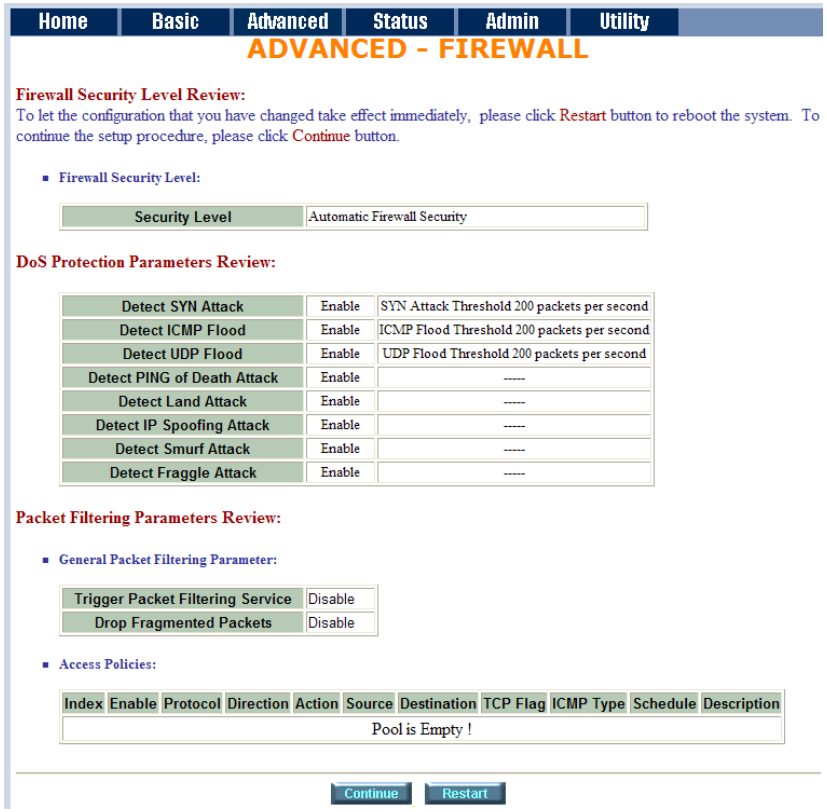
6.2.9.2 *Automatic Firewall Security*

Click Automatic Firewall Security.



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

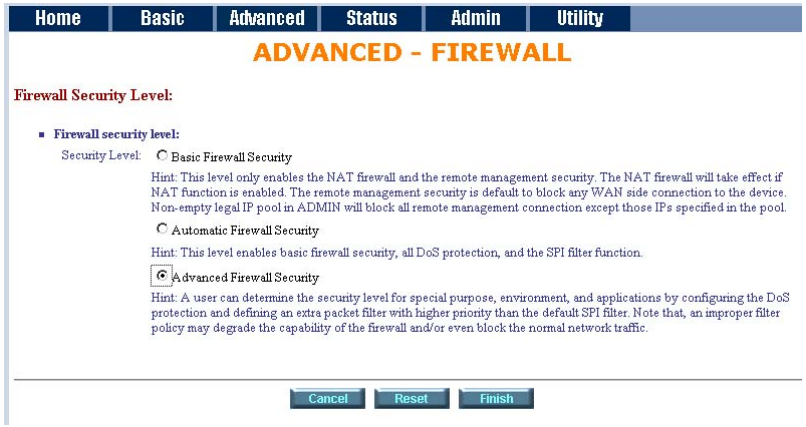
Press Finsih to finish setting firewall.



The screen will prompt the parameters, which will be written in NVRAM. Check the parameters. Press Restart to restart the router or press Continue to setup 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 with higher priority than the default SPI filter. Note that, an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.

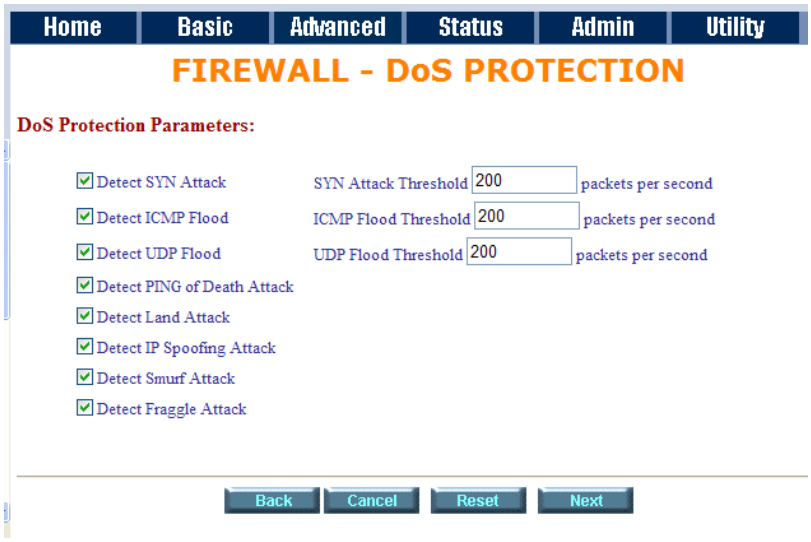
6.2.9.3 Advanced Firewall Security

Click 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 with higher priority than the default SPI 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 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.

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.

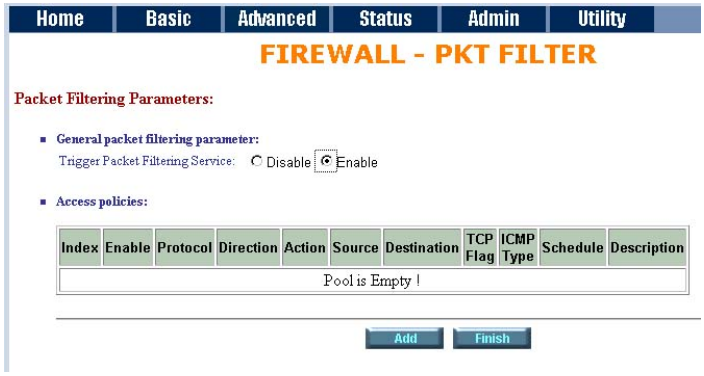
Traditional firewall is stateless meaning they have no memory of the connections of data or packets that pass through them. Such IP filtering firewalls simply examine header information in each packet and attempt to match it to a set of define rule. If the firewall finds a match, the prescribe action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

A stateful firewall maintains a memory of each connection and data passing through it. Stateful firewall records the context of connections during each session, continuously updating state information in dynamic tables. With this information, stateful firewalls inspect each connection traversing each interface of the firewall, testing the validity of data packets throughout each session. As data arrives, it is checked against the state tables and if the data is part of the session, it is accepted. Stateful firewalls enable a more intelligent, flexible and robust approach to network security, while defeating most intrusion methods that exploit state-less IP filtering firewalls.

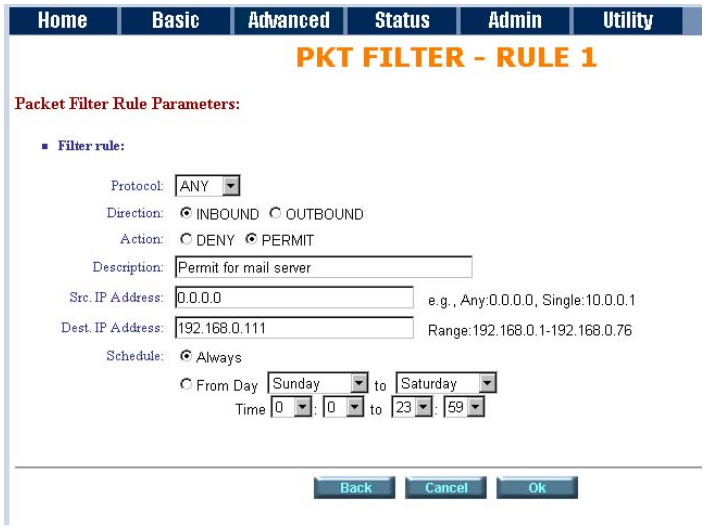
Packet filter

Click Next can set up the packet filtering parameters.

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



It can setup the packet filter rule parameters:

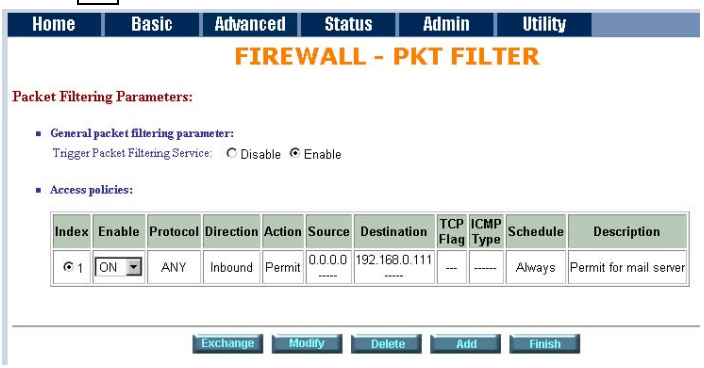


Select the Protocol and configure the parameter.

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



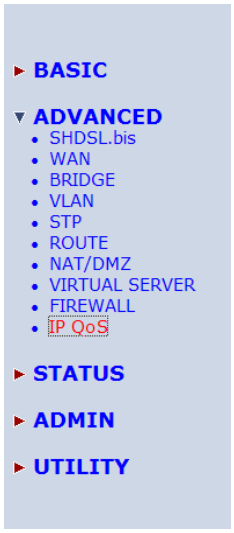
The screen will prompt the configured parameters.

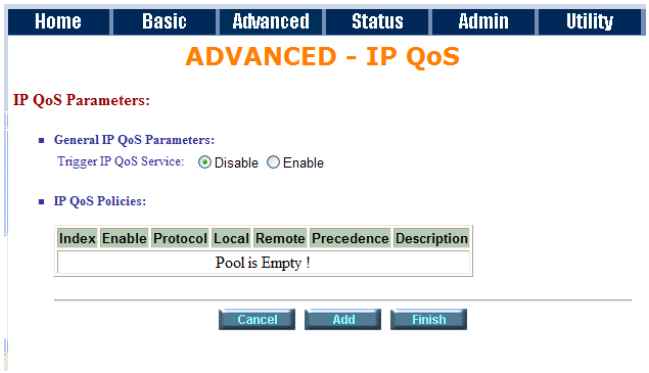
Click Enable on Trigger Packet Filtering Service item, to active the packet filtering service.

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

6.2.10 IP QoS

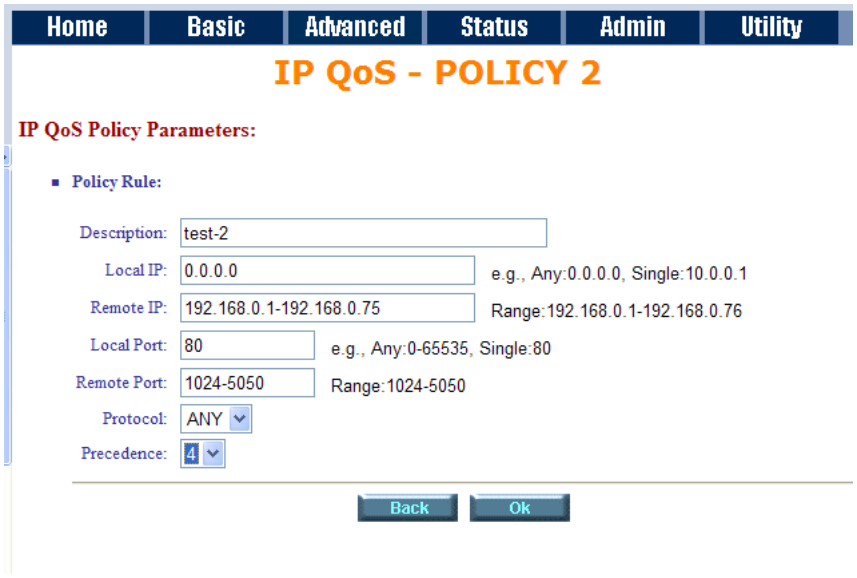
IP QoS is a good function to decide which PCs can get the priorities to pass though router once if the bandwidth is exhausted or fully saturated.





