

## **XL-GRT-402SB**

Bridge/router G.SHDSL bis/Ethernet

User's Guide



## TABLE OF CONTENTS

<b>1</b>	<b>DESCRIPTIONS</b>	<b>4</b>
1.1	FEATURES	4
1.2	SPECIFICATION	4
1.3	APPLICATIONS	6
<b>2</b>	<b>YOURS FIREWALL</b>	<b>7</b>
2.1	TYPES OF FIREWALL	7
2.1.1	Packet Filtering	7
2.1.2	Circuit Gateway	9
2.1.3	Application Gateway	9
2.2	DENIAL OF SERVICE ATTACK	10
<b>3</b>	<b>YOURS VLAN (VIRTUAL LOCAL AREA NETWORK)</b>	<b>12</b>
3.1	SPECIFICATION	12
3.2	FRAME SPECIFICATION	12
3.3	APPLICATIONS	13
<b>4</b>	<b>GETTING TO KNOW ABOUT THE ROUTER</b>	<b>15</b>
4.1	FRONT PANEL	15
4.2	REAR PANEL	16
4.3	SHDSL.BIS LINE CONNECTOR	17
4.4	CONSOLE CABLE	17
<b>5</b>	<b>CONFIGURATION TO THE ROUTER</b>	<b>18</b>
5.1	STEP 1: CHECK THE ETHERNET ADAPTER IN PC OR NB	18
5.2	STEP 2: CHECK THE WEB BROWSER IN PC OR NB	18
5.3	STEP 3: CHECK THE TERMINAL ACCESS PROGRAM	18
5.4	STEP 4: DETERMINE CONNECTION SETTING	18
5.5	STEP 5: INSTALL THE SHDSL.BIS ROUTER	19
<b>6</b>	<b>CONFIGURATION VIA WEB BROWSER</b>	<b>21</b>
<b>7</b>	<b>BASIC SETUP</b>	<b>23</b>
7.1	BRIDGE MODE	23
7.2	ROUTING MODE	24
7.2.1	DHCP Server	25
7.2.2	DHCP Client	26
7.2.3	DHCP relay	26
7.2.4	PPPoE or PPPoA	27

7.2.5	<i>IPoA or EoA</i> .....	29
<b>8</b>	<b>ADVANCED SETUP</b> .....	<b>31</b>
8.1	SHDSL.BIS.....	31
8.2	WAN.....	33
8.3	BRIDGE.....	35
8.4	VLAN.....	36
8.5	ETHERNET.....	37
8.6	ROUTE.....	38
8.7	NAT/DMZ.....	40
8.8	VIRTUAL SERVER.....	42
8.9	FIREWALL.....	43
8.10	IP QoS.....	48
<b>9</b>	<b>ADMINISTRATION</b> .....	<b>50</b>
9.1	SECURITY.....	50
9.2	SNMP.....	51
9.3	TIME SYNC.....	52
<b>10</b>	<b>UTILITY</b> .....	<b>54</b>
10.1	SYSTEM INFO.....	54
10.2	CONFIG TOOL.....	54
10.3	UPGRADE.....	55
10.4	LOGOUT.....	55
10.5	RESTART.....	55
<b>11</b>	<b>STATUS</b> .....	<b>56</b>
<b>12</b>	<b>LAN-TO-LAN CONNECTION WITH BRIDGE MODE</b> .....	<b>57</b>
12.1	CO SIDE.....	57
12.2	CPE SIDE.....	58
<b>13</b>	<b>LAN TO LAN CONNECTION WITH ROUTING MODE</b> .....	<b>59</b>
13.1	CO SIDE.....	59
13.2	CPE SIDE.....	60
<b>14</b>	<b>CONFIGURATION VIA SERIAL CONSOLE OR TELNET WITH MANU DRIVEN INTERFACE</b> .....	<b>61</b>
14.1	SERIAL CONSOLE.....	61
14.2	TELNET.....	61
14.3	OPERATION INTERFACE.....	61

14.4	WINDOW STRUCTURE .....	62
14.5	MENU DRIVEN INTERFACE COMMANDS.....	63
14.6	MENU TREE .....	63
14.7	CONFIGURATION .....	65
14.8	STATUS .....	66
14.9	SHOW .....	67
14.10	WRITE .....	68
14.11	REBOOT.....	69
14.12	PING .....	70
14.13	ADMINISTRATION .....	71
14.13.1	User Profile .....	71
14.13.2	Security.....	72
14.13.3	SNMP.....	72
14.13.4	Supervisor Password and ID.....	73
14.13.5	SNTP.....	73
14.14	UTILITY .....	75
14.15	EXIT .....	75
14.16	SETUP .....	75
14.16.1	Mode.....	76
14.16.2	SHDSL.bis .....	76
14.16.3	WAN.....	77
14.16.4	Bridge .....	78
14.16.5	VLAN .....	79
14.16.6	802.11Q VLAN.....	79
14.16.7	STP .....	80
14.16.8	Route.....	80
14.16.9	LAN.....	82
14.16.10	IP share.....	82
14.16.11	NAT.....	82
14.16.12	PAT.....	84
14.16.13	DMZ.....	85
14.16.14	Firewall.....	86
14.16.15	Packet Filtering .....	86
14.16.16	DoS Protection.....	87
14.16.17	IPQoS .....	87
14.16.18	DHCP .....	88
14.16.19	DNS proxy.....	89
14.16.20	Host name .....	90
14.16.21	Default .....	90

# 1 Descriptions

The SHDSL.bis (Symmetric High Speed Digital Subscriber Loop) routers comply with G.991.2(2004) standard with 10/100 Base-T auto-negotiation. It provides business-class, multi-range from 192Kbps to 5.696Mbps (for 2-wire mode) and 384Kbps to 11.392Mbps (4-wire router) payload rates over exiting single-pair copper wire. The SHDSL.bis routers are designed not only to optimize the service bit rate from central office to customer premises also it integrates high-end Bridging/Routing capabilities with advanced functions of Multi-DMZ, virtual server mapping and VPN pass-through.

Because of rapid growth of network, virtual LAN has become one of the major new areas in internetworking industry. The SHDSL.bis routers support port-based and IEEE 802.1q VLAN over ATM network.

The firewall routers provide not only advanced functions, Multi-DMZ, virtual server mapping and VPN pass-through but advanced firewall, SPI, NAT, DoS protection serving as a powerful firewall to protect from outside intruders of secure connection.

The 4-port routers support four ports 10Base-T /100Base-T auto-negotiation and auto-MDIX switching ports to meet the enterprise need.

The SHDSL.bis routers allow customers to leverage the latest in broadband technologies to meet their growing data communication needs. Through the power of SHDSL.bis products, you can access superior manageability and reliability.

## 1.1 Features

- ✧ Easy configuration and management with password control for various application environments
- ✧ Efficient IP routing and transparent learning bridge to support broadband Internet services
- ✧ VPN pass-through for safeguarded connections
- ✧ Virtual LANs (VLANs) offer significant benefit in terms of efficient use of bandwidth, flexibility, performance and security
- ✧ Build-in advanced SPI firewall (Firewall router)
- ✧ Four 10/100Mbps Auto-negotiation and Auto-MDIX switching port for flexible local area network connectivity (4-port router)
- ✧ DMZ host/Multi-DMZ/Multi-NAT enables multiple workstations on the LAN to access the Internet for the cost of IP address
- ✧ Fully ATM protocol stack implementation over SHDSL.bis
- ✧ PPPoA and PPPoE support user authentication with PAP/CHAP/MS-CHAP
- ✧ SNMP management with SNMPv1/SNMPv2 agent and MIB II
- ✧ Getting enhancements and new features via Internet software upgrade

## 1.2 Specification

### Routing

- Support IP/TCP/UDP/ARP/ICMP/IGMP protocols
- IP routing with static routing and RIPv1/RIPv2 (RFC1058/2453)
- IP multicast and IGMP proxy (RFC1112/2236)
- Network address translation (NAT/PAT) (RFC1631)
- NAT ALGs for ICQ/Netmeeting/MSN/Yahoo Messenger
- DNS relay and caching (RFC1034/1035)
- DHCP server, client and relay (RFC2131/2132)
- IP precedence (RFC 791) (Firewall router)

### Bridging

- IEEE 802.1D transparent learning bridge
- IEEE 802.1q VLAN
- Port-based VLAN (4-port router)
- Spanning tree protocol

**Security**

- DMZ host/Multi-DMZ/Multi-NAT function
- Virtual server mapping (RFC1631)
- VPN pass-through for PPTP/L2TP/IPSec tunneling
- Natural NAT firewall
- Advanced Stateful packet inspection (SPI) firewall (Firewall Router)
- Application level gateway for URL and keyword blocking (Firewall Router)
- User access control: deny certain PCs access to Internet service (Firewall Router)

**Management**

- Easy-to-use web-based GUI for quick setup, configuration and management
- Menu-driven interface/Command-line interface (CLI) for local console and Telnet access
- Password protected management and access control list for administration
- SNMP management with SNMPv1/SNMPv2 (RFC1157/1901/1905) agent and MIB II (RFC1213/1493)
- Software upgrade via web-browser/TFTP server

**ATM**

- Up to 8 PVCs
- OAM F5 AIS/RDI and loopback
- AAL5

**ATM QoS**

- UBR (Unspecified bit rate)
- CBR (Constant bit rate)
- VBR-rt (Variable bit rate real-time)
- VBR-nrt (Variable bit rate non-real-time)

**AAL5 Encapsulation**

- VC multiplexing and SNAP/LLC
- Ethernet over ATM (RFC 2684/1483)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)

**PPP**

- PPP over Ethernet for fixed and dynamic IP (RFC 2516)
- PPP over ATM for fixed and dynamic IP (RFC 2364)
- User authentication with PAP/CHAP/MS-CHAP

**WAN Interface**

- SHDSL.bis: ITU-T G.991.2 (2004) Annex A/B/F/G
- Encoding scheme: 16-TCPAM, 32-TCPAM,
- Data Rate: N x 64Kbps ,N=3~89, 0 for adaptive, 89 as default (2-wire mode)
- Data Rate: N x 128kbps (N= 3 ~ 89, 89 as default) (4-wire Router)
- Impedance: 135 ohms

**LAN Interface**

- 4-ports switching hub (4-port router)
- 10/100 Base-T auto-sensing and auto-negotiation
- Auto-MDIX (4-port router)

**Hardware Interface**

- WAN: RJ-45
- LAN: RJ-45 x 4 (4-port router) or RJ-45 x 1 (1-port router)
- Console: RS232 female
- RST: Reset button for factory default

**Indicators**

- General: PWR
- WAN: LNK, ACT
- LAN: 10M/ACT, 100M/ACT (1-port router)

- LAN: 1, 2, 3, 4 (4-port router)
- SHDSL.bis: ALM

**Physical/Electrical**

- Dimensions: 18.7 x 3.3 x 14.5cm (WxHxD)
- Power: 100~240VAC (via power adapter)
- Power consumption: 9 watts max
- Temperature: 0~45 ° C
- Humidity: 0%~95%RH (non-condensing)

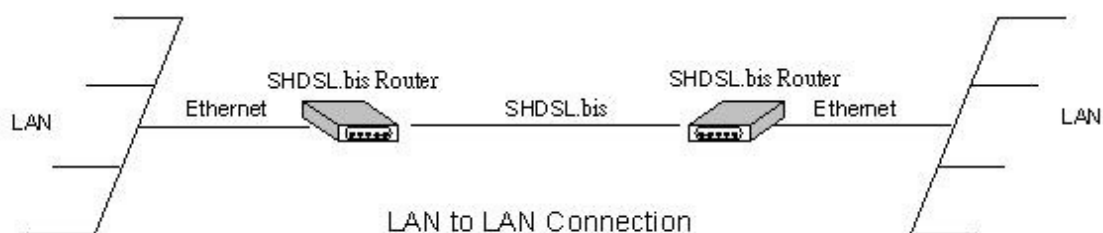
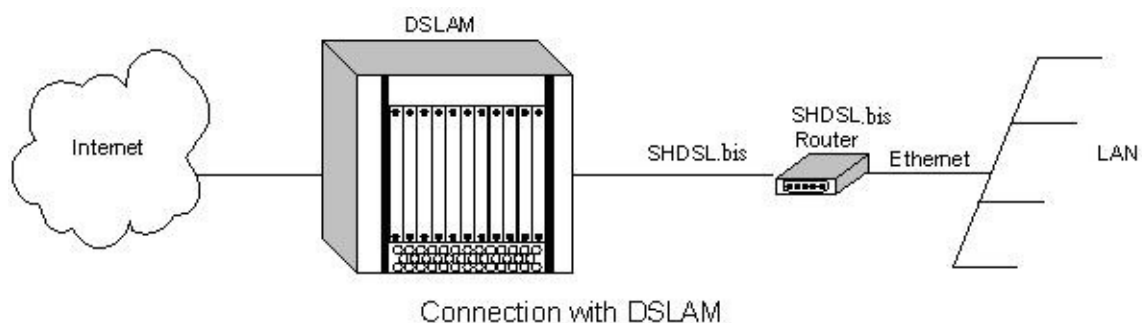
**Memory**

- 2MB Flash Memory, 8MB SDRAM

**Products' Information**

- G.shdsl.bis 2-wire router/bridge with 1-port LAN
- G.shdsl.bis 2-wire router/bridge with 1-port LAN VLAN and business class firewall
- G.shdsl.bis 2-wire router/bridge with 4-port switching hub LAN
- G.shdsl.bis 2-wire router/bridge with 4-port switching hub LAN, VLAN and business class firewall
- G.shdsl.bis 4-wire router/bridge with 4-port switching hub LAN
- G.shdsl.bis 4-wire router/bridge with 4-port switching hub LAN, VLAN and business class firewall

**1.3 Applications**

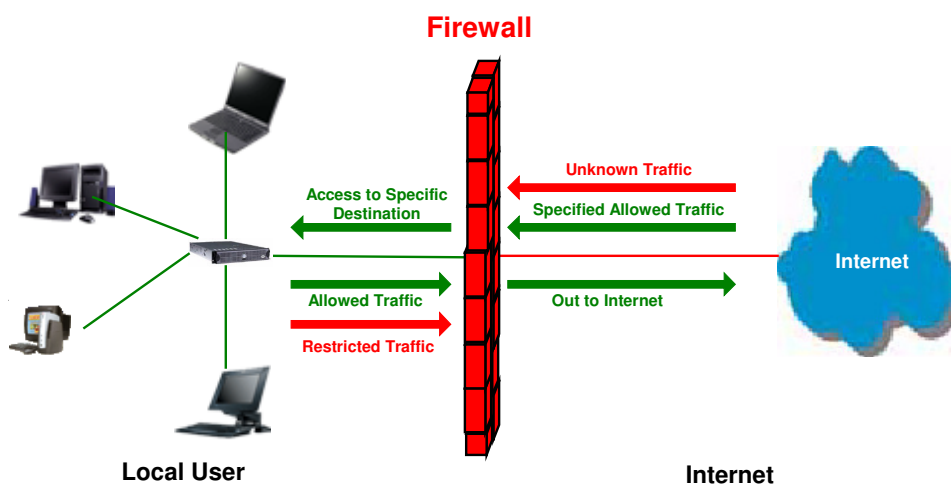


## 2 Yours Firewall

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 modems 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.