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

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



Description: A brief statement describe this policy

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

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

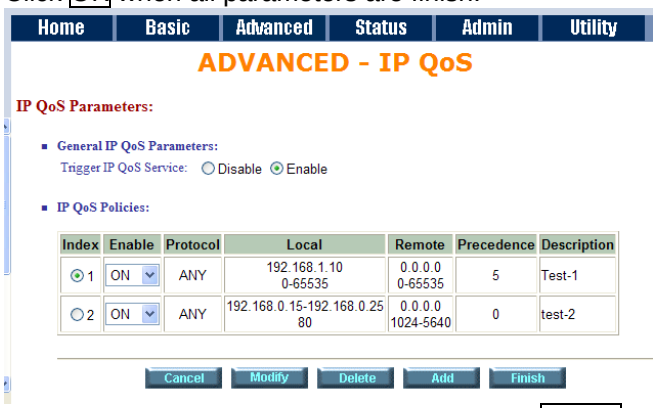
Local Port: type the service port number of local host in prioritized session.

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

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

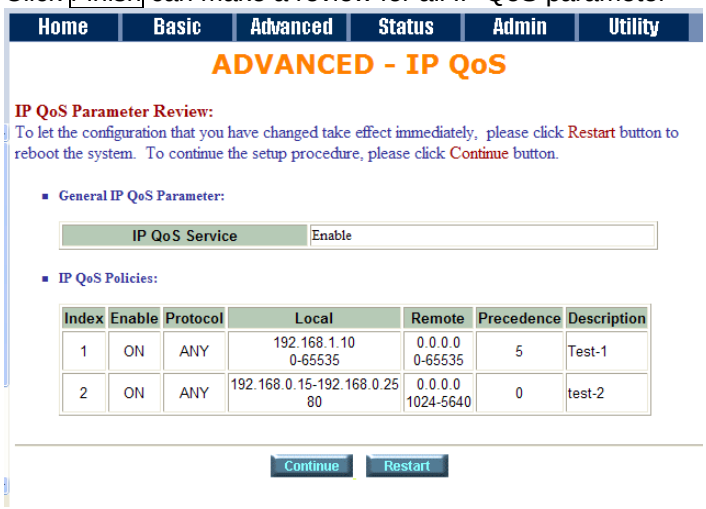
Precedence: type the session's prioritized level you classify, "**0**" is lowest priority, "**5**" is highest priority.

Click OK when all parameters are finish.



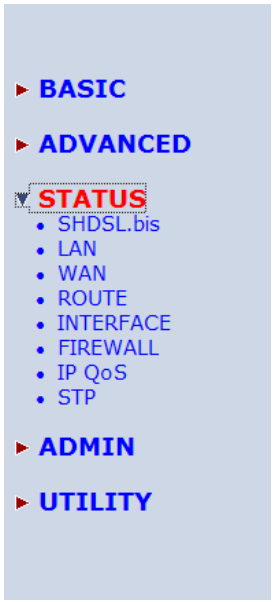
You can modify or delete the policies by click Modify or Delete command

Click Finish can make a review for all IP QoS parameter



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

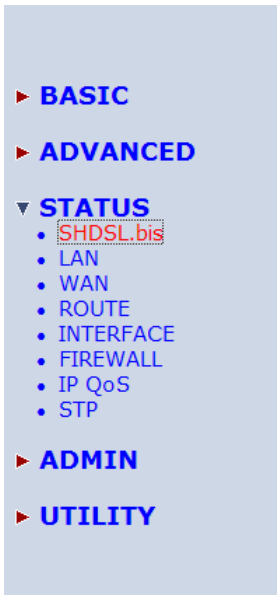
6.3 Status

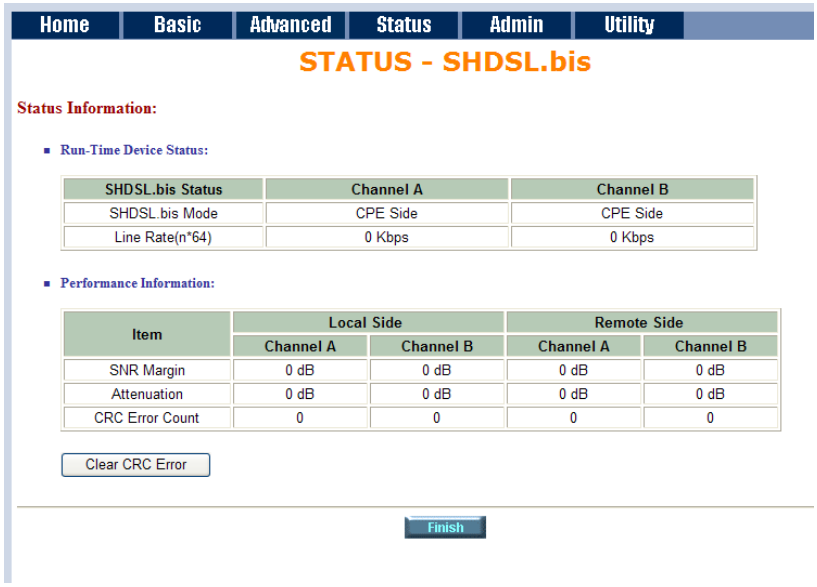


On STATUS item, you can monitor the following:

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 Port name.
INTERFACE	LAN and WAN statistics information.
FIREWALL	Current DoS protection status and dropped packets statistics.
IP QoS	IP QoS statistics on LAN interface
STP	STP information include Bridge parameter and Ports Parameter

6.3.1 SHDSL.bis

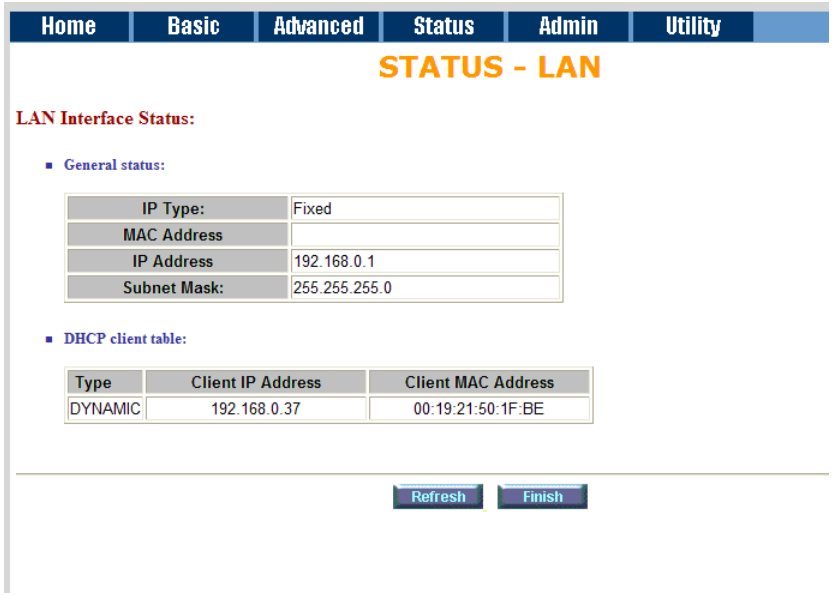




The status information shows this is 4-wire model which have channel A and B. If the router have connected to remote side, it can also show the performance information of remote side.

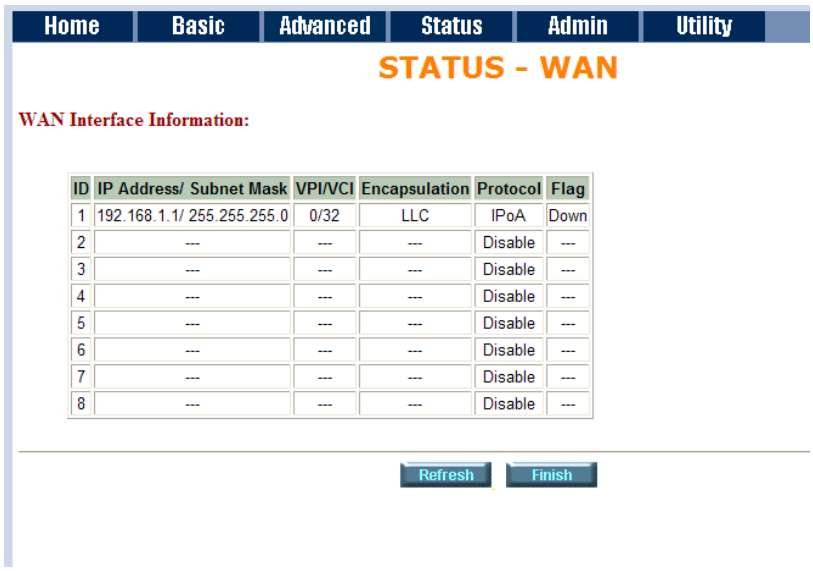
Click Clear CRC Error can clear the CRC error count.

6.3.2 LAN



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

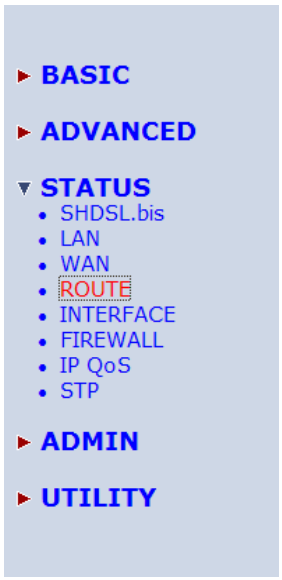
6.3.3 WAN

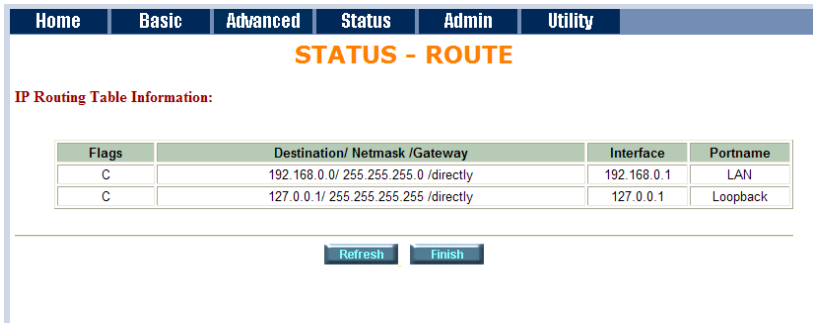


ID	IP Address/ Subnet Mask	VPI/VCI	Encapsulation	Protocol	Flag
1	192.168.1.1/ 255.255.255.0	0/32	LLC	IPoA	Down
2	---	---	---	Disable	---
3	---	---	---	Disable	---
4	---	---	---	Disable	---
5	---	---	---	Disable	---
6	---	---	---	Disable	---
7	---	---	---	Disable	---
8	---	---	---	Disable	---

This information shows all eight WAN interface.

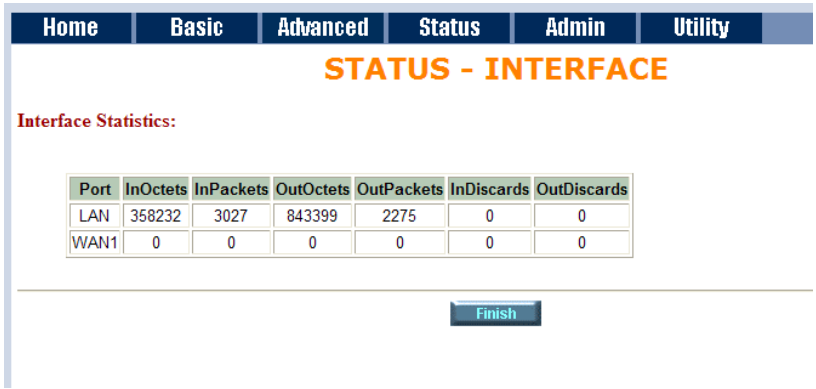
6.3.4 ROUTE





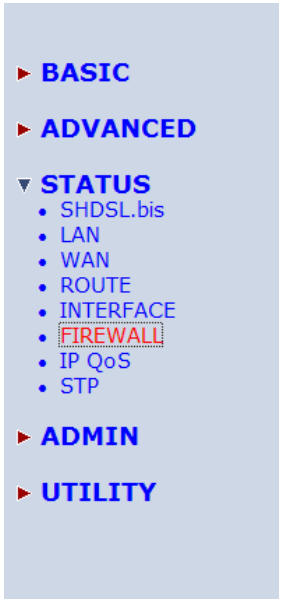
This information shows the IP routing table.