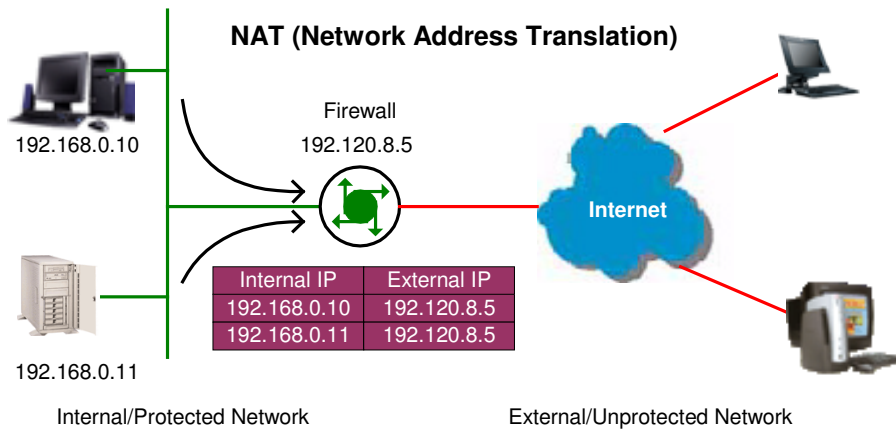
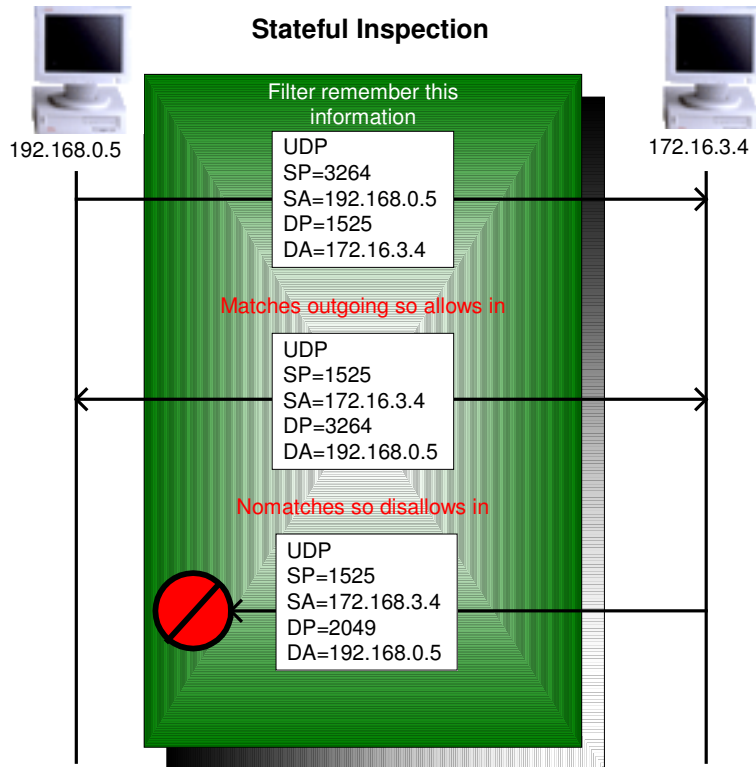
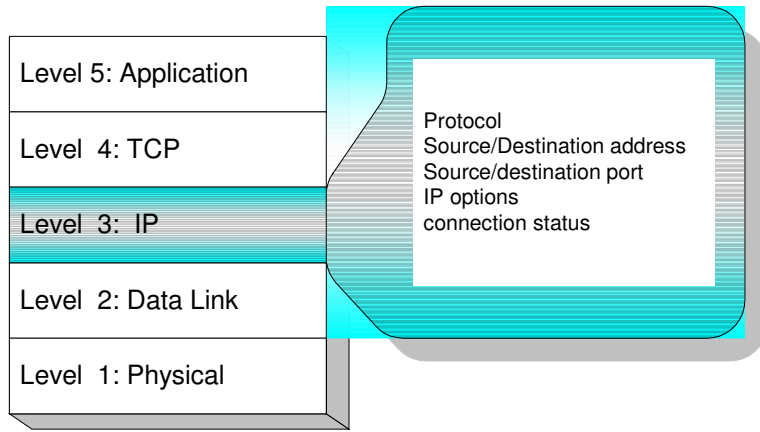
### 2.1 Types of Firewall

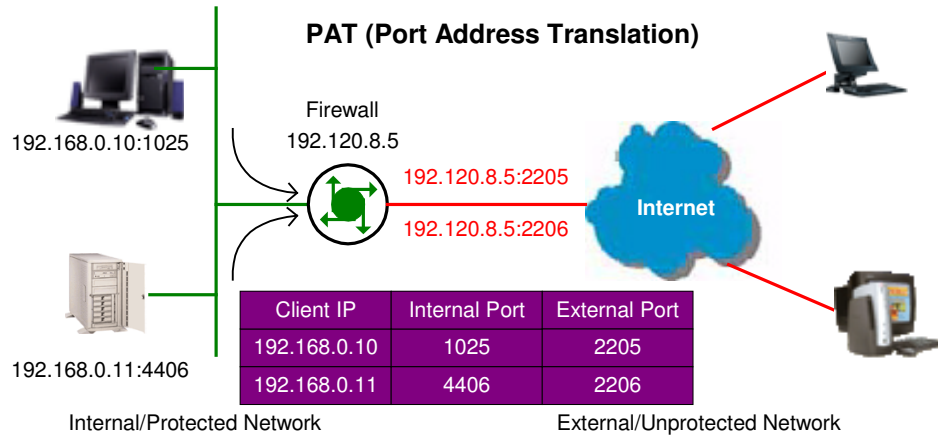
There are three types of firewall:

#### 2.1.1 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.

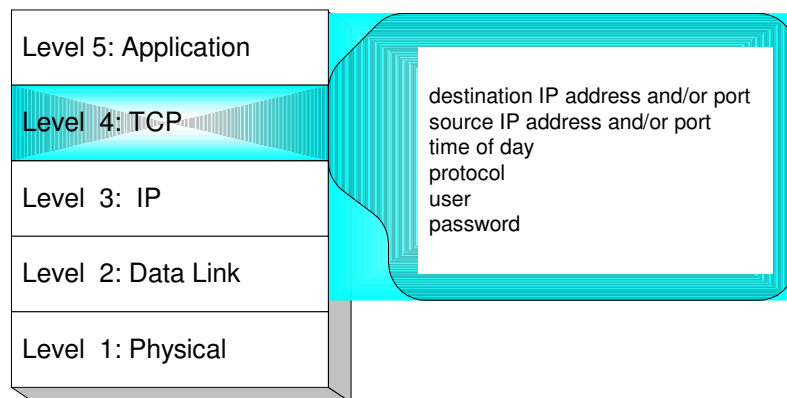






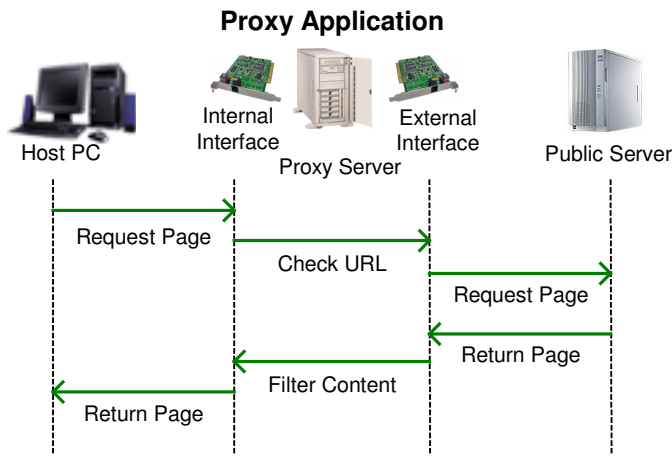
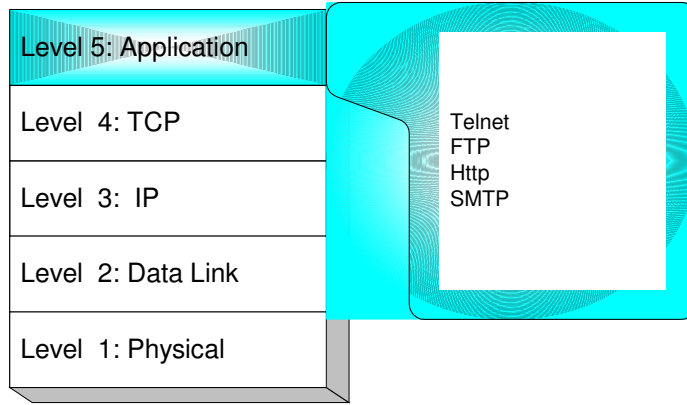
### 2.1.2 Circuit Gateway

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.



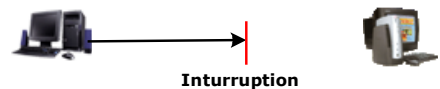
### 2.1.3 Application Gateway

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.

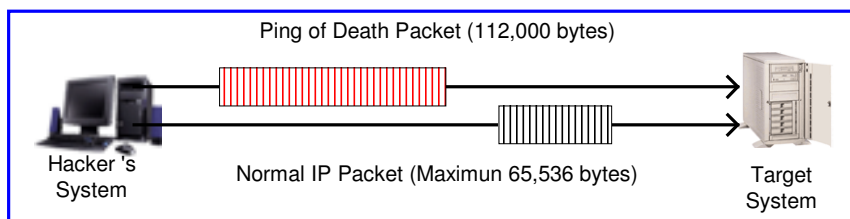


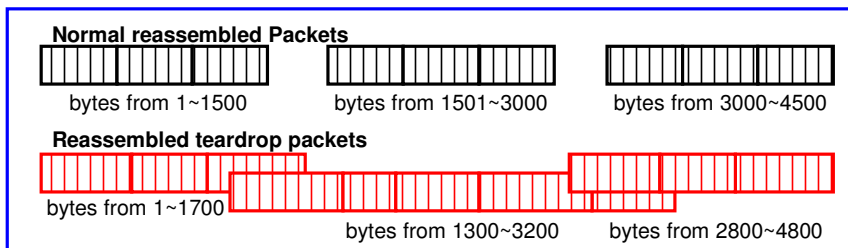
## 2.2 Denial of Service Attack

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.

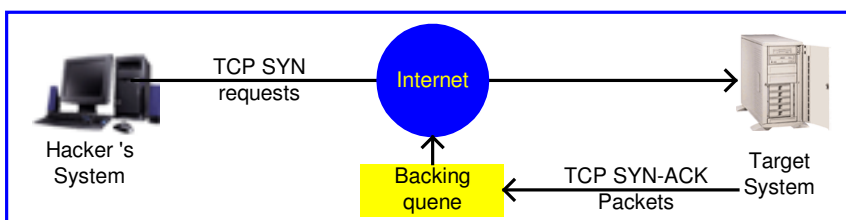


**Ping of death-** On the Internet, ping of death is a kind of denial of service (DoS) attack caused by deliberately sending an IP packet which size is larger than the 65,536 bytes allowed in the IP protocol. One of the features of TCP/IP is fragmentation, which allows a single IP packet to be broken 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.

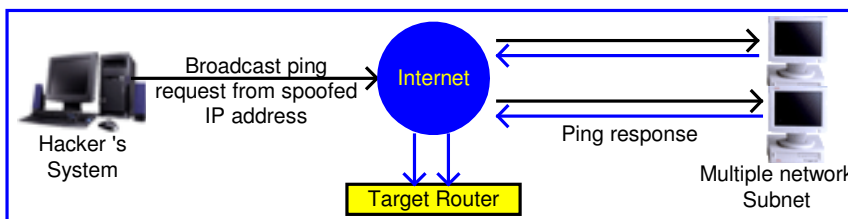


**ICMP Flood-** The attacker transmits a volume of ICMP request packets to cause all CPU resources to be consumed serving the phony requests.

**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.

**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.

**IP Spoofing-** IP Spoofing is a method of masking the identity of an intrusion by making it appear 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.

## 3 Yours VLAN (Virtual Local Area Network)

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.

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.

### 3.1 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.

### 3.2 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.

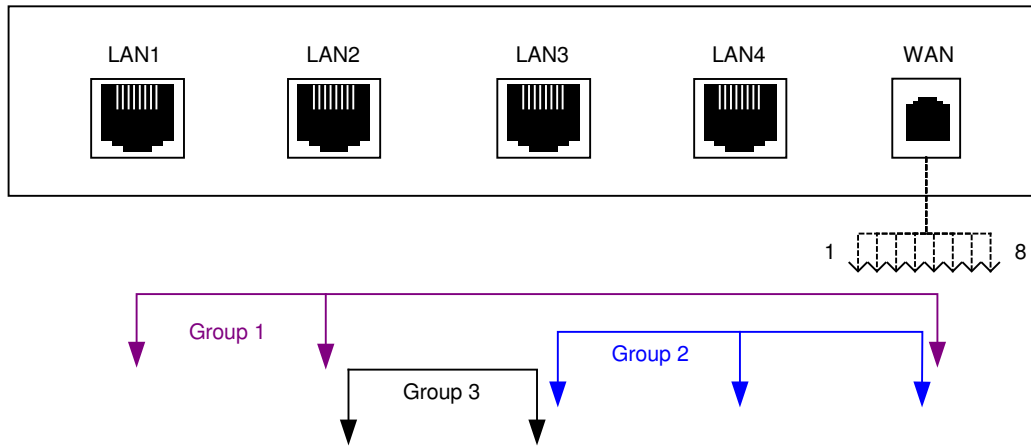
A VLAN-tagged frame carries an explicit identification of the VLAN to which it belongs; i.e., it carries a tag header that carries a non-null VID. This results in a minimum tagged frame length of 68 octets. Such a frame is classified as belonging to a particular VLAN based on the value of the VID that 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

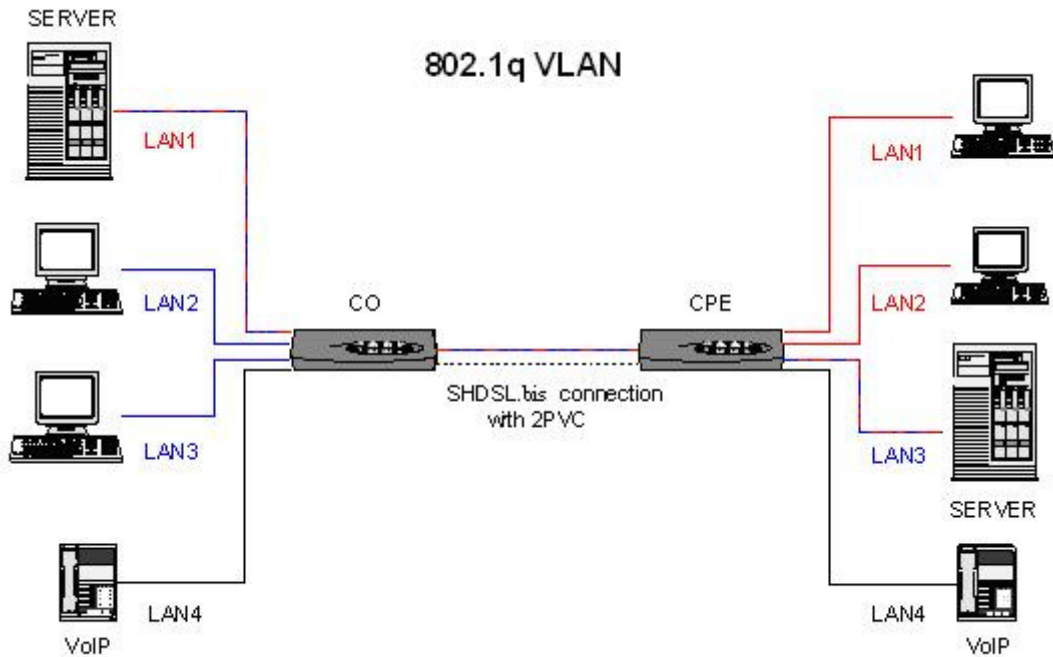
carry user priority information across bridged LANs in which individual LAN segments may be unable to signal priority information (e.g., 802.3/Ethernet segments). 2) The Canonical Format Indicator (CFI) is used to signal the presence or absence of a Routing Information Field (RIF) field, and, in combination 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.