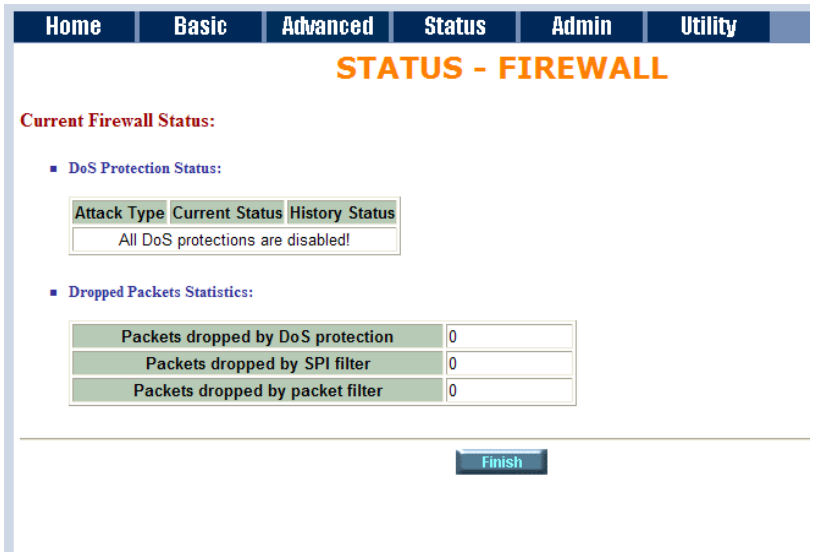
6.3.5 INTERFACE



This table shows the interface statistics.

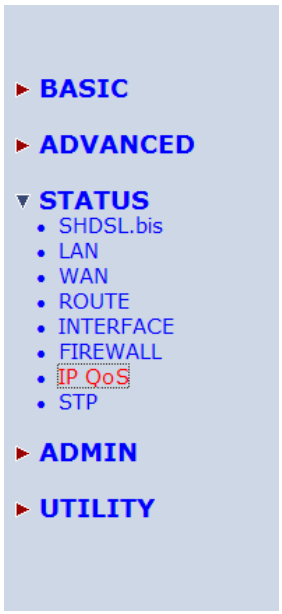
6.3.6 FIREWALL

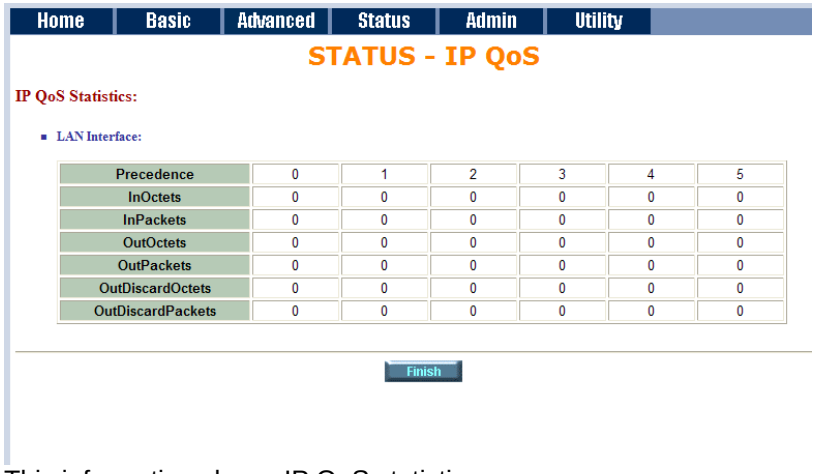




This information shows fireware status: DoS protection and dropped packets statistics.

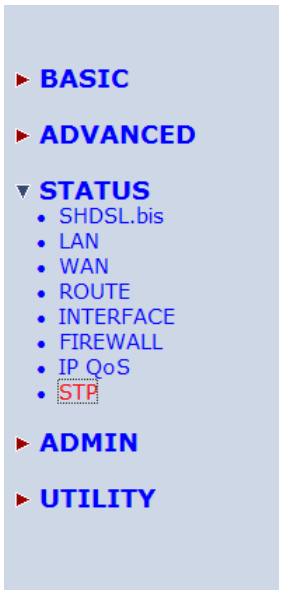
6.3.7 IP QoS

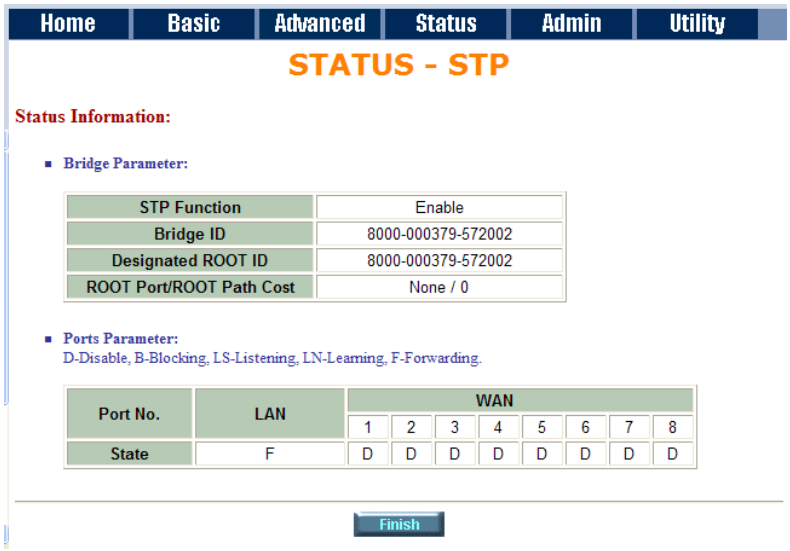




This information shows IP QoS statistics.

6.3.8 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.

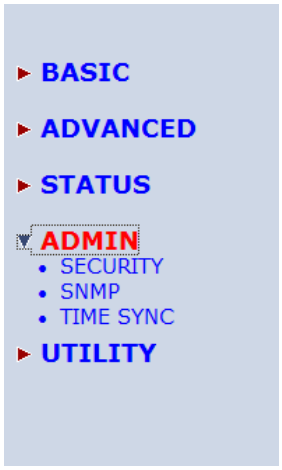
Forwarding: When a port receives or sends data. In other words, this is operating normally.

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

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

6.4 Administration

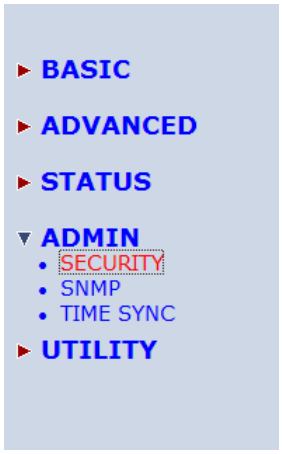
This session introduces security and simple network management protocol (SNMP) and time synchronous.



6.4.1 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.

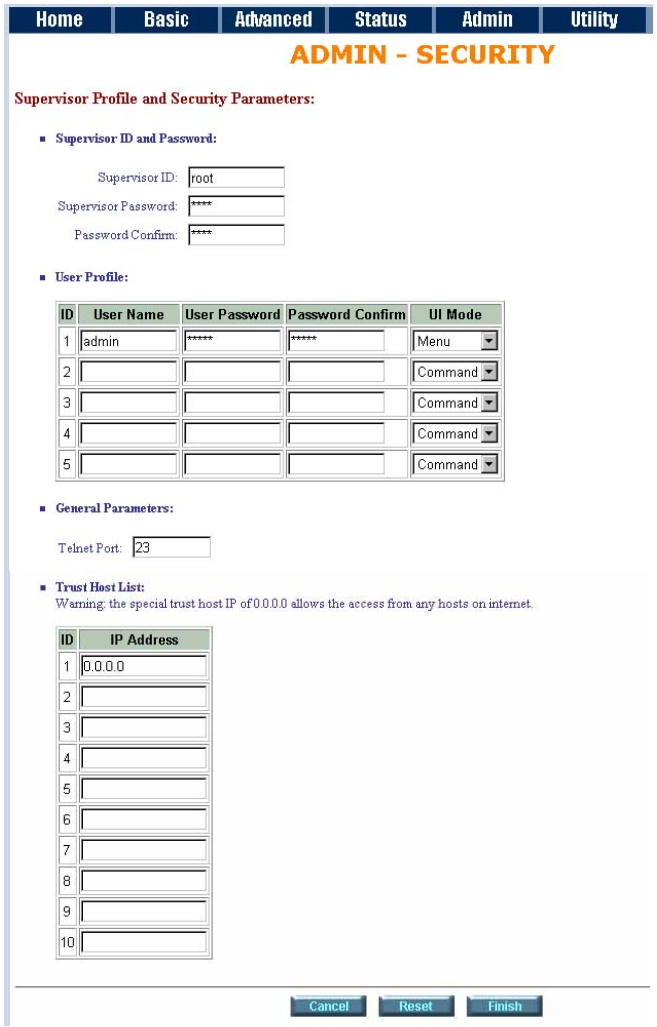
Press **Security** to setup the parameters.



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

You can authorize five legal users to access the router via telnet or console. There are two UI modes: **menu driven mode** and **line command mode** to configure the router.

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



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 excact IP address in the filed, only the host can access the router.
Click Finish to finish the setting.

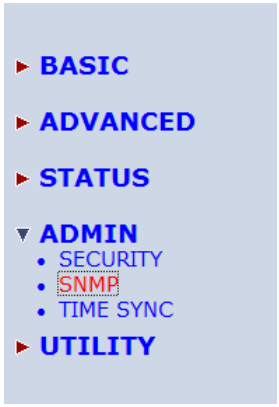
The browser will prompt the all configured parameters and check it before writing into NVRAM. Press Restart to restart the gateway working with the new parameters and press Continue to setup other parameters.

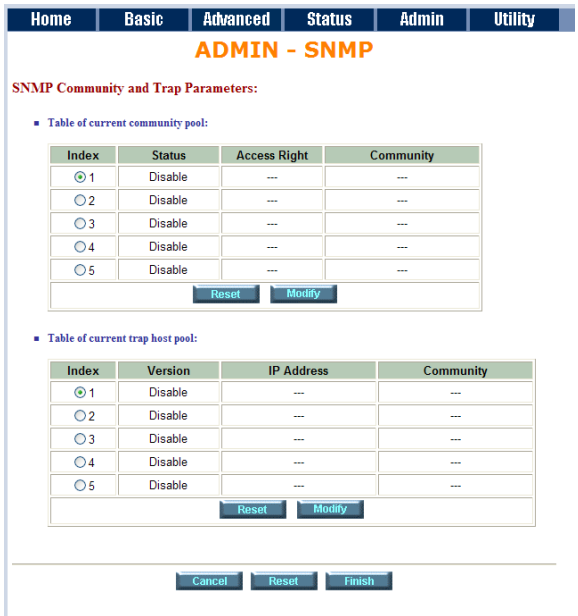
6.4.2 SNMP

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 both MIB I and MIB II.