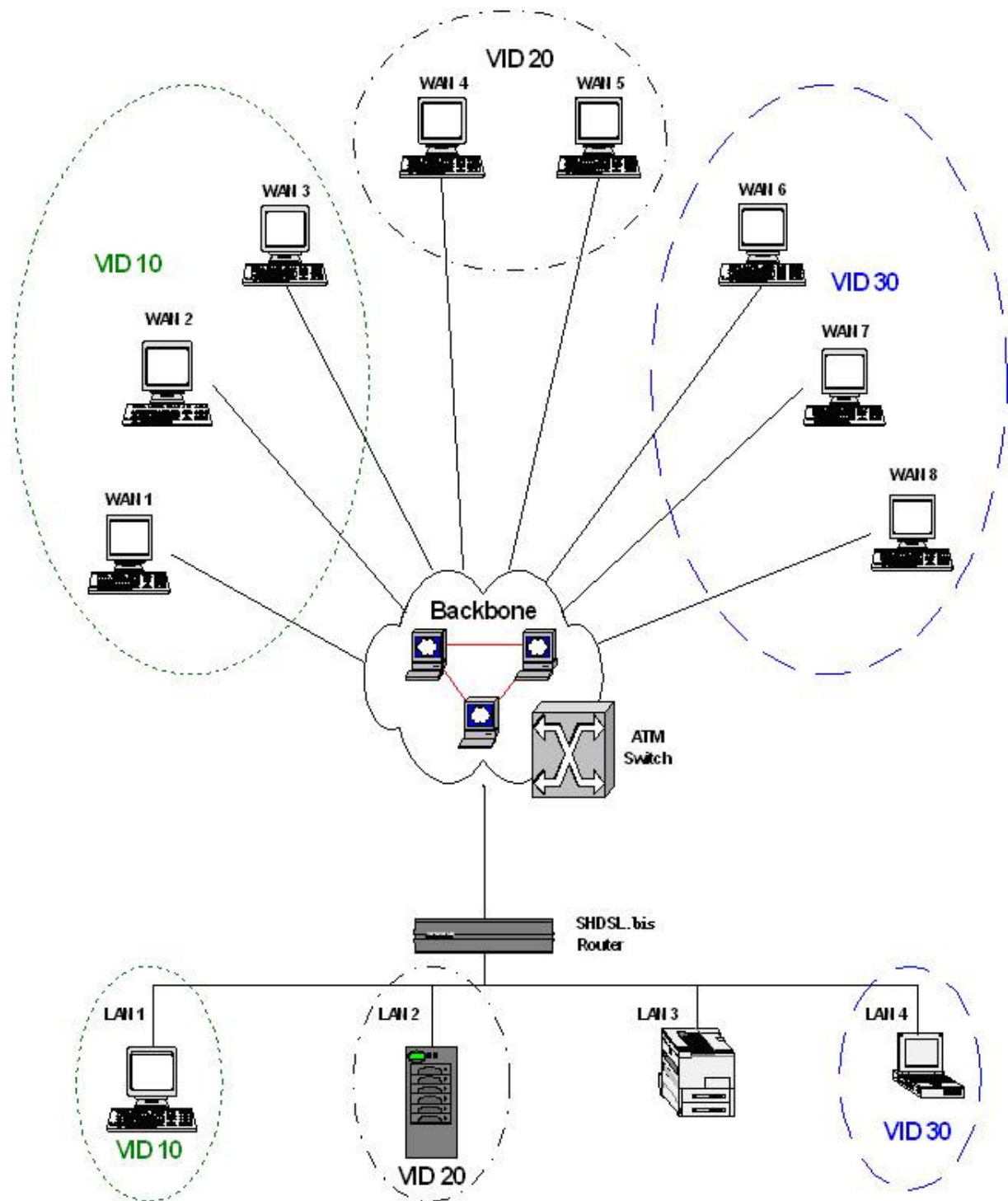
### 3.3 Applications

#### Port-based VLAN



#### 802.1q VLAN



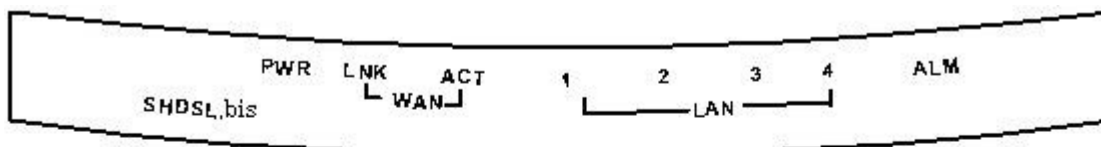


## 4 Getting to know about the router

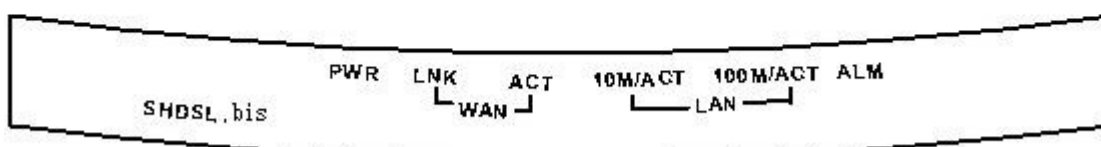
This section will introduce hardware of the router.

### 4.1 Front Panel

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



Front Panel of SHDSL .bis 4-wire/4-port router/bridge



Front Panel of SHDSL .bis 2-wire/1-port router/bridge

#### LED status of 4-wire/4-port router

LEDs	Active	Description
PWR	On	Power on
WAN	LNK	On SHDSL.bis line connection is established
		Blink SHDSL.bis handshake
	ACT	On Transmit or received data over SHDSL.bis link
LAN	1	On Ethernet cable is connected to LAN 1
		Blink Transmit or received data over LAN 1
	2	On Ethernet cable is connected to LAN 2
		Blink Transmit or received data over LAN 2
	3	On Ethernet cable is connected to LAN 3
		Blink Transmit or received data over LAN 3
	4	On Ethernet cable is connected to LAN 4
		Blink Transmit or received data over LAN 4
ALM	On	SHDSL.bis line connection is dropped
	Blink	SHDSL.bis self test

#### LED status of 2-wire/1-port router

LEDs	Active	Description
PWR	On	Power adaptor is connected to the router
WAN	LNK	On SHDSL.bis line connection is established
		Blink SHDSL.bis handshake
	ACT	Blink Transmit or received data over SHDSL.bis link
LAN	10M/ACT	On LAN port connect with 10M NIC
		Blink LAN port acts in 10M
	100M/ACT	On LAN port connect with 100M NIC
		Blink LAN port acts in 100M
ALM	On	SHDSL.bis line connection is dropped
	Blink	SHDSL.bis self test



## 4.2 Rear Panel

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



Rear Panel of SHDSL.bis 4-wire/2-wire,4-port router/bridge



Rear Panel of SHDSL.bis 2-wire/1-port router/bridge

### Connectors Description of 2-wire/1-port router

DC-IN	Power adaptor inlet: Input voltage 9VDC
LAN or LAN (1,2,3,4)	Ethernet 10BaseT for LAN port (RJ-45) 10/100BaseT auto-sensing and auto-MDIX for LAN port (RJ-45) (4-port Router)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	shdsl.bis interface for WAN port (RJ-45)
RST	Reset button for reboot or load factory default

### Connectors Description of 4-wire/4-port router

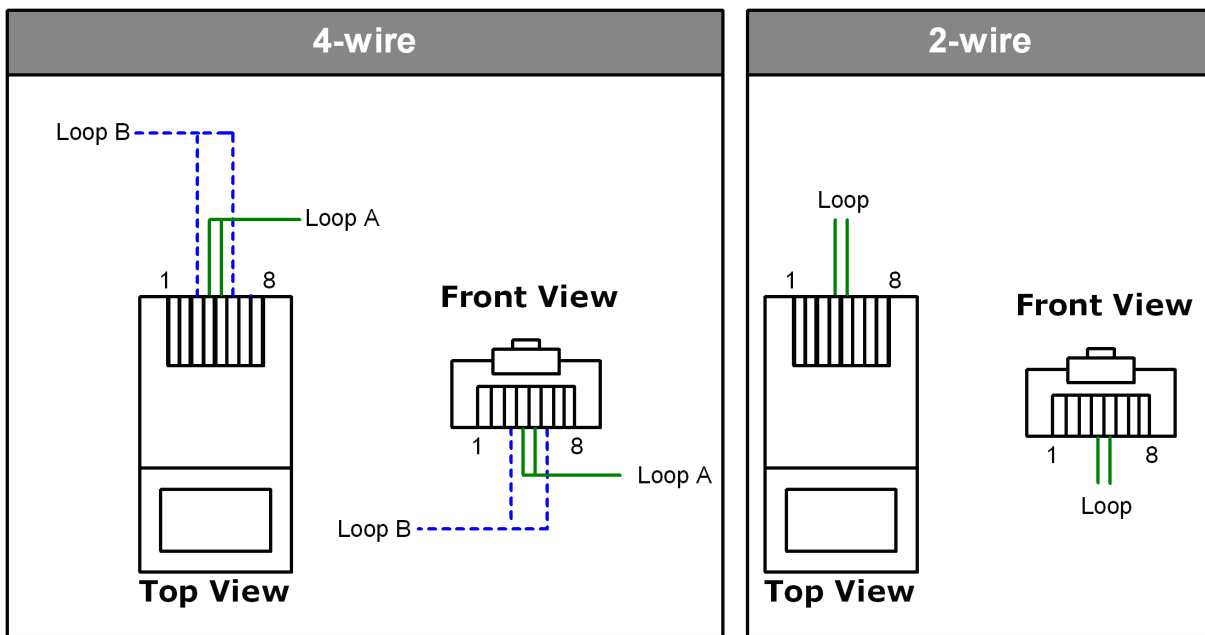
DC-IN	Power adaptor inlet: Input voltage 9VDC
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	SHDSL.bis interface for WAN port (RJ-45)
RST	Reset button for reboot or load factory default



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.

### 4.3 SHDSL.bis Line Connector



### 4.4 Console Cable

Pin Number	Description	Fuigure
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	

## 5 Configuration to the router

This guide is designed to lead users through Web Configuration of 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 step 3.

For Serial Console Configuration, you can skip step 1 and 2.

### 5.1 Step 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.

### 5.2 Step 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.

### 5.3 Step 3: Check the Terminal Access Program

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

### 5.4 Step 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 Protocol need to setup difference WAN parameters. After knowing the Ptorocol provided by ISP, you have to ask the necessary WAN parameters to setup it.

### Bridge EoA

VPI: \_  
 VCI: \_  
 Encapsulation:  
 Gateway:  
 Host Name: (if applicable)

### Route EoA

VPI: \_  
 VCI: \_  
 Encapsulation:  
 IP Address:  
 Subnet Mask: \_  
 Gateway:  
 DNS Server: \_  
 Host Name: (if applicable)

### IPoA

VPI: \_  
 VCI: \_  
 Encapsulation:  
 IP Address:  
 Subnet Mask: \_  
 Gateway:  
 DNS Server: \_  
 Host Name: (if applicable)

### PPPoA

VPI: \_  
 VCI: \_  
 Encapsulation:  
 User Name:  
 Password:  
 DNS Server: \_  
 Host Name: (if applicable)  
 IP Address: (if applicable)

### PPPoE

VPI: \_  
 VCI: \_  
 Encapsulation:  
 User Name:  
 Password:  
 DNS Server: \_  
 Host Name: (if applicable)  
 IP Address: (if applicable)

## 5.5 Step 5: Install the SHDSL.bis Router

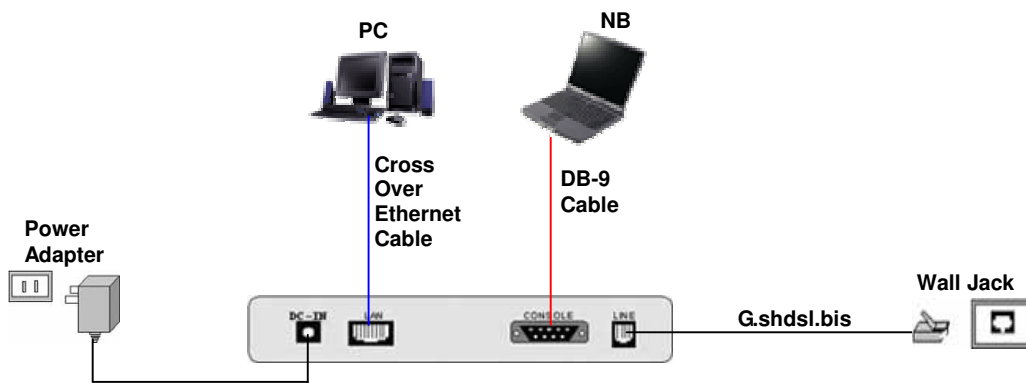


To avoid possible damage to this Router, do not turn on the router before Hardware Installation.

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

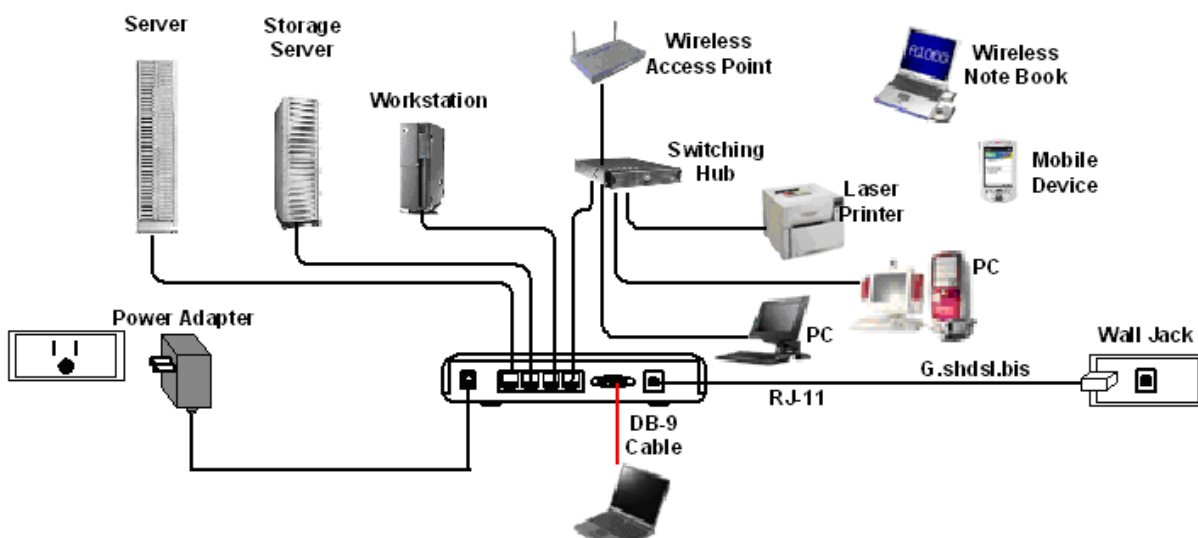
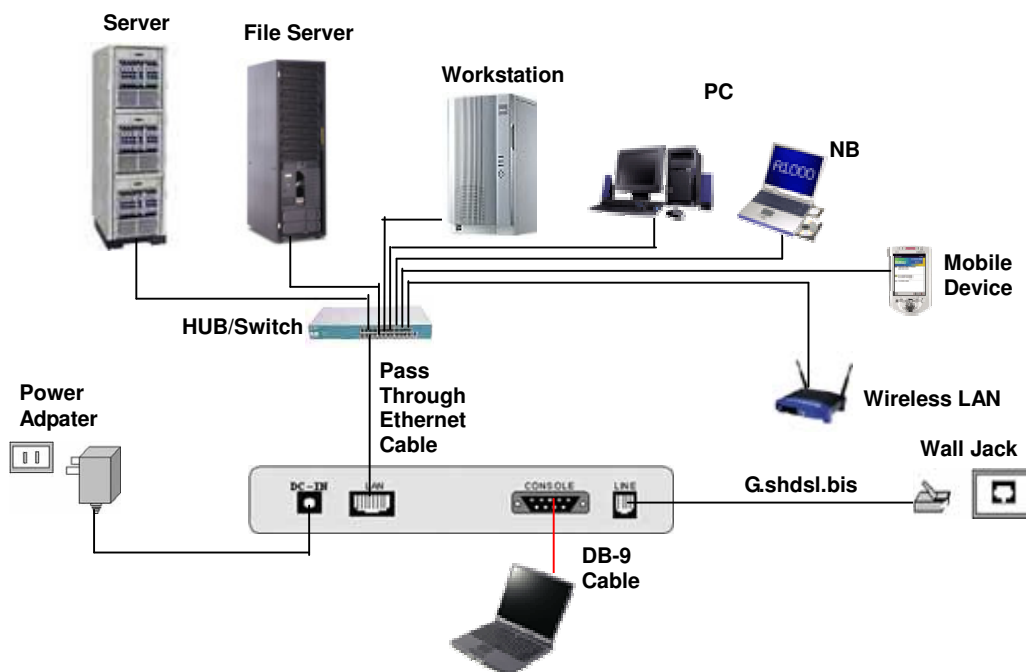
**Note:** The 1-port router and 4-port router both supports auto-MDIX switching hub so both straight through and cross-over Ethernet cable can be used.