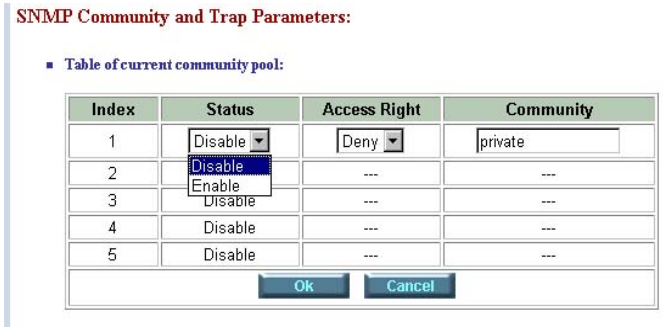
Click SNMP to configure the parameters.



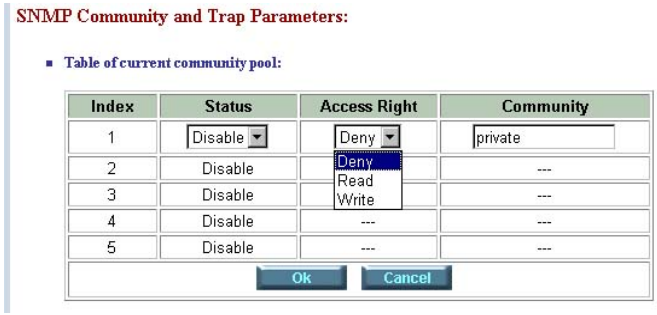


6.4.2.1 Community pool

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



SNMP **Status**: Enable

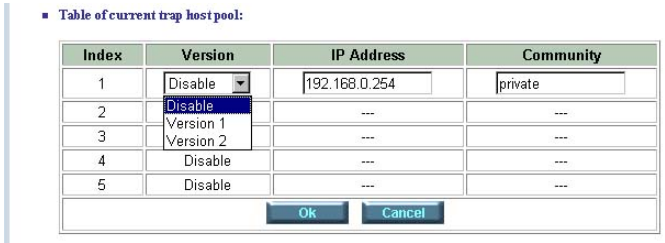


Access Right: Deny for deny all access
Read for access read only
Write for access read and write.

Community: it serves as password for access right.
After configuring the community pool, press OK.

6.4.2.2 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 setup in community pool.

Press OK to finish the setup.

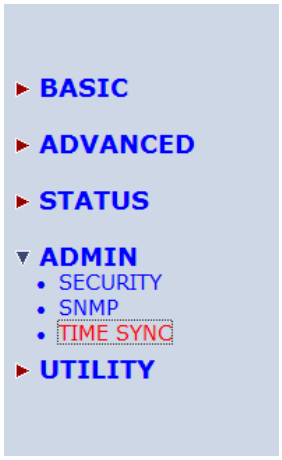
The browser will prompt the configured parameters and check it before writing into NVRAM.

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

6.4.3 Time Sync

Time synchronization is an essential element for any business, which relies on the IT system. The reason for this is that these systems all have clock that is the source of timer for their filing or operations. Without time synchronization, these system's clocks vary and cause the failure of firewall packet filtering schedule processes, compromised security, or virtual server working in wrong schedule.

Click TIME SYNC.



Time synchronization has two methods:

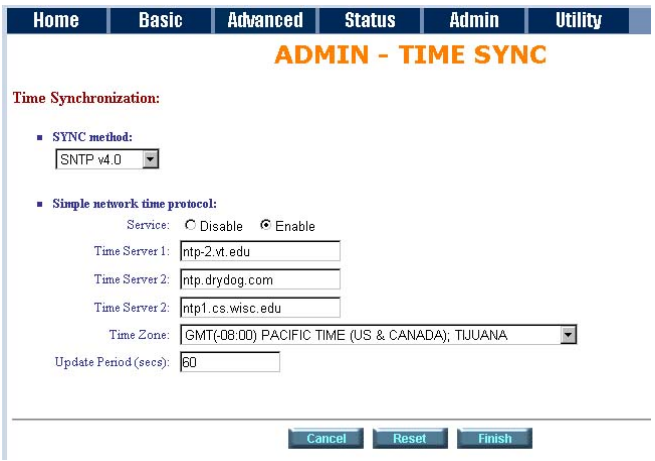
Sync with PC	Synchronization with PC
SNTP v4.0.	Simple Network Time Protocol with Version 4

6.4.3.1 Synchronization with PC

For synchronization with PC, select Sync with PC. The router will synchronize the time with the connecting PC.

6.4.3.2 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.

Service: Enable

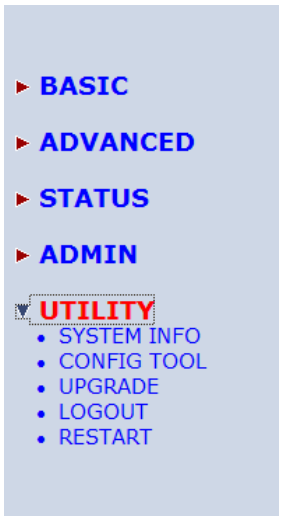
Time Server 1, Time Server 2 and Time Server 3: All of the time server around the world can be used but suggest using the time server nearby to your country. You can set up maximum three time server on here.

Time Zone: you have to choose the right GMT time zone on your country.

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

.

6.5 Utility

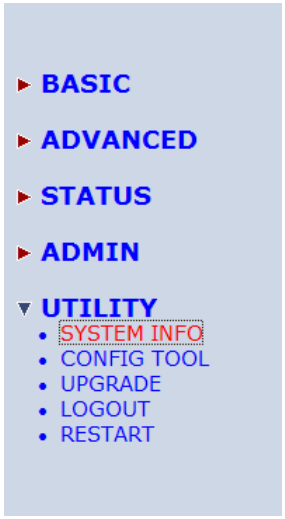


This section will describe the utility of the product including:

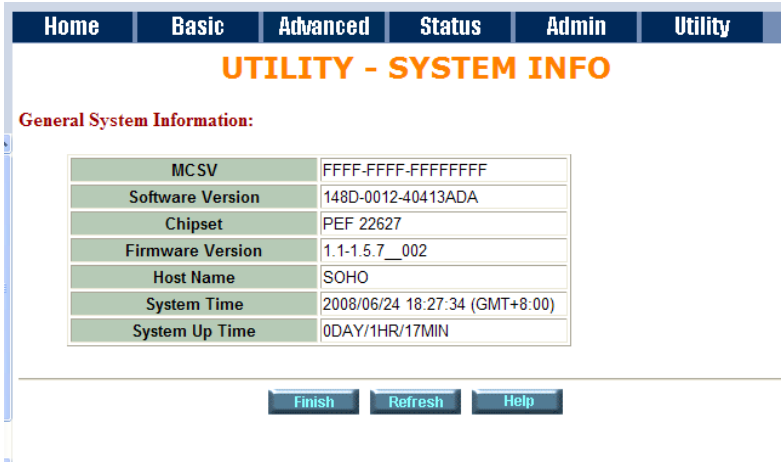
SYSTEM INFO	Show the system information
CONFIG TOOL	Load the factory default configuration, restore configuration and backup configuration
UPGRADE	Upgrade the firmware
LOGOUT	Logout the system
RESTART	Restart the router.

6.5.1 System Info

Click System Info for review the information.



The browser will prompt the system information.



There 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 modem's firmware version. This is sometimes needed by technicians to help 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 you enter in BASIC Setup. It is for identification purposes.

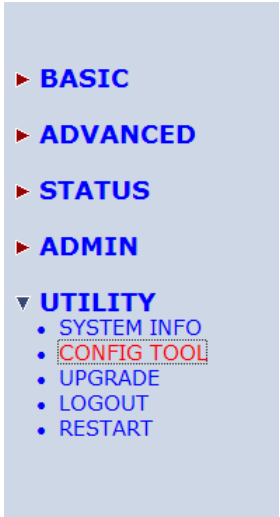
System Time: This field display your modem's present date and time.

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

6.5.2 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

6.5.2.1 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. On the other hand, you will lose all the existing configured parameters.

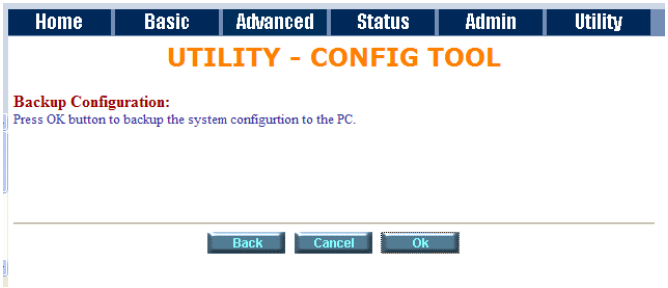
6.5.2.2 Restore Configuration

Sometime the configuration crushed occasionally. 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. Brower the place of restore file name or put the name. Then press OK. The router will automatically restore the saved configuration.

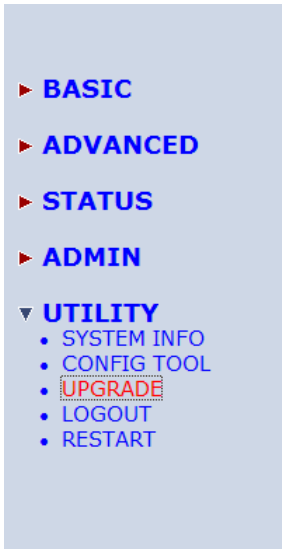
6.5.2.3 Backup Configuration

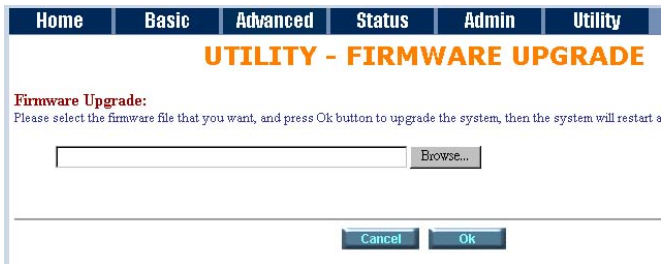
After configuration, suggest using the function to backup your router parameters in the PC. Select the Backup Configuration and then press Finish. Browse the place of backup file name or put the name. Then press OK. The router will automatically backup the configuration. If you don't put the file name, the system will use the default: *config1.log*



6.5.3 Upgrade

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

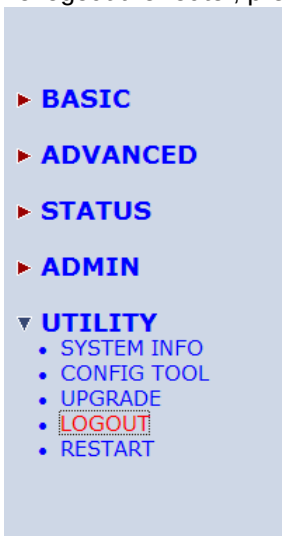




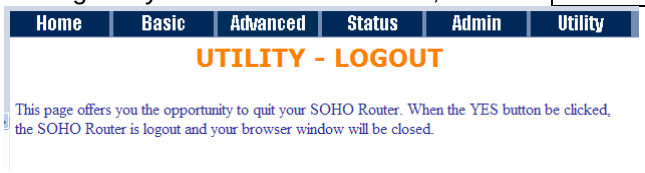
Select the firmware file name by click Browse on your PC or NB and press OK button to upgrade.
The system will reboot automatically after finish the firmware upgrade operation.

6.5.4 Logout

To logout the router, press LOGOUT in UTILITY.



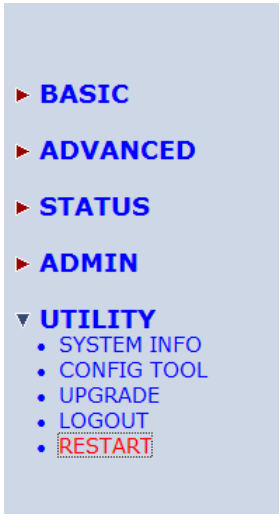
For logout system and close window, click the LOGOUT in UTILITY

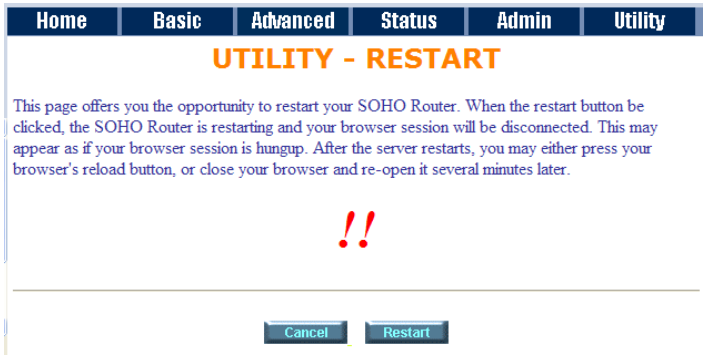


When click the Yes button, the Router will logout and browser window will be closed.

6.5.5 Restart

For restarting the router, click the RESTART in UTILITY.

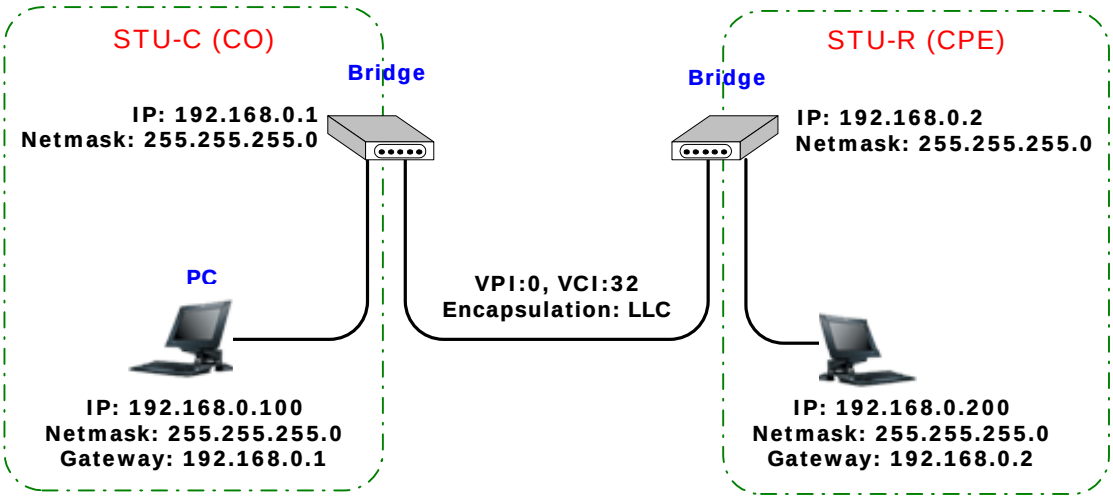




Press Restart to reboot the router.
When the restart button been clicked, the router will restarting and the browser session will be disconnected. This may appear as if your browser session is hung up. After the router restarts, you may either click the browser's reload button or close the browser and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

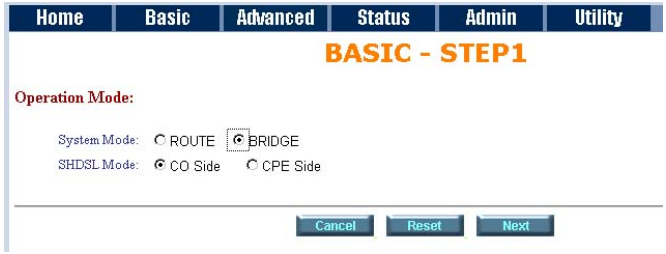
6.6 Example

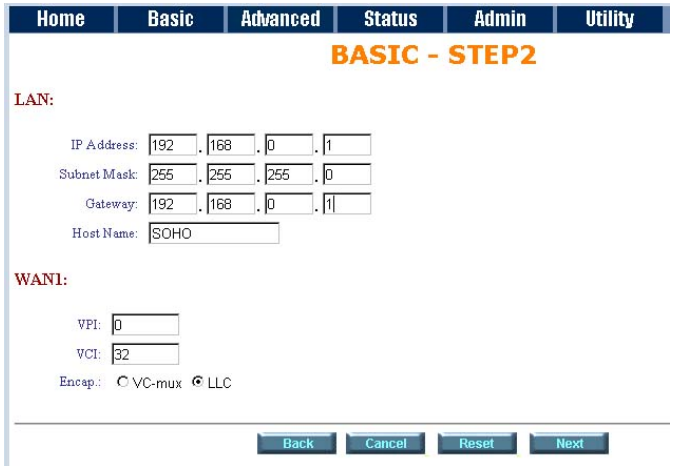
6.6.1 LAN-to-LAN connection with bridge Mode



6.6.1.1 CO side

Click Bridge and CO Side to setup Bridging mode of the Router and then click Next.





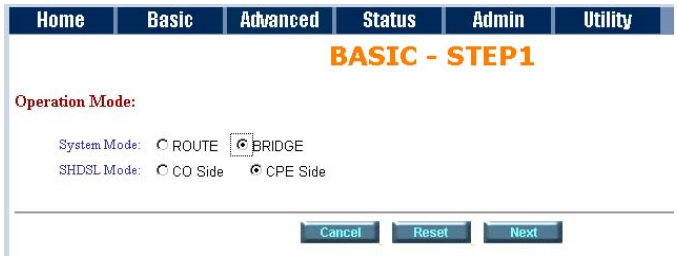
Enter **LAN** Parameters
IP: 192.168.0.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.1
Host Name: SOHO

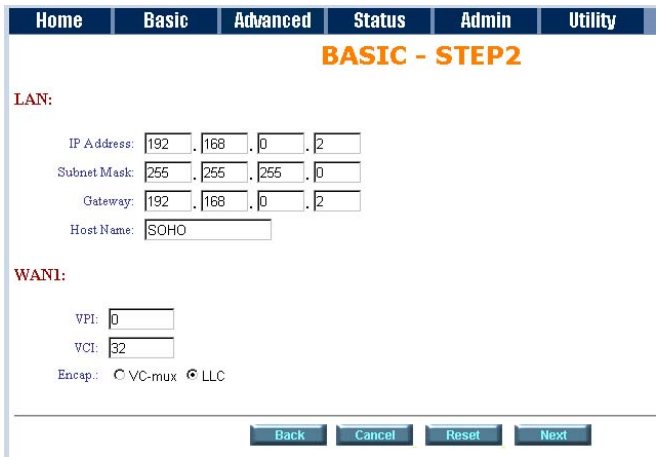
Enter **WAN1** Parameters
VPI: 0
VCI: 32
Click LLC
Click Next

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

6.6.1.2 CPE Side

Click Bridge and CPE Side to setup Bridge mode of the Router and then click Next.



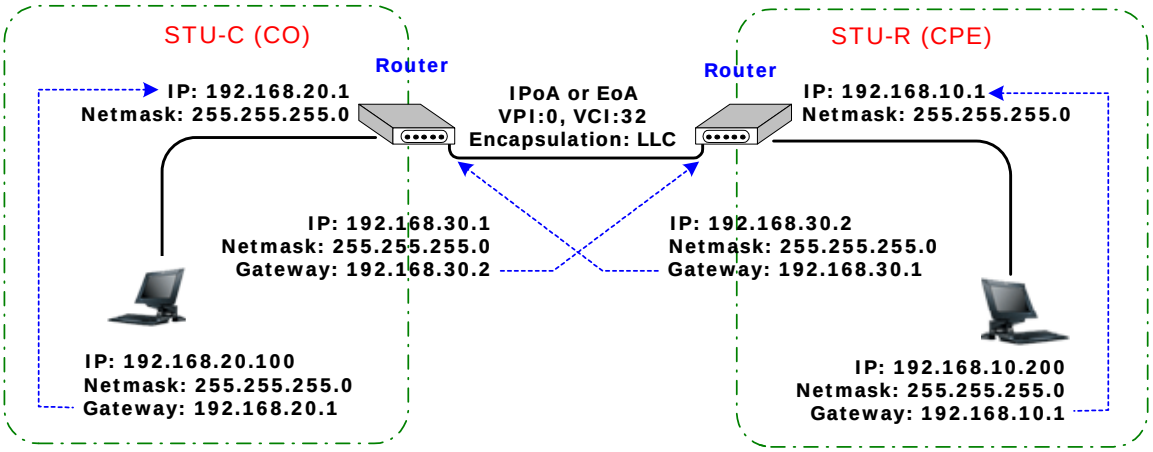


Enter **LAN** Parameters
IP: 192.168.0.2
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.2
Host Name: SOHO

Enter **WAN1** Parameters
VPI: 0
VCI: 32
Click LLC
Click Next

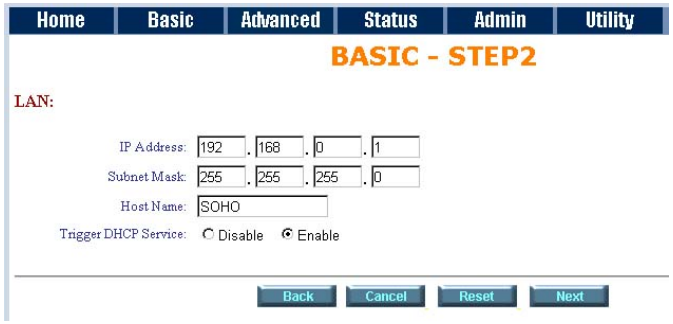
The screen will prompt the new configured parameters. Check the parameters and Click Restart
The router will reboot with the new setting.

6.6.2 LAN to LAN connection with routing mode

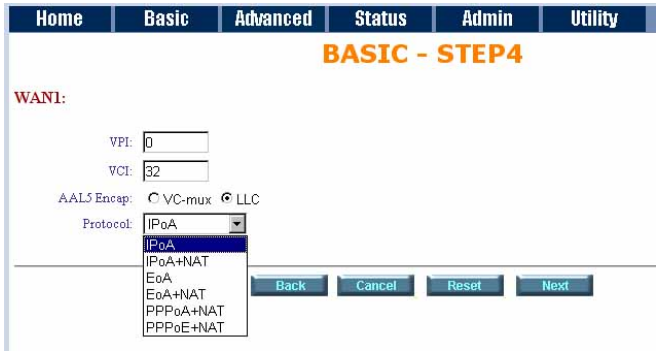


6.6.2.1 CO Side

Click ROUTE and CO Side to setup Routing mode of the Router and then click Next

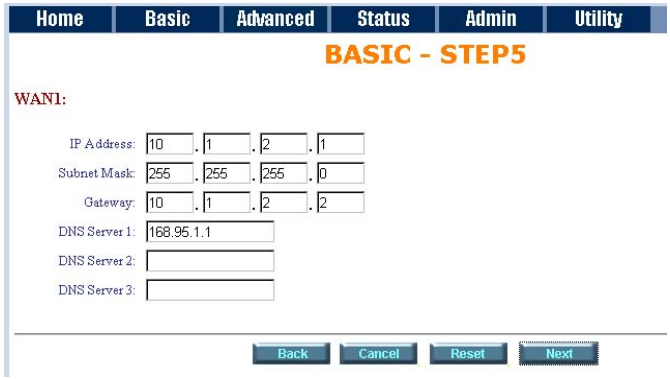


Type **LAN** parameters:
IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: Disable or Enable
For more **DHCP** service, review the chapter on DHCP Service



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 setup the IP parameters.

For more understanding about **NAT,** review the chapter of NAT/DMZ .