- ✓ Connect the phone cable to the product and the other side of phone cable to wall jack.
- ✓ Connect the power adapter to power source.
- ✓ Turn on the PC or NB, which is used for configuration the Router.



Direct Connection with PC or NB for 1-port router

Connection with Hub/Switch for 1-port router



4-port router with complex network topology

## 6 Configuration via Web Browser

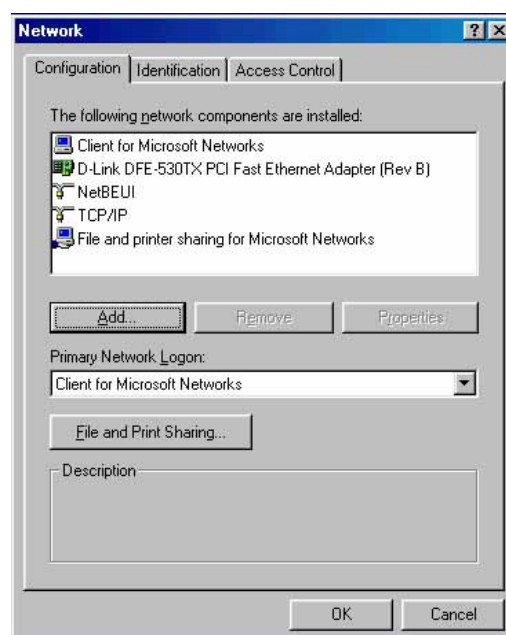
Step.1 For Win85, 98 and Me, click the **start** button. Select **setting** and **control panel**.



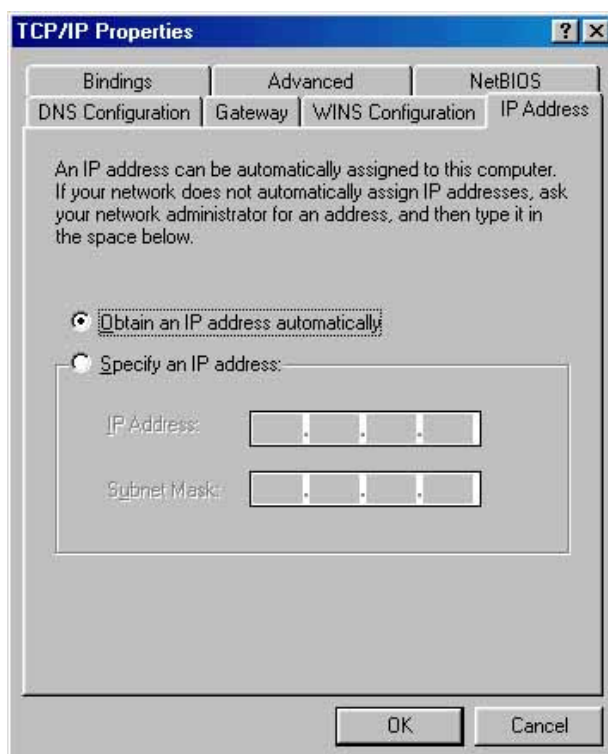
Step.2 Double click the **network** icon.



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.



## 7 Basic Setup

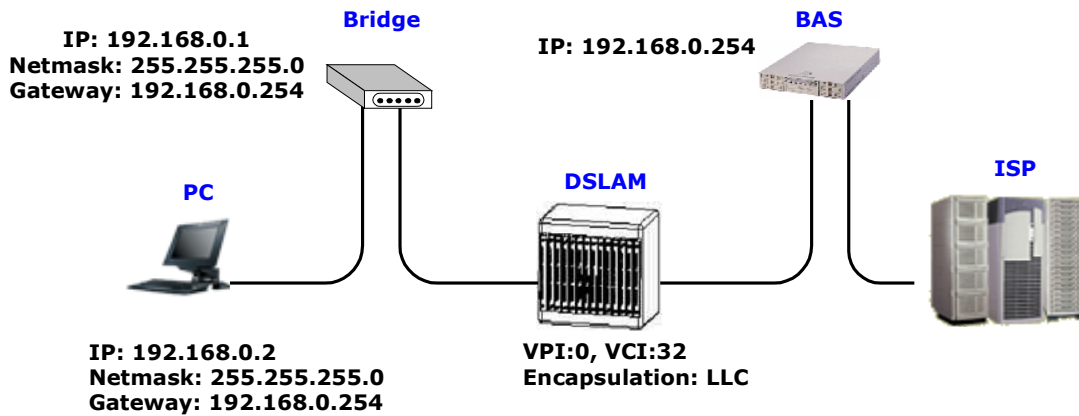
The Basic Setup contains LAN, WAN, Bridge and Route operation mode. User can use it to completely setup the router. After successfully completing it, you can access Internet. This is the easiest and possible way to setup the router.

**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.

### 7.1 Bridge Mode

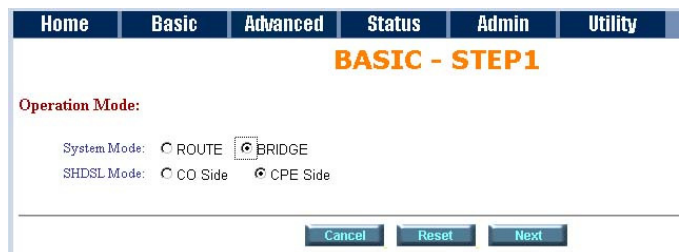


Before configuring the router in bridge mode, please check with your ISP about this information.

VPI: \_  
VCI: \_  
Encapsulation: \_\_\_\_\_  
Gateway: \_\_\_\_\_  
Host Name: (if applicable)

Click **Bridge** and **CPE** Side to setup Bridging mode of the Router and then click **Next** for the next setting.

This product can be setup as two SHDSL.bis working mode: CO (Central Office) and CPE (Customer Premises Equipment). For connection with DSLAM, the SHDSL.bis working mode is CPE. For "LAN to LAN" connection, one side must be CO and the other side must be CPE.





Enter Parameters in **BASIC – STEP2:**

**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

Click **LLC**, Click **Next**

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.

**Home Basic Advanced Status Admin Utility**

**BASIC - STEP 2**

**LAN:**

IP Address: 192 . 168 . 0 . 1  
 Subnet Mask: 255 . 255 . 255 . 0  
 Gateway: 192 . 168 . 0 . 254  
 Host Name: SOHO

**WAN1:**

VPI: 0  
 VCI: 32  
 Encap.:  VC-mux  LLC

**Back Cancel Reset Next**

**Home Basic Advanced Status Admin Utility**

**BASIC - REVIEW**

**REVIEW:**  
 To let the configuration that you have changed take effect immediately, please click **Restart** button to reboot. To continue the setup procedure, please click **Continue** button.

- System Operation Mode:
 

System Mode	Bridge Mode
SHDSL Mode	CPE Side
- LAN Interface:
 

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	192.168.0.254
Hostname	SOHO
- WAN1 interface:
 

VPI	0
VCI	32
AAL5 Encap.	LLC

**Continue Restart**

**7.2 Routing Mode**

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.

Click **ROUTE** and **CPE Side** then press **Next**.

This product can be setup as two SHDSL.bis working mode: CO (Central Office) and CPE (Customer Premises Equipment). For connection with DSLAM, the SHDSL.bis working mode is CPE. For "LAN to LAN" connection, one side must be CO and the other side must be CPE.



## 7.2.1 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.

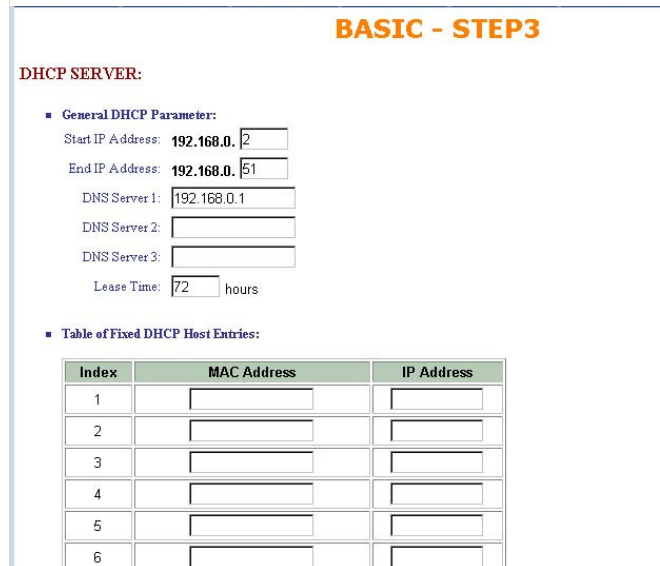
The embedded DHCP server assigns network configuration information at most 253 users accessing the Internet in the same time.

**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.

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 from Start IP Address to End IP Address. The legal IP address range is from 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 than 1. Lease time 72 hours indicates that the DHCP server will reassign IP information in every 72 hours.



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

7			
8			
9			
10			

Back Cancel Reset Next

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**.

Press **Next** to setup WAN1 parameters.

### 7.2.2 DHCP Client

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.

LAN IP Type: **Dynamic**

Click **Next** to setup WAN1 parameters.

### 7.2.3 DHCP relay

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

IP Type: **Fixed**  
 IP Address: 192.168.0.1  
 Subnet Mask: 255.255.255.0  
 Host Name: SOHO

Some of the 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.

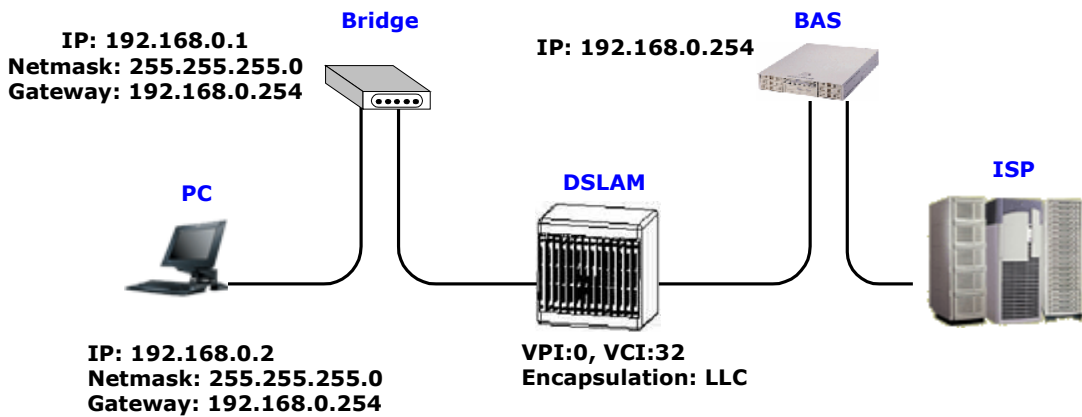
Trigger DHCP Service: **Relay**  
 Press **Next** to setup DHCP server parameter.

Enter DHCP server IP address in IP address field.

Press **Next**

## 7.2.4 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.



Before configure the router, check with your ISP about this information.

VPI: \_  
 VCI: \_  
 Encapsulation:  
 User Name:  
 Password:  
 DNS Server: \_  
 Host Name: (if applicable)  
 IP address: (if applicable)

Enter Parameters in **BASIC – STEP2.**

WAN1 parameters:

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 at page 40.

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.

Home	Basic	Advanced	Status	Admin	Utility
------	-------	----------	--------	-------	---------

BASIC - STEP4

WAN1:

VPI:

VCI:

AAL5 Encap:  VC-mux  LLC

Protocol: 

IPoA  
 IPoA+NAT  
 EoA  
 EoA+NAT  
 PPPoA+NAT  
 PPPoE+NAT

---

Home	Basic	Advanced	Status	Admin	Utility
------	-------	----------	--------	-------	---------

BASIC - STEP4

ISP1:

Username:

Password:

Password Confirm:

Idle Time:  minutes

IP Type:

IP Address:

**IP Type:** .

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:**

**IP Address:** 192.168.1.1

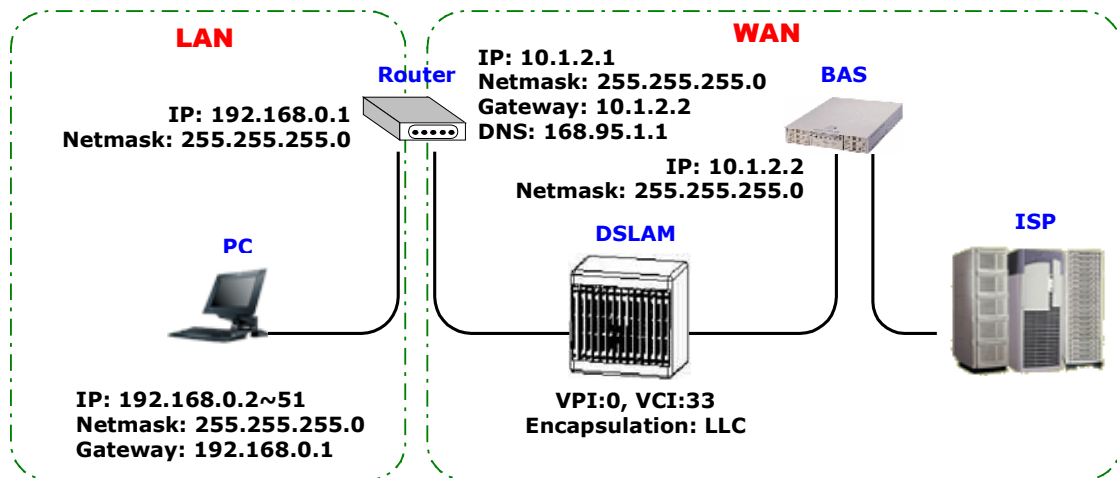
Click .

**Note:** For safety, the password will be prompt as star symbol.

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

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

## 7.2.5 IPoA or EoA



Before configuration the router, check with your ISP about this information.

VPI: \_  
 VCI: \_  
 Encapsulation: \_  
 IP Address: \_  
 Subnet Mask: \_  
 Gateway: \_  
 DNS Server: \_  
 Host Name: (if applicable)

Enter Parameters in **BASIC – STEP2**

Wan Parameters;

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 at page 40.

**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**

Home Basic Advanced Status Admin Utility

**BASIC - STEP4**

WANI:

VPI: 0

VCI: 32

AAL5 Encap:  VC-mux  LLC

Protocol: IPoA

IPoA  
 IPoA+NAT  
 EoA  
 EoA+NAT  
 PPPoA+NAT  
 PPPoE+NAT

Back Cancel Reset Next

Home Basic Advanced Status Admin Utility

**BASIC - STEP5**

WANI:

IP Address: 10 . 1 . 2 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 10 . 1 . 2 . 2

DNS Server 1: 168.95.1.1

DNS Server 2:

DNS Server 3:

Back Cancel Reset Next

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

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

Home
Basic
Advanced
Status
Admin
Utility

BASIC - REVIEW

**REVIEW:**  
To let the configuration that you have changed take effect immediately, please click Restart button to reb continue the setup procedure, please click Continue button.