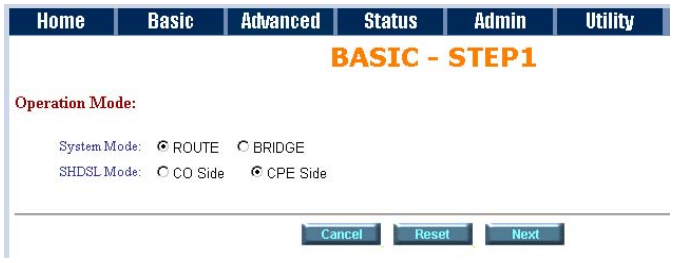
IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0
Gateway: 192.169.30.2
Click Next

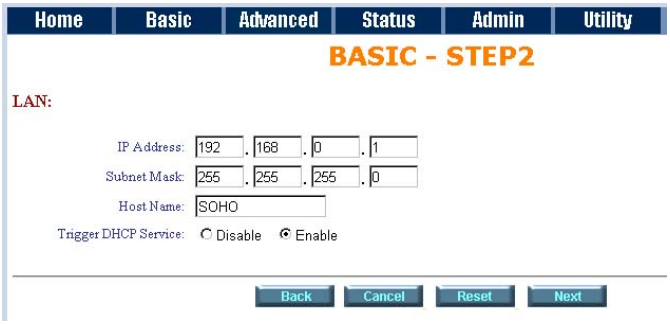
The screen will prompt the parameters that we will write in NVRAM. Check the parameters before writing in NVRAM.

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

6.6.2.2 CPE side

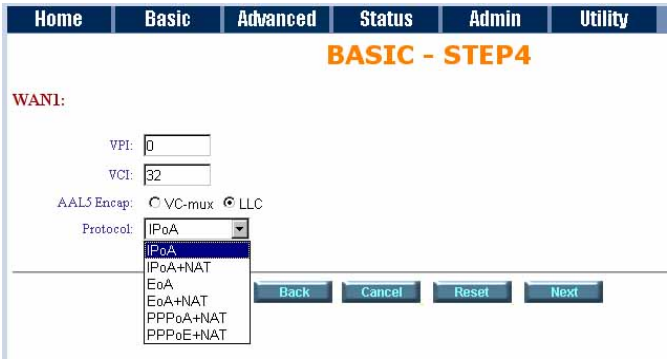
Click ROUTE and CPE Side then press Next.





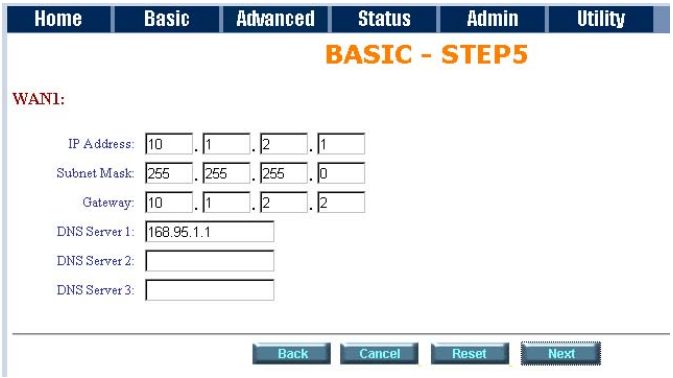
Type LAN parameters:
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: Disable or Enable
For more **DHCP** service, review the chapter of DHCP Service.

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 setup the IP parameters.

For more understanding about **NAT**, review the chapter of NAT/DMZ.



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 we will write 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.

7 Configuration via Serial Console or Telnet with Manu Driven Interface

In this section, the detail of menu-driven user interface will be described below line by line

7.1 Introduction

7.1.1 Serial Console

Check the connectivity of the RS-232 cable. Connect the male 9-pin end of console port of the router and connect the female end to a serial port of your computer.
Start your terminal access program by VT100 terminal emulation with the following parameters:

Parameter	Value
Baudrate	9600bps
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.

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

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

Note: The factory default **User** and **Password** are "admin" both.

7.1.2 Telnet

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

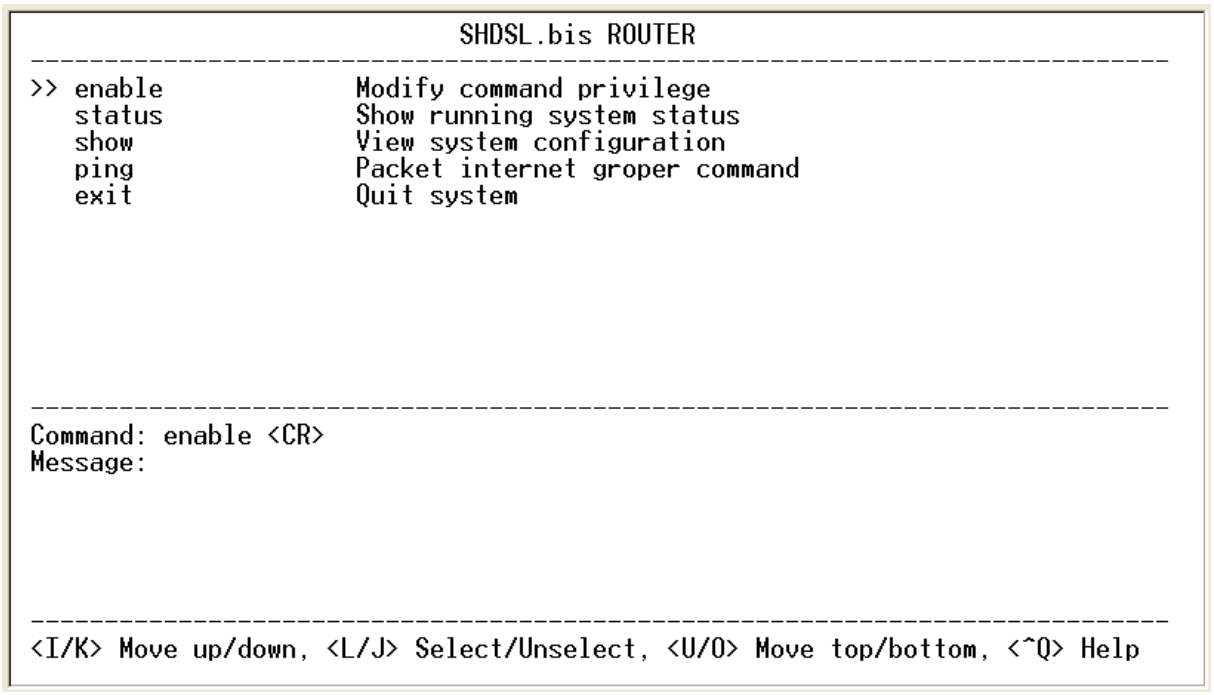
```
User: admin
Password: *****
```

Note: The default IP address is 192.168.0.1.

7.1.3 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 shall see a submenu and select "system" command in this submenu, then the system will show you the general information.



7.1.4 Window structure

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

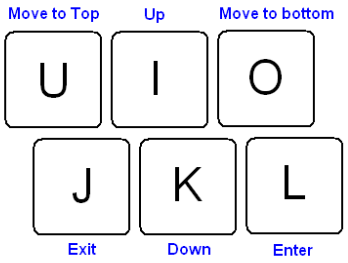
1. **Product name**: "SHDSL.bis ROUTER"
2. **Menu field**: Menu tree prompts on this field. Symbol "**>>**" indicates the cursor place.
3. **Configuring field**: You will configure the parameters in this field. **< parameters >** indicates the parameters you can choose and **< more…>** indicates that 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.

7.1.5 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] or L	Move forward to submenu
[ENTER]	Move forward to submenu
[TAB]	To choose another parameters
Ctrl + C	To quit the configuring item
Ctrl + D	Disconnection
Ctrl + U	Hot-key switch to command line interface
Ctrl + Q	Display help menu

7.2 Main menu before enable

When enter to menu on the following. 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

7.3 Enable

To setup 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 setup 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 NVRAM and reboot the router to work with new setting.

The screen will prompt as follow.

```
-------------------------------------------------------------------------------------------------
>> 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
-------------------------------------------------------------------------------------------------
```

Command Description:

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 by "**reboot**" command, or 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 are working via "**utility**" command.
exit	Quit system

7.4 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
   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
-------------------------------------------------------------------------------------------------
```

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).
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	The current and history status of firewall are shown in this command.
Ip_qos	Show the current IP QoS statistics on LAN interface
stp	Show the STP status on all LANs and WANs

7.4.1 Shdsl.bis

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

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

Show SHDSL.bis status includes the Mode, Line Rate, Current SNR Margin, Attenuation and CRC error count on both side.

7.4.2 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

7.4.3 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.

7.4.4 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 eight WAN ports.

7.4.5 Firewall

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

```
------------------------------------------------------------------------------
Monitoring Window...
<Current Firewall Status>
      Attack Type    Current Status History Status
---------------------- -------------- --------------
          SYN Attack     --------       --------
          ICMP Flood     --------       --------
           UDP Flood     --------       --------
  PING of Death Attack   --------       --------
         Land Attack     --------       --------
   IP Spoofing Attack    --------       --------
        Smurf Attack     --------       --------
       Fraggle Attack    --------       --------
---------------------- -------------- --------------
Packets dropped by DoS protect function: 0
Packets dropped by SPI filter function: 0
Packets dropped by packet filter function: 0
------------------------------------------------------------------------
```

You can view all current firewall status including number of packets dropped on DoS protect, SPI filter and Packet filter

7.4.6 IP_QoS

Move cursor " **>>** " to **IP_QoS** and press enter.
Select the Interface number from 0 to 8 (0 for LAN, 1 to 8 for WAN1 to WAN8)

```
-------------------------------------------------------------------------------
 Command: status ip_qos <0~8>
 Message: Please input the following information.
 Interface number <0~8>:0
-------------------------------------------------------------------------------



-------------------------------------------------------------------------------
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

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

You can view current IP QoS statistics for six produces per ports.

7.4.7 STP

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

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

<STP Status>
Bridge ID / Designated ROOT ID  : 8000-000379-000001 / 8000-000379-000001
ROOT Port / ROOT Path Cost      : None /     0
Max Age/Forward Delay/Hello Time:   20 /   15 /    2(secs)

           LAN1 LAN2 LAN3 LAN4 WAN1 WAN2 WAN3 WAN4 WAN5 WAN6 WAN7 WAN8
 ----------  ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
     State     D   LN    D    D    D    D    D    D    D    D    D    D
   Priority   128  128  128  128  128  128  128  128  128  128  128  128
  Path Cost   100  100  100  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 LANs 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

7.5 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 detail configuration information.
script	Configuration information will prompt in command script.

7.5.1 System information

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

```
-------------------------------------------------------------------------
Status Window...
General system information
 MCSV               :FFFF-FFFF-FFFFFFFF
 Software Version   :148D-0012-40413ADA
 Chipset            :PEF 22627
 Firmware Version   :1.1-1.5.7__002
 Hostname           :SOHO
 System Up Time     :0DAY/2HR/39MIN

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

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

7.5.2 Configuration information

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

You can view all setting using table format.

```
-------------------------------------------------------------------------
Status Window...

WAN Interface Parameters
 No   Link       IP Address/        Netmask VPI/   VCI Encap.  QoS   PCR
 -- -------- ------------------------------- ---------- ------ ----- ----
  1     IPoA    192.168.1.1/   255.255.255.0    0/   32    LLC   UBR 11392
  2 Ethernet     192.168.2.1/   255.255.255.0   0/   33    LLC   UBR 11392
  3 Ethernet     192.168.3.1/   255.255.255.0   0/   34    LLC   UBR 11392
  4     IPoA    192.168.4.1/   255.255.255.0    0/   35    LLC   UBR 11392
  5    PPPoA    192.168.5.1/   255.255.255.0    0/   36    LLC   UBR 11392
  6 Ethernet     192.168.6.1/   255.255.255.0   0/   37    LLC   UBR 11392
  7 Ethernet     192.168.7.1/   255.255.255.0   0/   38    LLC   UBR 11392
  8 Ethernet     192.168.8.1/   255.255.255.0   0/   39    LLC   UBR 11392

 No             ISP Account Username               Idle Time  SCR MBS
 -- ------------------------------------------------ --------- ---- ---
  1                                      test      10   11392   1
  2                                      test      10   11392   1
```

```
  3                                          test     10   11392   1
  3                                          test     10   11392   1
  4                                          test     10   11392   1
  5                                          test     10   11392   1
  6                                          test     10   11392   1
  7                                          test     10   11392   1
  8                                          test     10   11392   1

RIP Parameters
  <Generic RIP Parameters>
    RIP Mode    : Disable
    Auto Summary: Disable

  <Interface RIP Parameters>
   Net    Mode     Ver  Authenticate  Poison Rev.  Authenticate code
 ------- --------- ----- ------------ ------------- -----------------
  LAN 1   Disable
  WAN 1   Disable
  WAN 2   Disable
  WAN 3   Disable
  WAN 4   Disable
  WAN 5   Disable
  WAN 6   Disable
  WAN 7   Disable
  WAN 8   Disable

Static Route Parameters
    No data in the static SRT entry!