- System Operation Mode:
 

System Mode	Route Mode
SHDSL Mode	CPE Side
- LAN Interface:
 

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Hostname	SOHO
Trigger DHCP service	Enable
- DHCP server:
 

Default gateway	192.168.0.1
Subnet mask	255.255.255.0
Start IP address	192.168.0.2
End IP address	192.168.0.51
DNS Server 1	192.168.0.1
DNS Server 2	
DNS Server 3	
Lease time	72 hours
- Table of Fixed DHCP Host List:
 

Index	MAC Address	IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
- WAN1 interface:
 

VPI	0
VCI	32
AAL5 Encap.	LLC
Protocol	IP over ATM
WAN1 IP address	10.1.2.1
WAN1 subnet mask	255.255.255.0
Gateway	10.1.2.2
DNS Server 1	168.95.1.1
DNS Server 2	
DNS Server 3	

Continue
Restart

## 8 Advanced Setup

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

### 8.1 SHDSL.bis

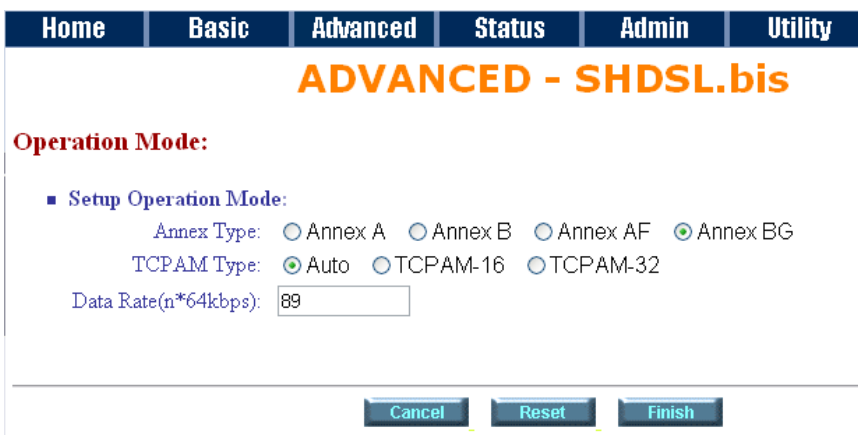
You can setup the Annex type, data rate and SNR margin for SHDSL.bis parameters in SHDSL.bis.

Click [SHDSL.bis](#)



**Annex Type:** There are four Annex types, **Annex A** (ANSI), **Annex B** (ETSI), **AnnexAF** and **Annex BG** in SHDSL.bis. Check with your ISP about it.

**TCPAM Type:** the default option is **Auto**. You may assign the different type manually by click the caption **TPCAM-16** or **TPCAM-32**



**Data Rate (2W):** you can setup the SHDSL.bis data rate in the multiple of 64kbps.

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

Under Annex F/G

TPCAM32 ; data rate is 768Kbps ~ 5696Kbps (Nx64kbps, N=12~89)

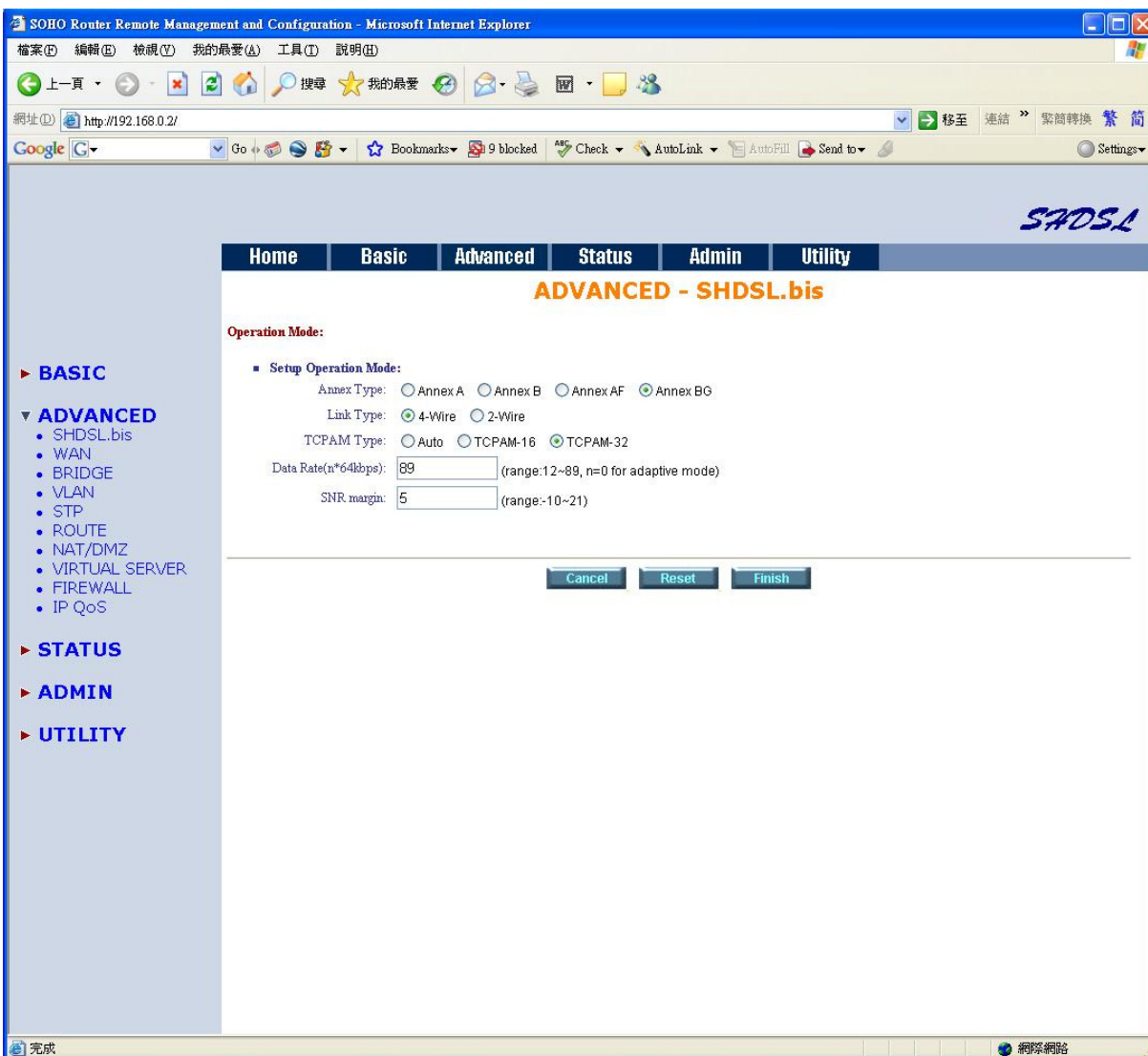
TPCAM16 ; data rate is 192Kbps ~ 3840Kbps (Nx64kbps, N=3~60)

Under Annex A/B

TPCAM16 ; 192Kbps ~ 2304Kbps (Nx 64kbps, N=3~36)

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





**Data Rate (4W):** you can setup the SHDSL.bis data rate in the multiple of 128kbps.

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

Under Annex F/G

TCPAM32 ; data rate is 1536Kbps ~ 11392Kbps (Nx128kbps, N=12~ 89)

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

Under Annex A/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.

SNR margin 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 2, the SHDSL.bis connection will drop and reconnect when the SNR margin is lower than 2. 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 EPROM. Check the parameters before writing in EPROM.

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

## 8.2 WAN

The SHDSL.bis router supports up to 8 PVCs. WAN 1 was configured via BASIC except QoS. If you want to setup another PVCs, 2 to 7, the parameters are setup in the page of WAN under ADVANCED. On the other hand, you do not need to setup WAN except you apply two or more Internet Services with ISPs.

- ▶ BASIC
- ▼ ADVANCED
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - ETHERNET
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- ▶ STATUS
- ▶ ADMIN

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:

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 ignore 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 ignore the information, but erasion or blank in default setting will cause system error.

Home Basic **Advanced** Status Admin Utility

**ADVANCED - WAN**

WAN Interface Parameters:

■ Table of Current WAN Interface Parameter:

No	WAN	VC	ISP
1	Protocol: IP over ATM IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0	VPI: 0 VCI: 32 AAL5 Encap: LLC QoS Class: UBR QoS PCR: 2400 QoS SCR: 2400 QoS MBS: 1	Username: test Password: **** Password Confirm: **** Idle Time: 10 IP Type: Dynamic
2	Protocol: Disable IP Address: 192.168.2.1 Subnet Mask: 255.255.255.0	VPI: 0 VCI: 33 AAL5 Encap: LLC QoS Class: UBR QoS PCR: 2400	Username: test Password: **** Password Confirm: **** Idle Time: 10 IP Type: Dynamic

QoS (Quality of Service): 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 Quality of Service that the network need to provide for that traffic.

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 available during the connection life time. This bandwidth is characterized by Peak Cell Rate (PCR). Based on the PCR of the CBR traffic, specific cell slots are assigned for the VC in the schedule table. The ATM always sends a single cell during the CBR connection's assigned cell slot.

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

VBR-nrt (Variable Bit Rate non-real-time)

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 means of reducing latency, not increasing bandwidth. The range of PCR is 64kbps to 2400kbps

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 64kbps to 2400kbps.

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.

Press **Finish** to finish setting.

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

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

### 8.3 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.

- ▶ **BASIC**
- ▼ **ADVANCED**
  - SHDSL.bis
  - WAN
  - **BRIDGE**
  - VLAN
  - ETHERNET
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- ▶ **STATUS**
- ▶ **ADMIN**
- ▶ **UTILITY**

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.

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

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

Home Basic Advanced Status Admin Utility

ADVANCED - BRIDGE

**Generic Bridge Parameters:**

- General Parameter:
 

Default Gateway:

**Static Bridge Parameters:**

- Table of Current MAC Entries:

No	MAC Address	LAN	WAN1 - 4	WAN5 - 8
1	00:00:00:00:00:00	Filter	1, Filter	5, Filter
			2, Filter	6, Filter
			3, Filter	7, Filter
			4, Filter	8, Filter

Home Basic Advanced Status Admin Utility

ADVANCED - BRIDGE

**Bridge Parameters Review:**

To let the configuration that you have changed take effect immediately, please click Restart button to reboot the sys continue the setup procedure, please click Continue button.

- Generic Bridge Parameter:
 

Default Gateway
- Static Bridge Parameter:
 

No	MAC Address	LAN	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
Pool is Empty !										

## 8.4 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.

Click **VLAN** to configure VLAN.

- ▶ **BASIC**
- ▼ **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - **VLAN**
  - ETHERNET
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- ▶ **STATUS**
- ▶ **ADMIN**
- ▶ **UTILITY**

The product support two types of VLAN:  
**802.1Q Tag-Based VLAN**  
**Port-Based VLAN.**

User can configure one of them to the router.

For setting 802.1Q VLAN click the **802.1Q Tag-Based VLAN**. The screen will prompt as follow.

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - VLAN

Virtual LAN Parameters:

- General Parameter:
  - Mode:  Disable  802.1Q Tag-Based VLAN  Port-Based VLAN

Home
Basic
Advanced
Status
Admin
Utility

Virtual LAN Parameters:

- General Parameter:
  - Mode:  Disable  802.1Q Tag-Based VLAN  Port-Based VLAN
- 802.1Q Tag-Based VLAN Table:
 

No	VID	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1
Link Type	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access

**VID:** Virtual LAN ID. It is an definite number of ID which number is from 1 to 4094.

**PVID:** Port VID which is an untagged member 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.

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

Click **Port-Based VLAN** to configure the router.

**Home Basic Advanced Status Admin Utility**

**ADVANCED - VLAN**

**Virtual LAN Parameters:**

- General Parameter:**

Mode:  Disable  802.1Q Tag-Based VLAN  Port-Based VLAN
- Port Based VLAN Table:**

No	LAN1	LAN2	LAN3	LAN4	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	WAN7	WAN8
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Cancel Reset Finish**

## 8.5 Ethernet

This page of function let user configure the media type of Ethernet.

Click **ETHERNET** to configure Ethernet.

Here are several options: **AutoSense, 100Base-TX**

- ▶ **BASIC**
- ▼ **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - **ETHERNET**
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- ▶ **STATUS**
- ▶ **ADMIN**
- ▶ **UTILITY**

**Home Basic Advanced Status Admin Utility**

**ADVANCED - Ethernet**

**Ethernet Parameter:**

- PHY Parameter:**

Media Type:

**Cancel Reset Finish**

## 8.6 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.

- ▶ **BASIC**
- ▼ **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - ETHERNET
  - **ROUTE**
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- ▶ **STATUS**
- ▶ **ADMIN**
- ▶ **UTILITY**

Click **Route** to modify the routing information.

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - ROUTE

Static Route and RIP Parameters:

- Table of Current Static Route Entries:

Index	Network Address	Subnet Mask	Gateway
1	0.0.0.0	0.0.0.0	10.1.2.2
2	<input type="text"/>	<input type="text"/>	<input type="text"/>

- General RIP Parameter:

RIP Mode:  Disable  Enable  
 Auto RIP Summary:  Disable  Enable

- Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	None
WAN1	Disable	2	None	Enable	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None

To modify the RIP (Routing information protocol) Parameters:

**RIP Mode:** **Enable**

**Auto RIP Summary:** **Enable**

Press **Modify**

Home
Basic
Advanced
Status
Admin
Utility

- General RIP Parameter:

RIP Mode:  Disable  Enable  
 Auto RIP Summary:  Disable  Enable

- Table of Current Interface RIP Parameter:

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

**RIP Mode:** this parameter determines how the product 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 incorporates 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 send 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** is for the purpose of promptly broadcast or multicast the RIP while the route is changed. (ex shutting down one of the routers in routing table)

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

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

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.

Table of Current Interface RIP Parameter:

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

Buttons: Cancel, Ok, Reset

Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	
WAN1	Disable	1	None	Enable	None
WAN2	Disable	--	None	Disable	None
WAN3	Disable	--	None	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Buttons: Cancel, Ok, Reset

Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
LAN	Disable	2	None	Enable	
WAN1	Disable	2	None	Enable	None
WAN2	Disable	--	Password	Disable	None
WAN3	Disable	--	MD5	Disable	None
WAN4	Disable	--	None	Disable	None
WAN5	Disable	--	None	Disable	None
WAN6	Disable	--	None	Disable	None
WAN7	Disable	--	None	Disable	None
WAN8	Disable	--	None	Disable	None

Buttons: Cancel, Ok, Reset

Table of Current Interface RIP Parameter:

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

Buttons: Cancel, Ok, Reset



## 8.7 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.

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.

- ▶ **BASIC**
- ▼ **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - ETHERNET
  - ROUTE
  - **NAT/DMZ**
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- ▶ **STATUS**
- ▶ **ADMIN**
- ▶ **UTILITY**

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - NAT/DMZ

Network Address Translation and DMZ Hosts Parameters:

- **NAT/DMZ function:**  
 NAT/DMZ Function:  Disable  Enable
- **DMZ Host:**  
 DMZ Host Function:  Disable  Enable  
 Virtual IP Address:   
 Active Interface:
- **Multi-DMZ:**

ID	Virtual IP Address	Global IP Address	Interface
1	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
2	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
3	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
4	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
5	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
6	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
7	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
8	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
9	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
10	<input type="text"/>	<input type="text"/>	<input type="text" value="WAN1"/>
- **Multi-NAT:**

ID	Virtual Start IP Address	Count	Global Start IP Address	Count	Interface
1	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="WAN1"/>
2	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="WAN1"/>
3	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="WAN1"/>
4	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="WAN1"/>
5	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="WAN1"/>

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

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

## 8.8 Virtual Server

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.

Click **Virtual Server** to configure the parameters.

Press **Modify** for modify 1.