Generic Bridging Parameters
    Gateway IP address : 192.168.0.254

Static Bridging Parameters
    No data in the static bridge entry!

DHCP Server Generic Parameters
    Service          : Enable
    Interface        : LAN
    Default Gateway  : 192.168.0.1
    Subnet Mask      : 255.255.255.0
    DHCP Start IP    : 192.168.0.2
    DHCP IP Count    : 50
    Max Lease Time   : 72
    Name Server IP   : 192.168.0.1

DHCP Server Fixed Host Entries
  No    MAC  Address       IP Address
 ---- ------------------- ------------------
    1           (Empty)
    2           (Empty)
    3           (Empty)
    4           (Empty)
    5           (Empty)
    6           (Empty)
    7           (Empty)
    8           (Empty)
    9           (Empty)
   10           (Empty)

DHCP Relay Parameters
 Trigger Relay function: Disable
      Remote Server IP: 192.168.0.124

Virtual Server Mapping Pool
  No    Service Name     Protocol   Port      Host IP    / Port  Interface
 --- ------------------- ---------- ------ ------------------------ ---------
    1         (Empty)
    2         (Empty)
    3         (Empty)
    4         (Empty)
    5         (Empty)
    6         (Empty)
    7         (Empty)
    8         (Empty)
    9         (Empty)
   10         (Empty)

  No         Schedule
```

```
 --- ----------------------------
   1         (Empty)
   2         (Empty)
   3         (Empty)
   4         (Empty)
   5         (Empty)
   6         (Empty)
   7         (Empty)
   8         (Empty)
   9         (Empty)
  10         (Empty)

NAT Virtual IP Address Pool
  No    Base Address    Count
 ---- ------------------ -------
   1          (Empty)
   2          (Empty)
   3          (Empty)
   4          (Empty)
   5          (Empty)

NAT Global IP Address Pool
  No    Base Address    Count   Interface
 ---- ------------------ ------- -----------
   1          (Empty)
   2          (Empty)
   3          (Empty)
   4          (Empty)
   5          (Empty)

NAT Fixed IP Address Mapping Pool
  No    Local Address     Global Address    Interface
 ---- ------------------- ------------------- -----------
    1          (Empty)
    2          (Empty)
    3          (Empty)
    4          (Empty)
    5          (Empty)
    6          (Empty)
    7          (Empty)
    8          (Empty)
    9          (Empty)
   10          (Empty)

Packet Filter Active Parameter
    Packet Filtering Function : Disable
    Drop Fragmented Packets   : Disable

Packet Filtering Table
    No entry in the access policy table!

System Mode Parameters
 System Mode               : ROUTE MODE

SHDSL.bis Chipset Parameters
 Operation Mode             : STU-R
 Data Rate(kbps)            : n = 89
 Annex Type                 : Annex_BG

LAN Interface Parameters
 IP Type                   : Fixed
 IP Address                : 192.168.0.1
 Subnet Mask               : 255.255.255.0
 Network Type              : Global
 Hostname                  : SOHO

 DNS Proxy Parameters
 DNS Proxy Server 1 168.95.1.1
 DNS Proxy Server 2 168.95.192.1

Legal Access User Profile
  No     User  Name     UI Mode
 ---- ------------------ -----------
   1           admin      Menu
   2          (Empty)
   3          (Empty)
   4          (Empty)
   5          (Empty)
```

```
Configuration Generic Parameter
 Telnet Listening TCP Port   : 23

Trust Host IP Address
  No     IP Address
 ---- ------------------
   1          0.0.0.0
   2          (Empty)
   3          (Empty)
   4          (Empty)
   5          (Empty)
   6          (Empty)
   7          (Empty)
   8          (Empty)
   9          (Empty)
  10          (Empty)
  11          (Empty)
  12          (Empty)
  13          (Empty)
  14          (Empty)
  15          (Empty)
  16          (Empty)

SNMP Community Pool
  No           Community             Access Right
 ---- -------------------------------- ------------------
   1                     (Empty)
   2                     (Empty)
   3                     (Empty)
   4                     (Empty)
   5                     (Empty)

SNMP Trap Host Pool
  No           Trap                IP Address      Version
 ---- -------------------------------- ------------------ -------
   1                     private     192.168.0.254  Disable
   2                     private     192.168.0.254  Disable
   3                     private     192.168.0.254  Disable
   4                     private     192.168.0.254  Disable
   5                     private     192.168.0.254  Disable

Time Synchronization Parameters
 Method                    : Sync with PC
 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

Virtual LAN Parameter
VLAN Mode                 : Disable

Virtual LAN Table
 No  VID  LAN1 LAN2 LAN3 LAN4 WAN1 WAN2 WAN3 WAN4 WAN5 WAN6 WAN7 WAN8
 -- ----- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
  1    1   1    1    1    1    1    1    1    1    1    1    1    1
  2    0   -    -    -    -    -    -    -    -    -    -    -    -
  3    0   -    -    -    -    -    -    -    -    -    -    -    -
  4    0   -    -    -    -    -    -    -    -    -    -    -    -
  5    0   -    -    -    -    -    -    -    -    -    -    -    -
  6    0   -    -    -    -    -    -    -    -    -    -    -    -
  7    0   -    -    -    -    -    -    -    -    -    -    -    -
  8    0   -    -    -    -    -    -    -    -    -    -    -    -

IP QoS Generic Parameter
   IP QoS Function         : Disable

IP QoS Policy Table
   No entry in the policy table!

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

7.5.3 Configuration with Script format

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

You can view all setting using script format.

```
------------------------------------------------------------------------
Status Window...

Showing System Configuration.....

setup mode Route
setup shdsl.bis mode STU-R
setup shdsl.bis link M-Pair
setup shdsl.bis n*64 89
setup shdsl.bis tcpam Auto
setup shdsl.bis margin 5
setup wan 1 protocol IPoA
setup wan 1 address 192.168.1.1 255.255.255.0
setup wan 1 vpi_vci 0 32
setup wan 1 encap LLC
setup wan 1 qos class UBR
setup wan 1 qos pcr 11392
setup wan 1 qos scr 11392
setup wan 1 isp test test 10
setup wan 1 ip_type Dynamic
setup wan 2 protocol Ethernet
setup wan 2 address 192.168.2.1 255.255.255.0
setup wan 2 vpi_vci 0 33
setup wan 2 encap LLC
setup wan 2 qos class UBR
setup wan 2 qos pcr 11392
setup wan 2 qos scr 11392
setup wan 2 isp test test 10
setup wan 2 ip_type Dynamic
setup wan 3 protocol Ethernet
setup wan 3 address 192.168.3.1 255.255.255.0
setup wan 3 vpi_vci 0 34
setup wan 3 encap LLC
setup wan 3 qos class UBR
setup wan 3 qos pcr 11392
setup wan 3 qos scr 11392
setup wan 3 isp test test 10
setup wan 3 ip_type Dynamic
setup wan 4 protocol IPoA
setup wan 4 address 192.168.4.1 255.255.255.0
setup wan 4 vpi_vci 0 35
setup wan 4 encap LLC
setup wan 4 qos class UBR
setup wan 4 qos pcr 11392
setup wan 4 qos scr 11392
setup wan 4 isp test test 10
setup wan 4 ip_type Dynamic
setup wan 5 protocol PPPoA
setup wan 5 address 192.168.5.1 255.255.255.0
setup wan 5 vpi_vci 0 36
setup wan 5 encap LLC
setup wan 5 qos class UBR
setup wan 5 qos pcr 11392
setup wan 5 qos scr 11392
setup wan 5 isp test test 10
setup wan 5 ip_type Dynamic
setup wan 6 protocol Ethernet
setup wan 6 address 192.168.6.1 255.255.255.0
setup wan 6 vpi_vci 0 37
setup wan 6 encap LLC
setup wan 6 qos class UBR
setup wan 6 qos pcr 11392
setup wan 6 qos scr 11392
setup wan 6 isp test test 10
setup wan 6 ip_type Dynamic
setup wan 7 protocol Ethernet
setup wan 7 address 192.168.7.1 255.255.255.0
setup wan 7 vpi_vci 0 38
setup wan 7 encap LLC
```

```
setup wan 7 qos class UBR
setup wan 7 qos pcr 11392
setup wan 7 qos scr 11392
setup wan 7 isp test test 10
setup wan 7 ip_type Dynamic
setup wan 8 protocol Ethernet
setup wan 8 address 192.168.8.1 255.255.255.0
setup wan 8 vpi_vci 0 39
setup wan 8 encap LLC
setup wan 8 qos class UBR
setup wan 8 qos pcr 11392
setup wan 8 qos scr 11392
setup wan 8 isp test test 10
setup wan 8 ip_type Dynamic
setup bridge gateway 192.168.0.254
setup vlan mode Disable
setup vlan modify 1 1 111111111111
setup vlan modify 2 0 000000000000
setup vlan modify 3 0 000000000000
setup vlan modify 4 0 000000000000
setup vlan modify 5 0 000000000000
setup vlan modify 6 0 000000000000
setup vlan modify 7 0 000000000000
setup vlan modify 8 0 000000000000
setup vlan pvid 1 1
setup vlan pvid 2 1
setup vlan pvid 3 1
setup vlan pvid 4 1
setup vlan pvid 5 1
setup vlan pvid 6 1
setup vlan pvid 7 1
setup vlan pvid 8 1
setup vlan pvid 9 1
setup vlan pvid 10 1
setup vlan pvid 11 1
setup vlan pvid 12 1
setup vlan link_mode 1 Access
setup vlan link_mode 2 Access
setup vlan link_mode 3 Access
setup vlan link_mode 4 Access
setup vlan link_mode 5 Access
setup vlan link_mode 6 Access
setup vlan link_mode 7 Access
setup vlan link_mode 8 Access
setup vlan link_mode 9 Access
setup vlan link_mode 10 Access
setup vlan link_mode 11 Access
setup vlan link_mode 12 Access
setup stp active Disable
setup route rip generic Disable Disable
setup route rip lan 1 version 2
setup route rip lan 1 attrib Disable None Enable
setup route rip wan 1 version 2
setup route rip wan 1 attrib Disable None Enable
setup lan 1 address 192.168.0.1 255.255.255.0
setup lan 1 attrib Global
setup lan 1 ip_type Fixed
setup ip_share pat modify 1 interface 1
setup ip_share pat modify 2 interface 1
setup ip_share pat modify 3 interface 1
setup ip_share pat modify 4 interface 1
setup ip_share pat modify 5 interface 1
setup ip_share pat modify 6 interface 1
setup ip_share pat modify 7 interface 1
setup ip_share pat modify 8 interface 1
setup ip_share pat modify 9 interface 1
setup ip_share pat modify 10 interface 1
setup firewall level Basic
setup firewall dos_protect syn_flood Disable 200
setup firewall dos_protect icmp_flood Disable 200
setup firewall dos_protect udp_flood Disable 200
setup firewall dos_protect ping_death Disable
setup firewall dos_protect land_attack Disable
setup firewall dos_protect ip_spoof Disable
setup firewall dos_protect smurf_attack Disable
setup firewall dos_protect fraggle_attack Disable
setup ip_qos active Disable
setup dhcp generic active Enable
```

```
setup dhcp generic gateway 192.168.0.1
setup dhcp generic netmask 255.255.255.0
setup dhcp generic ip_range 192.168.0.2 50
setup dhcp generic lease_time 72
setup dhcp generic name_server1 192.168.0.1
setup dhcp relay Disable 192.168.0.124
setup dns_proxy 168.95.1.1 168.95.192.1
setup hostname SOHO
admin passwd ****
admin id root
admin user modify 1 attrib Menu
admin user modify 1 profile admin *****
admin user modify 2 attrib Command
admin user modify 3 attrib Command
admin user modify 4 attrib Command
admin user modify 5 attrib Command
admin security port 23
admin security ip_pool modify 1 0.0.0.0
admin snmp community 1 edit Disable private Denied
admin snmp community 2 edit Disable private Denied
admin snmp community 3 edit Disable private Denied
admin snmp community 4 edit Disable private Denied
admin snmp community 5 edit Disable private Denied
admin snmp trap 1 edit Disable 192.168.0.254 private
admin snmp trap 2 edit Disable 192.168.0.254 private
admin snmp trap 3 edit Disable 192.168.0.254 private
admin snmp trap 4 edit Disable 192.168.0.254 private
admin snmp trap 5 edit Disable 192.168.0.254 private
admin sntp method SyncWithPC
admin sntp service Enable
admin sntp time_server1 ntp-2.vt.edu
admin sntp time_server2 ntp.drydog.com
admin sntp time_server3 ntp1.cs.wisc.edu
admin sntp update_rate 3600
admin sntp time_zone 8

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

7.6 Write

For any changes of configuration, you must write the new configuration to NVRAM 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.

7.7 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.

7.8 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

7.9 Administration

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

7.9.1 User Profile

You can use **user** command to clear, modify and list the user profile. You can setup 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 follow.

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

There are two UI mode, **command** and **menu** mode, to setup 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 follow:

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

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

Finally, you can use **list** command to check the listing of five profiles including on user name and their UI mode.

The screen will prompt as follow:

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

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

7.9.2 Security

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

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