- ▶ **BASIC**
- ▼ **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - ETHERNET
  - ROUTE
  - NAT/DMZ
  - **VIRTUAL SERVER**
  - FIREWALL
  - IP QoS
- ▶ **STATUS**
- ▶ **ADMIN**
- ▶ **UTILITY**

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - VIRTUAL SERVER

Virtual Server Mapping Parameters:

■ Table of Current Virtual Server Entries:

Index	Service Name	Interface	Private IP	Protocol	Schedule
⊕ 1	---	---	---	Disable	---
⊖ 2	---	---	---	Disable	---
⊖ 3	---	---	---	Disable	---
⊖ 4	---	---	---	Disable	---
⊖ 5	---	---	---	Disable	---
⊖ 6	---	---	---	Disable	---
⊖ 7	---	---	---	Disable	---
⊖ 8	---	---	---	Disable	---
⊖ 9	---	---	---	Disable	---
⊖ 10	---	---	---	Disable	---

Cancel Modify Finish

Type the necessary parameters then click **Finish**.

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

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - VIRTUAL SERVER

Virtual Server Mapping Parameters:

■ Virtual Server 1:

Protocol: TCP

Interface: WAN1

Service Name:  

Private IP:  

Private Port: 0

Public Port: 0

Schedule:  Always

From Day Sunday to Saturday  
 Time 0:0 to 23:59

Back Reset Ok

## 8.9 Firewall

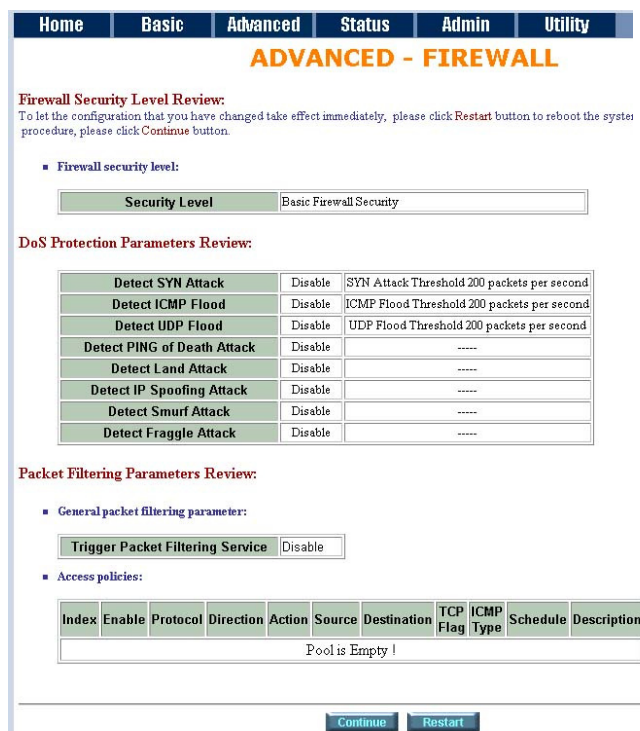
A firewall is a set of related programs that protects the resources of a private network from other networks. It is helpful to users that allow preventing hackers to access its own private data resource accidentally.

- ▶ **BASIC**
- ▼ **ADVANCED**
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - ETHERNET
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - **FIREWALL**
  - IP QoS
- ▶ **STATUS**
- ▶ **ADMIN**
- ▶ **UTILITY**

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



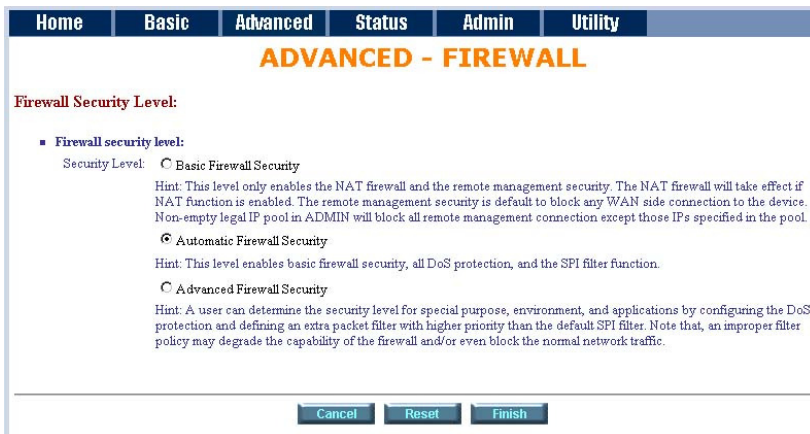
The screen will prompt the parameters, which router will record in EPROM. Check the parameters.



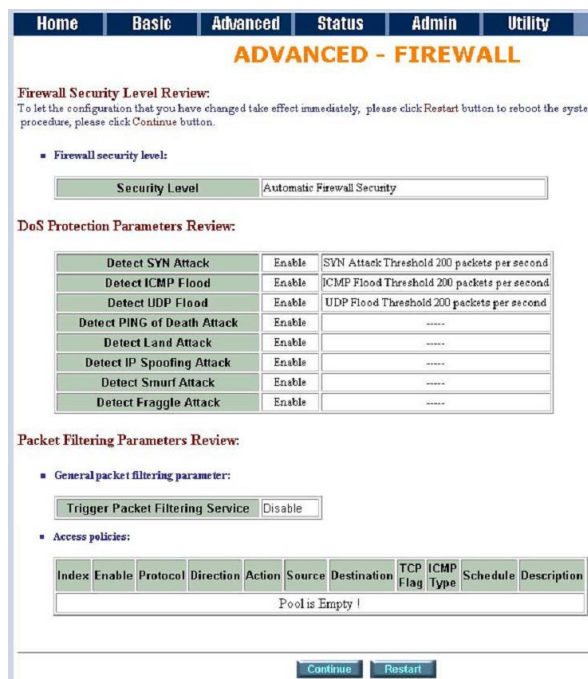
Press **Restart** to restart the router or press **Continue** to setup another function.

Click **Automatic Firewall Security**. This level enables basic firewall security, all DoS protection, and the SPI filter function.

Press **Finish** to finish setting firewall.



The screen will prompt the parameters, which will be written in EPROM. 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.

Click **Advanced Firewall Security** and then press **Finish**.

A SYN flood 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 sender transmits a volume of requests for UDP diagnostic services which cause all CPU resources to be consumed serving the phony requests.

A ping of death attack attempts to crash your system by sending a fragmented packet, when reconstructed is larger than the maximum allowable size. Other known variants of the ping of death include teardrop, bonk and nestea.

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 is a method of masking the identity of an intrusion by making it appear 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.

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.

IP Spoofing: Falsify the IP header information to deceive the destination host.

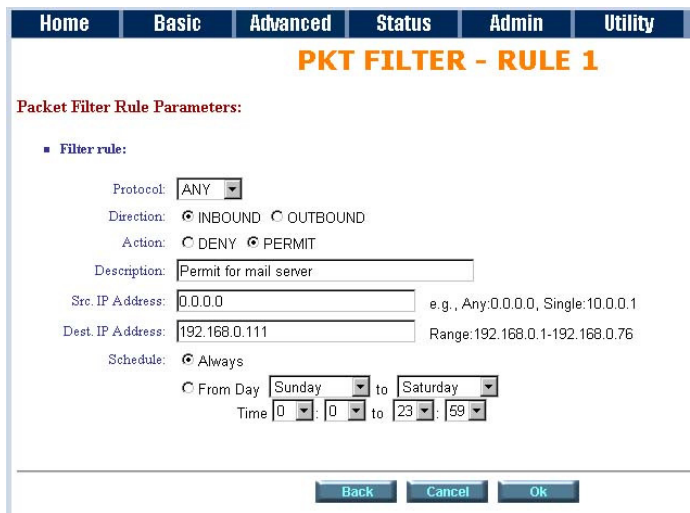
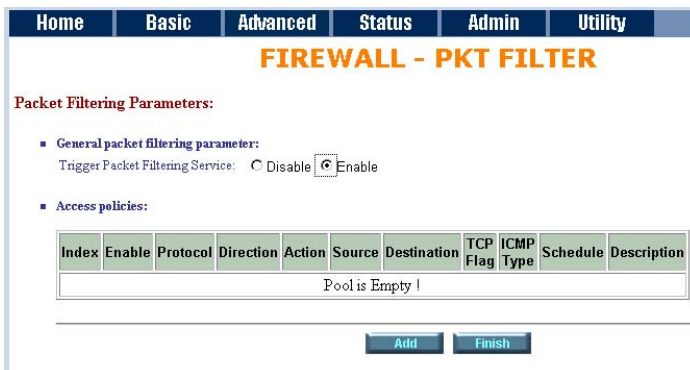
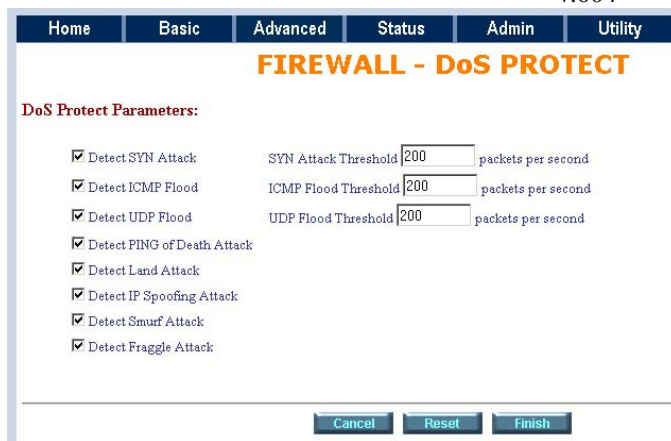
Traditional firewall is stateless meaning they have no memory of the connections of data or packets that pass through them. Such IP filtering firewalls simply examine header information in each packet and attempt to match it to a set of define rule. If the firewall finds a match, the prescribe action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

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

Select the Protocol and configure the parameter.

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 to LAN, and OUTBOUND is LAN to WAN.)

**Description:** Hacker

**Src. IP Address:** 200.1.1.1

**Dest. IP Address:** 192.168.0.2-192.168.0.50

Press **OK** to finish.

The screen will prompt the configured parameters. Check the parameters.

Click **Restart** to restart the gateway or Continue to configure another parameters.

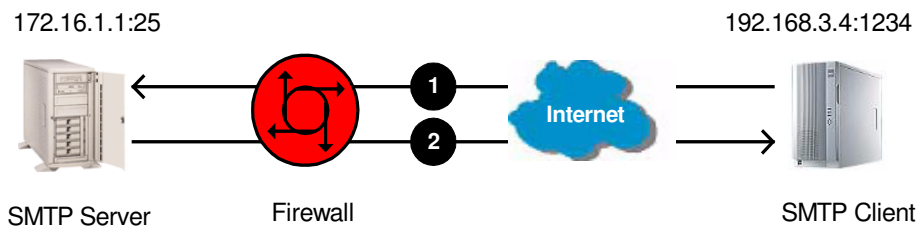


Filtering Rule for SMTP connection

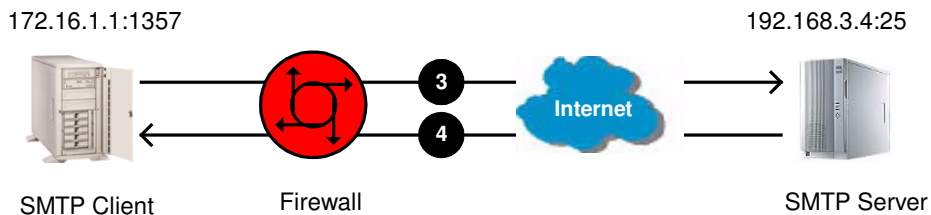
Filtering rule will be configured as follow

Index	Protocol	Direction	Action	Source	Destination	Dest. Port	Schedule
1	TCP	Inbound	Permit	External	Internal	25	Always
2	TCP	Outbound	Permit	Internal	External	>1023	Always
3	TCP	Outbound	Permit	Internal	External	25	Always
4	TCP	Inbound	Permit	External	Internal	>1023	Always
5	Any	Either	Deny	Any	Any	Any	Always

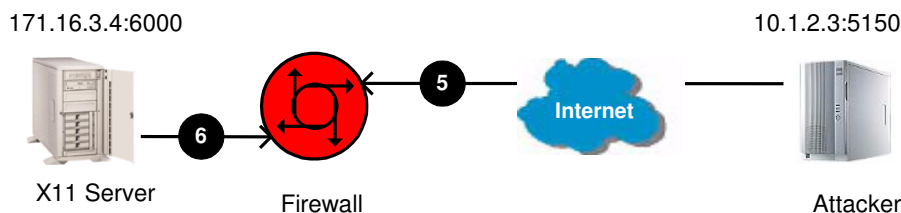
Packet	Direction	Source	Destination	Protocol	Dest. Port	Action (Rule)
1	Inbound	192.168.3.4	172.16.1.1	TCP	25	Permit (A)
2	Outbound	172.16.1.1	192.168.3.4	TCP	1234	Permit (B)



Packet	Direction	Source	Destination	Protocol	Dest. Port	Action (Rule)
3	Outbound	172.16.1.1	192.168.3.4	TCP	25	Permit (C)
4	Inbound	192.168.3.4	172.16.1.1	TCP	1357	Permit (D)



Packet	Direction	Source	Destination	Protocol	Dest. Port	Action (Rule)
5	Inbound	10.1.2.3	171.16.3.4	TCP	6000	Deny (E)
6	Outbound	171.16.3.4	10.1.2.3	TCP	5150	Deny (E)



Update Filtering Rule

Index	Protocol	Direction	Action	Source	Destination	Source Port	Dest. Port
1	TCP	Inbound	Permit	External	Internal	>1023	25
2	TCP	Outbound	Permit	Internal	External	25	>1023
3	TCP	Outbound	Permit	Internal	External	>1023	25
4	TCP	Inbound	Permit	External	Internal	25	>1023
5	Any	Either	Deny	Any	Any	Any	Any

Filtering Result

Index	Protocol	Direction	Action	Source	Destination	Source Port	Dest. Port
1	TCP	Inbound	Permit(A)	192.168.3.4	171.16.1.1	1234	25
2	TCP	Outbound	Permit(B)	171.16.1.1	192.168.3.4	25	1234
3	TCP	Outbound	Permit(C)	171.16.1.1	192.168.3.4	1357	25
4	TCP	Inbound	Permit(D)	192.168.3.4	171.16.1.1	25	1357
5	TCP	Inbound	Deny(E)	10.1.2.3	171.16.3.4	5150	6000
6	TCP	Outbound	Deny(E)	171.16.3.4	10.1.2.3	6000	5150

Rule Order

The rules order affects the filtering result. The filtering process will proceed from top to bottom, changing the order as the different result of filtering.

Rule	Source Address	Destination Address	Action
A	10.0.0.0	172.16.6.0	Permit
B	10.1.99.0	172.16.0.0	Deny
C	Any	Any	Deny

Where “0” at the last eight bits indicates “from 1 to 254”, “0” at any eight bits preceding “0”, “0.0” or “0.0.0” indicates “from 1 to 254”. On the other hand, “0” and all “0” successive with “0” represents any.

When the rule is ordered as ABC:

Index	Source Address	Destination Address	Action
1	10.1.99.1	172.16.1.1	Deny (B)
2	10.1.99.1	172.16.6.1	Permit (A)
3	10.1.1.1	172.16.6.1	Permit (A)
4	10.1.1.1	172.16.1.1	Deny (C)
5	192.168.3.4	172.16.6.1	Deny (C)

The rule order will permit 10.1.99.1 to access 172.16.6.1.



When the rule is ordered as BAC:

Index	Source Address	Destination Address	Action
1	10.1.99.1	172.16.1.1	Deny (B)
2	10.1.99.1	172.16.6.1	Deny (B)
3	10.1.1.1	172.16.6.1	Permit (A)
4	10.1.1.1	172.16.1.1	Deny (C)
5	192.168.3.4	172.16.6.1	Deny (C)

The rule order will deny 10.1.99.1 to access 172.6.6.1.

## 8.10 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.

- ▶ BASIC
- ▼ ADVANCED
  - SHDSL.bis
  - WAN
  - BRIDGE
  - VLAN
  - ETHERNET
  - ROUTE
  - NAT/DMZ
  - VIRTUAL SERVER
  - FIREWALL
  - IP QoS
- ▶ STATUS
- ▶ ADMIN
- ▶ UTILITY

Click **Enable** at item Trigger IP QoS Service in General IP QoS Parameter, which turn on this function if you want to enable it.

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

The screenshot shows the 'ADVANCED - IP QoS' configuration page. It includes a navigation bar with tabs: Home, Basic, Advanced, Status, Admin, and Utility. The main content area is titled 'ADVANCED - IP QoS' and contains the following sections:

- IP QoS Parameters:**
  - General IP QoS Parameters:** Trigger IP QoS Service:  Disable  Enable
  - IP QoS Policies:** (Empty table)

The table for IP QoS Policies has the following columns: Index, Enable, Protocol, Local, Remote, Precedence, and Description. The current state of the table is 'Pool is Empty!'. At the bottom right, there are three buttons: Cancel, Add, and Finish.

Set the policy to action.

**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.

**IP QoS - POLICY 1**

**IP QoS Policy Parameters:**

- Policy Rule:
  - Description:
  - Local IP:  e.g., Any:0.0.0.0, Single:10.0.0.1
  - Remote IP:  range:192.168.0.1-192.168.0.76
  - Local Port:  e.g., Any:0-65535, Single:80
  - Remote Port:  range:1024-5050
  - Protocol:
  - Precedence:

Buttons: Back, Ok

This is an example for your reference,

192.168.1.60 is the highest priority to undergo the over full bandwidth situation. 192.168.1.50 is the second high priority; 192.168.1.40 is the third high priority and so on.

**ADVANCED - IP QoS**

**IP QoS Parameters:**

- General IP QoS Parameters:
  - Trigger IP QoS Service:  Disable  Enable
- IP QoS Policies:
 

Index	Enable	Protocol	Local	Remote	Precedence	Description
C 1	<input type="text" value="ON"/>	ANY	192.168.1.10 0-65535	0.0.0.0 0-65535	0	priority 6
C 2	<input type="text" value="ON"/>	ANY	192.168.1.20 0-65535	0.0.0.0 0-65535	1	priority 5
C 3	<input type="text" value="ON"/>	ANY	192.168.1.30 0-65535	0.0.0.0 0-65535	2	priority 4
C 4	<input type="text" value="ON"/>	ANY	192.168.1.40 0-65535	0.0.0.0 0-65535	3	priority 3
C 5	<input type="text" value="ON"/>	ANY	192.168.1.50 0-65535	0.0.0.0 0-65535	4	priority 2
C 6	<input type="text" value="ON"/>	ANY	192.168.1.60 0-65535	0.0.0.0 0-65535	5	priority 1

Buttons: Cancel, Modify, Delete, Add, Finish

## 9 Administration

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



### 9.1 Security

For system security, 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 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.

Home Basic Advanced Status Admin Utility

**ADMIN - SECURITY**

Supervisor Profile and Security Parameters:

- Supervisor ID and Password:
  - Supervisor ID:
  - Supervisor Password:
  - Password Confirm:
- User Profile:
 

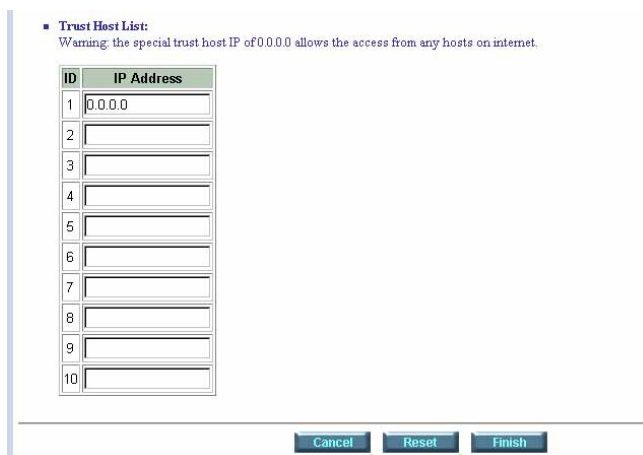
ID	User Name	User Password	Password Confirm	UI Mode
1	admin	****	****	Menu
2	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command
3	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command
4	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command
5	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command
- General Parameters:
  - Telnet Port:

Configured 0.0.0.0 will allow all hosts on Internet or LAN to access the router.

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

If you type the exact IP address in the field, only the host can access the router.

Click **Finish** to finish the setting.



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

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

## 9.2 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.

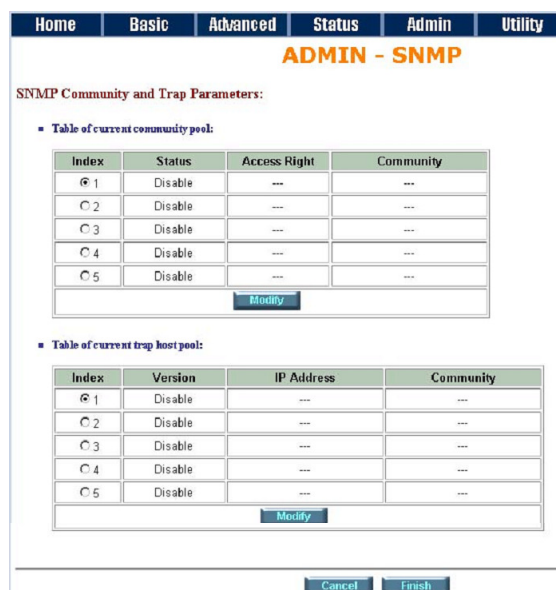
Click **SNMP** to configure the parameters.



In the table of current community pool, you can setup the access authority.

In the table of current trap host pool, you can setup the trap host.

Press **Modify** to modify the community pool.



SNMP status:

**SNMP Community and Trap Parameters:**

■ Table of current community pool:

Index	Status	Access Right	Community
1	<input type="text" value="Disable"/>	<input type="text" value="Deny"/>	<input type="text" value="private"/>
2	<input type="text" value="Disable"/>	---	---
3	<input type="text" value="Disable"/>	---	---
4	<input type="text" value="Disable"/>	---	---
5	<input type="text" value="Disable"/>	---	---

**Access Right:**  for deny all access  
 for access read only  
 for access read and write.

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

**SNMP Community and Trap Parameters:**

■ Table of current community pool:

Index	Status	Access Right	Community
1	<input type="text" value="Disable"/>	<input type="text" value="Deny"/>	<input type="text" value="private"/>
2	<input type="text" value="Disable"/>	<input type="text" value="Deny"/>	---
3	<input type="text" value="Disable"/>	<input type="text" value="Read"/>	---
4	<input type="text" value="Disable"/>	---	---
5	<input type="text" value="Disable"/>	---	---

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.  is for SNMPv1;  for SNMPv2).

**IP Address:** type the trap host IP address  
**Community:** type the community password. The community is setup in community pool. Press  to finish the setup.

■ Table of current trap host pool:

Index	Version	IP Address	Community
1	<input type="text" value="Disable"/>	<input type="text" value="192.168.0.254"/>	<input type="text" value="private"/>
2	<input type="text" value="Disable"/>	---	---
3	<input type="text" value="Disable"/>	---	---
4	<input type="text" value="Disable"/>	---	---
5	<input type="text" value="Disable"/>	---	---

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

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

### 9.3 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**.



Synchronization modes (**SYNC method**): **SNTP v4.0**, Simple Network Time Protocol **Sync with PC**, synchronization with PC.

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



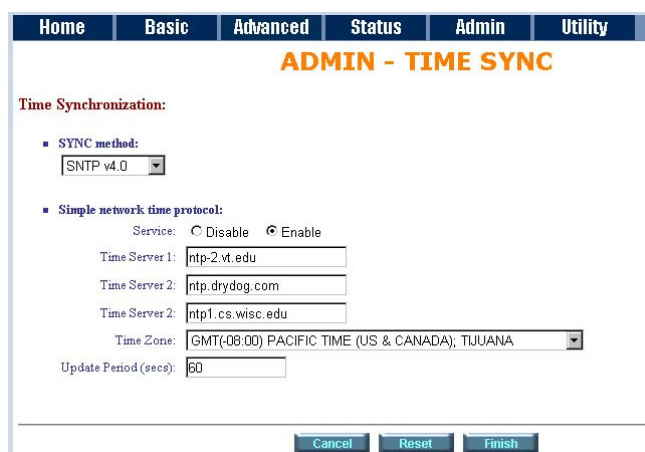
SNTP is the acronym for Simple Network Time Protocol, which is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. SNTP can be used when the ultimate performance of the full NTP implementation.

For SNTP, select **SNTP v4.0**.

**Service:** Enable

**Time Server 1:** All of the time server around the world can be used but suggest to use the timeserver nearby.

**Time Zone:** you have to choose the right time zone.



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

## 10 Utility

This section will describe the utility of the product including:

- SYSTEM INFO:** system information,
- CONFIG TOOL:** load the factory default configuration,
- UPGRADE:** upgrade the firmware
- LOGOUT:** logout the system
- RESTART:** restart the router.



### 10.1 System Info

Click **System Info** for review the information.

The browser will prompt the system information.



### 10.2 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**.

- **Load Factory Default:** it will load the factory default parameters to the gateway.

**Note:** This action will change all of the settings to factory default. On the other hand, you will lose all the existing configured parameters.

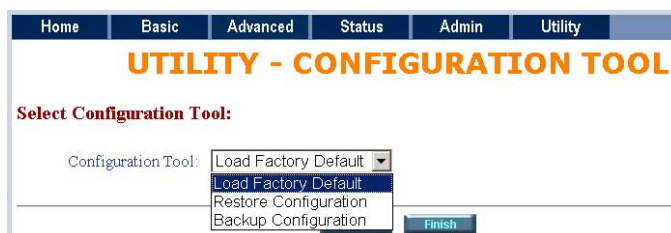
- **Restore Configuration:** Sometime the configuration crashed occasionally, it will help you to recover the backup configuration easily.

- ✧ Click **Finish** after selecting **Restore Configuration**.

- ✧ Browse the route of backup file then press finish. The router will automatically restore the saved configuration.

- **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 named backup. Press **Finish**. The router will automatically backup the configuration.



### 10.3 Upgrade

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



Browse the file and press **OK** button to upgrade. The system will reboot automatically after finishing.



### 10.4 Logout

To logout the router, press **LOGOUT** in **UTILITY**.



### 10.5 Restart

For restarting the router, click the **Restart** in **UTILITY**.

Press **Restart** to reboot the router.





## 11 Status

You can monitor the **SHDSL.bis** status including **mode**, **Tx power** and **Bitrate** and Performance information including **SNR margin**, **attenuation** and **CRC error count**.

**LAN** status will prompt the **MAC address**, **IP address**, **Subnet mask** and **DHCP client** table.

**WAN** status will display the WAN interface information.

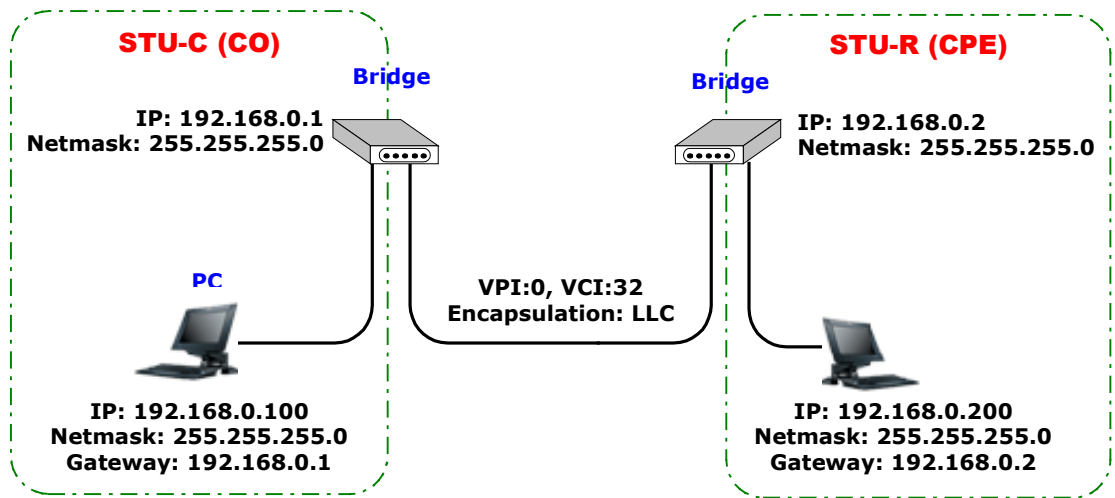
You can view the routing table in the status of **ROUTE**.

**INTERFACE** status includes LAN and WAN statistics information.

**FIREWALL** status displays DoS protection status and dropped packets statistics.



## 12 LAN-to-LAN connection with bridge Mode



### 12.1 CO side

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

Home	Basic	Advanced	Status	Admin	Utility
<b>BASIC - STEP 1</b>					
<b>Operation Mode:</b>					
System Mode: <input type="radio"/> ROUTE <input checked="" type="radio"/> BRIDGE					
SHDSL Mode: <input checked="" type="radio"/> CO Side <input type="radio"/> CPE Side					
<input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="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**

Home	Basic	Advanced	Status	Admin	Utility
<b>BASIC - STEP 2</b>					
<b>LAN:</b>					
IP Address: 192 . 168 . 0 . 1					
Subnet Mask: 255 . 255 . 255 . 0					
Gateway: 192 . 168 . 0 . 1					
Host Name: SOHO					
<b>WAN1:</b>					
VPI: 0					
VCI: 32					
Encap.: <input type="radio"/> VC-mux <input checked="" type="radio"/> LLC					
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="Next"/>					

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

## 12.2 CPE Side

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

The screenshot shows the 'BASIC - STEP 1' configuration screen. At the top, there is a navigation bar with tabs: Home, Basic, Advanced, Status, Admin, and Utility. Below the navigation bar, the title 'BASIC - STEP 1' is displayed in orange. Under the heading 'Operation Mode:', there are two rows of radio button options. The first row is 'System Mode:' with options 'ROUTE' (unselected) and 'BRIDGE' (selected). The second row is 'SHDSL Mode:' with options 'CO Side' (unselected) and 'CPE Side' (selected). At the bottom of the screen, there are three buttons: 'Cancel', 'Reset', and 'Next'.

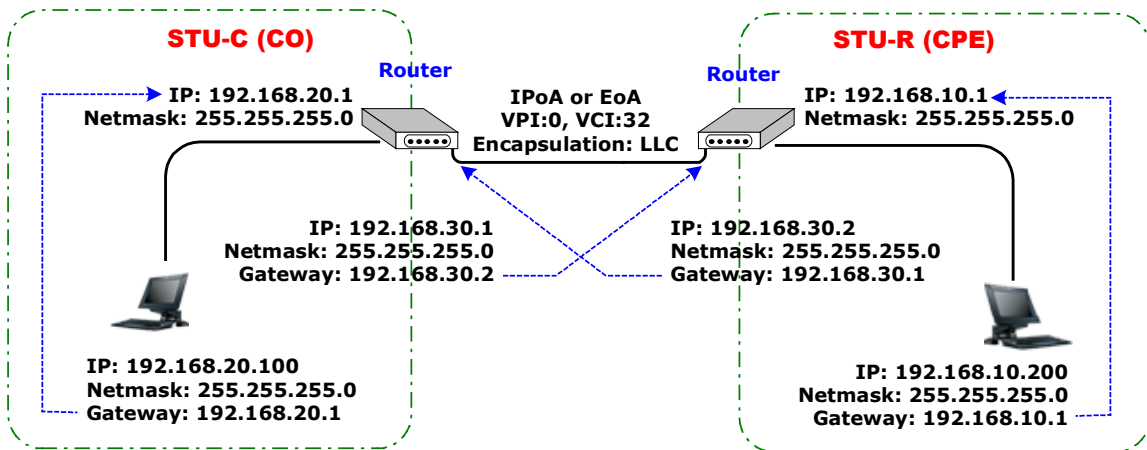
Enter **LAN** Parameters  
**IP:** 192.168.0.2  
**Subnet Mask:** 255.255.255.0  
**Gateway:** 192.168.0.2  
**Host Name:** SOHO

The screenshot shows the 'BASIC - STEP 2' configuration screen. It has the same navigation bar as Step 1. The title 'BASIC - STEP 2' is displayed in orange. Under the heading 'LAN:', there are four rows of input fields. The first row is 'IP Address:' with four boxes containing '192', '168', '0', and '2'. The second row is 'Subnet Mask:' with four boxes containing '255', '255', '255', and '0'. The third row is 'Gateway:' with four boxes containing '192', '168', '0', and '2'. The fourth row is 'Host Name:' with a text box containing 'SOHO'. Below the LAN section, under the heading 'WAN1:', there are two rows of input fields. The first row is 'VPI:' with a box containing '0'. The second row is 'VCI:' with a box containing '32'. Below these, there is an 'Encap:' section with radio button options 'VC-mux' (unselected) and 'LLC' (selected). At the bottom of the screen, there are four buttons: 'Back', 'Cancel', 'Reset', and 'Next'.