```
-------------------------------------------------------------------------------------------------
>> port           Configure telnet TCP port
   ip_pool        Legal client IP address pool
   list           Show security profile
-------------------------------------------------------------------------------------------------
```

Move the cursor to **port** and press enter. You can setup port number form 1 to 65534.

Move the cursor to **IP Pool** and press enter, there are sixteen legal IP address 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.

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.

7.9.3 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 support MIB I & II.

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

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

5 entries of SNMP community 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.
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

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

7.9.4 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 to change 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.

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

7.9.5 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, which 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's internal timer. If you choose SNTPv4, the router will use the protocol to synchronize with the time server. For synchronization the time server with SNTP v4, needs to configure service, **time_server** and **time_zone**. For synchronization with PC, doesn't 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
   Update_rate    Configure update period
   time_zone      Configure GMT time zone offset
   list           Show SNTP configuration
```

Please follow the below procedures to configure SNTP v4 time synchronization.

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. There will have a (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
-------------------------------------------------------------------------
```

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

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

7.10 Utility

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.

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

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

7.10.1 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.

7.10.2 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..

7.10.3 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.

7.11 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.

7.12 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.bis parameters
   wan            Configure WAN interface profile
   bridge         Configure transparent bridging
   vlan           Configure virtual LAN parameters
   stp            Configure bridge STP parameters
   route          Configure routing parameters
   lan            Configure LAN interface profile
   ip_share       Configure NAT/PAT parameters
   firewall       Configure Firewall parameters
   ip_qos         Configure IP QoS parameters
   dhcp           Configure DHCP parameters
   dns_proxy      Configure DNS proxy parameters
   hostname       Configure local host name
   default        Restore factory default setting
```

7.12.1 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
-----------------------------------------------------------------------
```

7.12.2 SHDSL.bis

You can setup the SHDSL.bis parameters by the command **shdsl.bis**. Move the cursor " **>>** " to shdsl.bis 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
    clear          Clear current CRC error count
    margin         Configure SHDSL.bis SNR margin
    tcpam          Configure shdsl.bis TCPAM type
```

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.

Link type will be 2-wire, M-Pair, M-Pair (Conexant), Auto_Fall_Back, StandBy, and Multi-link. 4-wire product can be worked under 2-wire mode.

You can setup the data rate by the multiple of 64Kbps where n is from 3 to 89.
If the router is 4 wire models and doesn't use on 2-wire mode, the line rate will double from 2-wire model's setting.
For adaptive mode, you have to setup n=0. The router will adapt the data rate according to the line status.

		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)

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

Clear command can clear CRC error count.

Generally, you cannot need to change SNR margin, which range is 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 is SNR margin; the better is line connection quality. 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.

There are two TCPAM setting on SHDSL.bis: TCPAM-16 or TCPAM-32. In most case, 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 use.

7.12.3 WAN

The router supports 8 PVC, private virtual circuit, and so you can setup 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
```

There are four types of protocols, IPoA, EoA, PPPoA and PPPoE, which you can setup.

For dynamic IP of PPPoA and PPPoE, you do not need to setup IP address and subnet mask.

There is a unique VPI 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).*

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

You can setup 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.*

ISP command can configure account name, password and idle time. Idle time is from 0 minute to 300 minutes.
Most of the ISP use dynamic IP for PPP connection but some of the ISP use static IP. You can configure the IP type: **Dynamic**, **Fixed** and **Unnumbered**. The setting is via **ip_type** command.

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

7.12.4 Bridge

You can setup the bridge parameters in bridge command. If the product is configured as a router, you do not want to setup the bridge parameters.

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

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

You can setup default gateway IP via gateway command.

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

```
>> deny_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.

After enter **add** menu, the screen will prompt as follow

```
>> 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
```

7.12.5 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. 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 VID
   link_mode     Modify port link type
   List          Show VLAN configuration
```

To active the VLAN function, move the cursor " **>>** " to mode and press enter. The products support two types of VLAN, 802.11q and Port-Based. 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 destination MAC address and its associated port.

7.12.6 802.11Q VLAN

Follow the following steps to configure 802.11q VLAN.

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

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

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)<111111111111>:111111000000
-------------------------------------------------------------------------
```

For each VLAN, VLAN ID is a unique number among 1~4095.

VLAN port status is a 12-digit binary number whose bit-1 location indicates the VLAN port membership in which 4MSBs and 8MSB represents LAN ports and WAN port, respectively. For example: the above setting means that the VID 20 member port includes LAN1, LAN2 and WAN.

The member ports are tagged members. Use PVID command to change the member port to untagged members

To assign PVID (Port VID), move the cursor ">>" to PVID and press enter. The port index 1 to 4 represents LAN1 to LAN4 respectively and port index 5 to 12 represents WAN1 to WAN8. VID value is the group at which you want to assign the PVID of the port. PVID is

```
-------------------------------------------------------------------
Command: setup vlan pvid <1~12> <1~4094>
Message: Please input the following information.

Port index <1~12>: 1
VID Value (Enter for default) <10>: 10
-------------------------------------------------------------------
```

To modify the link type of the port, move the cursor to link mode and press enter. There are two types of link: access and trunk. Trunk link will send the tagged packet form the port and access link will send un-tagged packet form the port. Port index 1 to 4 represents LAN1 to LAN4 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
-------------------------------------------------------------------
```

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

7.12.7 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
-------------------------------------------------------------------------------------------------
```

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

7.12.8 Route

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

```
-------------------------------------------------------------------------------------------------
>> static         Configure static routing table
   Rip            Configure RIP tool
-------------------------------------------------------------------------------------------------
```

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 Cable/DSL Firewall 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 setup 20 sets of static route in static command. After entering **static** menu, the screen will show as follow:

```
>> 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.

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

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

To configure Routing Information Protocol (RIP), you can use **rip** command to setup 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 command can setup RIP mode and auto summery mode.

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

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 follow:

```
>> 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.

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

7.12.9 LAN

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

```
>> Ip_type        IP type
   Address        LAN IP address and subnet mask
   Attrib         NAT network type
```

7.12.10 IP share

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

7.12.10.1 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
```

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 range of virtual IP address, delete virtual IP address, and show virtual IP address.

```
>> 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
-----------------------------------------------------------------------
```

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.
To setup 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 bind command.

```
-----------------------------------------------------------------------
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.

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

```
-------------------------------------------------------------------------------------------------------
>> 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 entries via **range** command.

```
-------------------------------------------------------------------------
Command: setup ip_share nat fixed modify <1~1o> <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
-------------------------------------------------------------------------
```

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

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

Fixed NAT mapping entry number <1~5>: 1
Active interface number (Enter for default) <1~8>: 1
-------------------------------------------------------------------------
```

You can delete fixed NAT mapping entry- from 1 to 5- by using **delete** command.

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

7.12.10.2 PAT

Port Address Translation (PAT) is a feature of a network 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 there is generally 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>
Message: Please input the following information.

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

After key in enter, the screen will prompt as below.

```
-------------------------------------------------------------------------------------------------------
>> 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 setup via **protocol** command.

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

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

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

7.12.10.3 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 setup demilitarized zone, move the cursor ">>" to **dmz** and press enter.

```
-------------------------------------------------------------------------------------------------------
>> active        Trigger 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> <1~10>
Message: Please input the following information.

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

7.12.11 Firewall

7.12.11.1 Firewall security level

The product supports advanced firewall. To setup the advanced firewall, you can use **firewall** to configure.

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

There are three level 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, all DoS protection, and the SPI filter function.

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 than the default SPI filter. 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.

7.12.11.2 Packet Filtering

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

```
>> active         Trigger packet filtering function
   drop_flag      Drop fragmented packets
   Add            Add packet filtering rule
   Delete         Delete packet filtering rule
   Modify         Modify packet filtering rule
   Exchange       Exchange the filtering rules
   list           Show packet filtering table
```

Command	Description
Active	Enable packet filtering function
Drop_flag	Enable drop fragmented packets function
Add	Add packet filtering rule
Delete	Delete packet filtering rule
Modify	Modify packet filtering rules
Exchange	Exchange the filtering rules
List	Show all the packet filtering table

Add the packet filtering rule via **add** 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
```

Command	Description
Protocol	Configure protocol type (ANY,TCP,UDP,ICMP,GRE,RSVP,ESP,AH)
Direction	Configure direction mode (INBOUND,OUTBOUND)
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 (ON,OFF)
Begin	The schedule of beginning time
End	The schedule of ending time
Action	Configure action mode (DENY, PERMIT)

7.12.11.3 DoS Protection

DoS protection parameters can be configured in dos_protect menu.
Move the cursor to **dos_protect** 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
```

Command	Description
syn_flood	Enable protecting SYN flood attack (Threshold packets per second : 0~700)
icmp_flood	Enable protecting ICMP flood attack (Threshold packets per second : 0~700)
udp_flood	Enable protecting UDP flood attack (Threshold packets per second : 0~700)
ping_death	Enable protecting PING of death attack
land_attack	Enable protecting land attack
ip_spoff	Enable protecting IP spoofing attack
smurf_attack	Enable protecting smurf 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 (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 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.

7.12.12 IPQoS

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

To configure IP QoS function, move the cursor to **IPQoS** 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
```

Command	Description
Active	Enable the IP QoS function
Add	Add parameters of IP QoS
Delete	Delete the IP QoS parameter
Modify	Modify the IP QoS parameter
List	View the IP QoS configuration

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
```

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 port range
Description	Define the description of policy
Enable	Enable the policy
Precedence	Define the priority of the policy

7.12.13 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
```

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

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 as the same time.
There can be set up to 10 maximum fixed host IP address.
Active the DHCP relay and remote server IP address via **relay** command

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

7.12.14 DNS proxy

Enter the IP address via 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.

7.12.15 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.

7.12.16 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 : 4-wire G.SHDSL.bis Bridge Router w/4-port switch
*Model Number : GRT-504

* 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)
Safety	EN 60950	(2000)

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 **Allen Huang**

Position / Title : **Product Manager**

Taiwan	**26th Sep., 2008**	Allen
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