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.

# 13 LAN to LAN Connection with Routing Mode



## 13.1 CO Side

Click **ROUTE** and **CO Side**, then **Next**.

Home	Basic	Advanced	Status	Admin	Utility
<b>BASIC - STEP1</b>					
Operation Mode:					
System Mode: <input checked="" type="radio"/> ROUTE <input type="radio"/> BRIDGE					
SHDSL Mode: <input type="radio"/> CO Side <input checked="" type="radio"/> CPE Side					
<input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="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 DHCP Service on page 25.

Home	Basic	Advanced	Status	Admin	Utility
<b>BASIC - STEP2</b>					
LAN:					
IP Address: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="20"/> . <input type="text" value="1"/>					
Subnet Mask: <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>					
Host Name: <input type="text" value="SOHO"/>					
Trigger DHCP Service: <input type="radio"/> Disable <input checked="" type="radio"/> Enable					
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="Next"/>					

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.

Home	Basic	Advanced	Status	Admin	Utility
<b>BASIC - STEP4</b>					
WAN1:					
VPI: <input type="text" value="0"/>					
VCI: <input type="text" value="32"/>					
AAL5 Encap: <input type="radio"/> VC-mux <input checked="" type="radio"/> LLC					
Protocol: <input type="text" value="IPoA"/>					
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="Next"/>					

For more understanding about NAT, review NAT/DMZ on page 40.

**IP Address:** 192.168.20.1

Home	Basic	Advanced	Status	Admin	Utility
<b>BASIC - STEP5</b>					
WAN1:					
IP Address: <input type="text" value="10"/> . <input type="text" value="1"/> . <input type="text" value="2"/> . <input type="text" value="1"/>					
Subnet Mask: <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>					
Gateway: <input type="text" value="10"/> . <input type="text" value="1"/> . <input type="text" value="2"/> . <input type="text" value="2"/>					
DNS Server 1: <input type="text" value="168.95.1.1"/>					
DNS Server 2: <input type="text"/>					
DNS Server 3: <input type="text"/>					
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="Next"/>					

**Subnet Mask:** 255.255.255.0

**Gateway:** 192.169.30.2

Click **Next**

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

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

### 13.2 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 DHCP Service on page 25..

Type the WAN Parameters;

**VPI:** 0

**VCI:** 32

**AAL5 Encap:** LLC

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

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

Click **Next** to setup the IP parameters.

For more understanding about **NAT**, review NAT/DMZ on page 40.

**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 EPROM. Check the parameters before writing in EPROM.

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

The image shows three screenshots of the router's configuration web interface, specifically the 'Basic' configuration steps.

- Basic - Step 1:** Shows the 'Operation Mode' section. 'System Mode' has radio buttons for 'ROUTE' (selected) and 'BRIDGE'. 'SHDSL Mode' has radio buttons for 'CO Side' and 'CPE Side' (selected). Buttons for 'Cancel', 'Reset', and 'Next' are at the bottom.
- Basic - Step 2:** Shows the 'LAN' configuration. Fields include 'IP Address' (192.168.10.1), 'Subnet Mask' (255.255.255.0), and 'Host Name' (SOHO). 'Trigger DHCP Service' has radio buttons for 'Disable' and 'Enable' (selected). Buttons for 'Back', 'Cancel', 'Reset', and 'Next' are at the bottom.
- Basic - Step 5:** Shows the 'WAN1' configuration. Fields include 'VPI' (0), 'VCI' (32), 'AAL5 Encap' (VC-mux and LLC), and a 'Protocol' dropdown menu (IPoA selected). Below this, 'IP Address' (10.1.2.1), 'Subnet Mask' (255.255.255.0), and 'Gateway' (10.1.2.2) are shown. 'DNS Server 1' is 168.95.1.1. Buttons for 'Back', 'Cancel', 'Reset', and 'Next' are at the bottom.

## 14 Configuration via Serial Console or Telnet with Menu Driven Interface

### 14.1 Serial Console

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

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

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

**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.

### 14.2 Telnet

Make sure the correct Ethernet cable connected the LAN port of your computer to ROUTER. The LAN LNK 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,

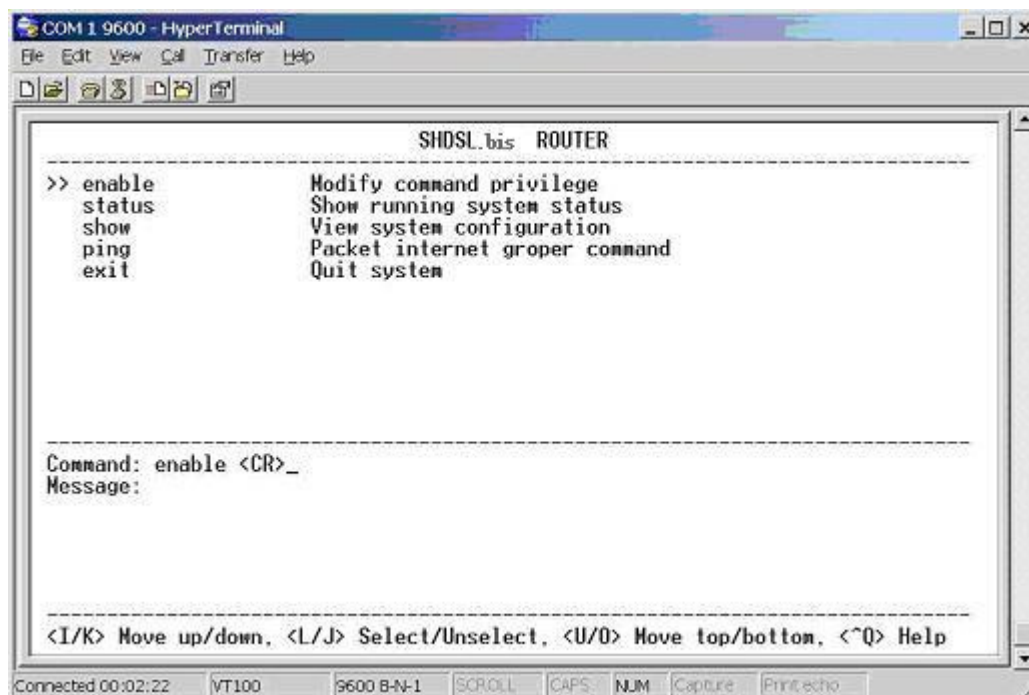
```
User: admin
Password: *****
```

**Note:** The default IP address is 192.168.0.1.

### 14.3 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 `↑`/`↓`, select one command by key `→`, and go back to a higher level of menu by key `←`. For example, to show the system information, just logon to the ROUTER, move down the cursor by pressing key `↓` twice and select “show” command by key `→`, you shall see a submenu and select “system” command in this submenu, then the system will show you the general information.



## 14.4 Window structure

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

1. **Product name**
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 <b>192.168.0.3</b> .
<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, <b>Route</b> 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.

## 14.5 Menu Driven Interface Commands

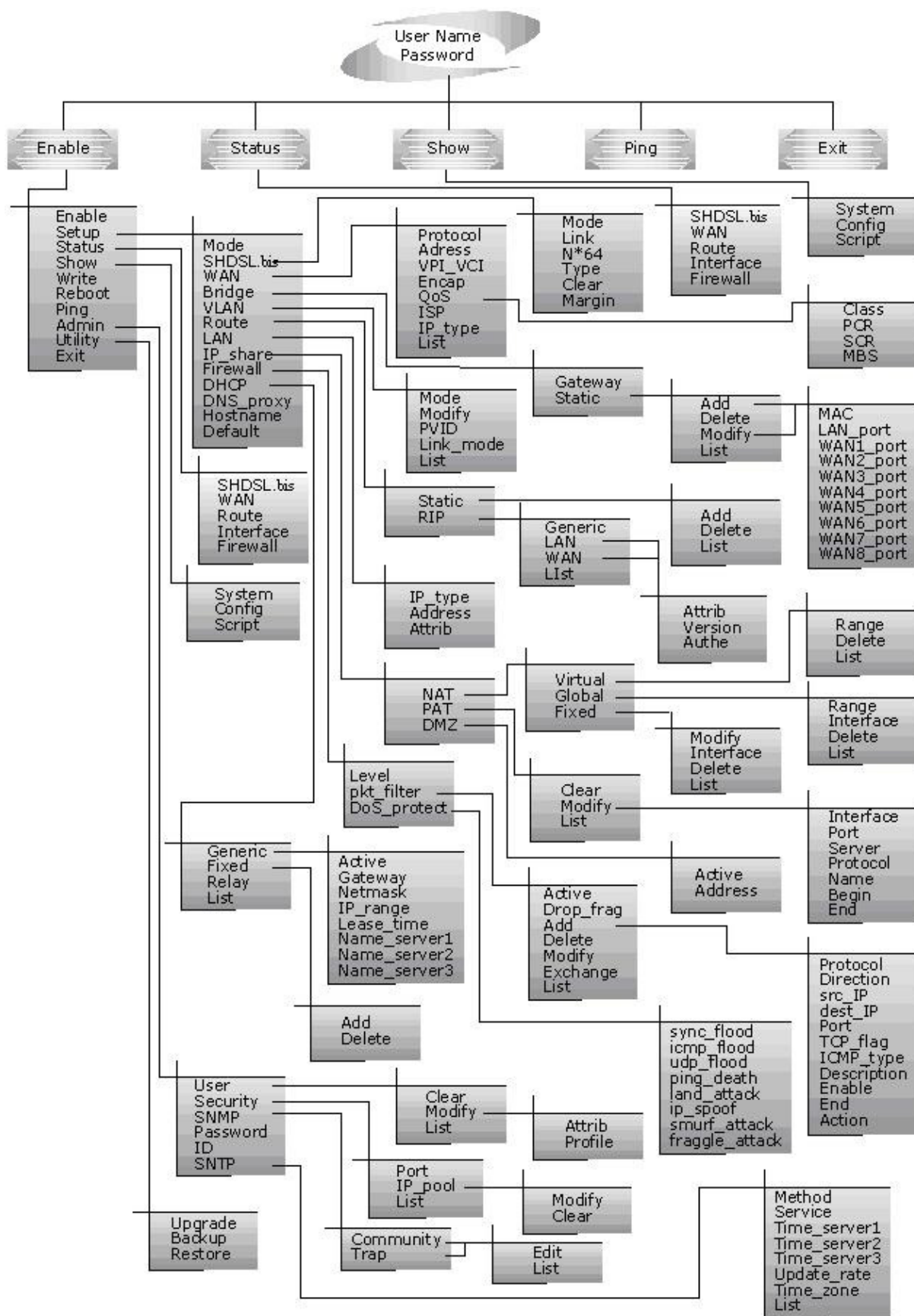
Before changing the configuration, familiarize yourself with the operations list in the following table. The operation list will be shown on the window.

<b>Menu Driven Interface Commands</b>	
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.
[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 + Q	For help

## 14.6 Menu Tree

The menu tree are as following figures. 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.





## 14.7 Configuration

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 EPROM 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 product, you have to use the setup command.
status	View the status of product.
show	Show the system and configuration of product.
write	Update flash configuration. After you have completed all necessary setting, make sure to write the new configuration to NVRAM by “ <b>write</b> ” 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 “ <b>reboot</b> ” command, or all of your changes will not take effect.
ping	Packet internet groper command.
admin	You can setup management features in this command.
utility	Upgrade software and backup and restore configuration are working via “ <b>utility</b> ” command.
exit	Quit system

## 14.8 Status

You can view running system status of SHDSL.bis, WAN, route and interface 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
-----

```

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 product access remote side information via EOC (embedded operation channel).
wan	WAN status shows the 8 PVC 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.

## 14.9 Show

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

Move cursor “ >> ” to **show** and press enter.

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

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

## 14.10 Write

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

Move cursor to “>>” to **write** and press enter.

-----  
Command: write <CR>

Message: Please input the following information.

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

## 14.11 Reboot

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

-----  
Command: reboot <CR>

Message: Please input the following information.

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

## 14.12 Ping

Ping command will be used to test the connection of router. 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 types of number of ping request packet to send, default, 1~65534 and -t. Default will send 4 packet and -t continuous packet until you key in Ctrl+c to stop.

## 14.13 Administration

You can modify the user profile, telnet access, 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
-----
```

### 14.13.1 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 product. We will not discuss command mode in this manual.



### 14.13.2 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. The default legal address is 0.0.0.0. It means that there is no restriction of IP to access the router via telnet.

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

### 14.13.3 SNMP

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

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

Move the cursor “>>” to **snmp** and press enter.

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

5 SNMP community entry 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
-----
```

5 SNMP trap entry can 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
-----
```

### 14.13.4 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
-----
```

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

Move the cursor “>>” to **sntp** and press enter.

```
-----
>> method          Select time synchronization method
   service          Tigger SNTP v4.0 service
   time_server1     Configure time server 1
   time_server2     Configure time server 2
   time_server3     Configure time server 3
   updatarate       Configure update period
-----
```

```
-----
time_zone      Configure GMT time zone offset
list           Show SNTP configuration
-----
```

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

move the cursor to method and press enter.

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

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

Move the cursor to service and press enter.

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

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

Move the cursor to time\_server1 and press enter.

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

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

You can configure three time servers in this system.

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) : 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.

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

GTM time zone offset (hours) (Enter for default) : -8
-----
```

Move the cursor to list and review the setting.

## 14.14 Utility

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

Move the cursor “>>” to **utility** and press enter.

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

## 14.15 Exit

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

## 14.16 Setup

All of the setup parameters are located in the subdirectories of setup. Move the cursor “>>” to **setup**

and press enter.

```

-----
>> mode          Switch system operation mode
   shdsl.bis     Configure SHDSL.bis parameters
   wan           Configure WAN interface profile
   bridge        Configure transparent bridging
   vlan          Configure virtual LAN parameters
   route         Configure routing parameters
   lan           Configure LAN interface profile
   ip_share      Configure NAT/PAT parameters
   firewall      Configure Firewall parameters
   dhcp          Configure DHCP parameters
   dns_proxy     Configure DNS proxy parameters
   hostname      Configure local host name
   default       Restore factory default setting
-----

```

### 14.16.1 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
-----

```

### 14.16.2 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
-----

```

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

Link type will be 2-wire or 4-wire mode according to the product. 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.

There are four types of SHDSL.bis Annex type, Annex-A, Annex-B, Annex-F, and Annex-G.

Clear command can clear CRC error count.

Generally, you cannot need to change SNR margin, which range is from 0 to 10. 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 2, the SHDSL.bis connection will drop and reconnect when the SNR margin is lower than 2. On the other hand, the device will reduce the line rate and reconnect for better line connection.

### 14.16.3 WAN

The router supports 8 PVC, private virtual circuit, and so you can setup eight WAN, WAN1 to WAN8. Move the cursor ">>" to **wan** and press enter. To setup WAN1, type **1**.

```
-----
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 an unique VPI and VCI value for Internet connection supported by ISP. The range of VPI is from 0 to 255 and VCI from 0 to 65535.

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 product supports UBR, CBR, VBR-rt and VBR-nrt. The peak cell rate can be configured from 64kbps to 2400kbps. 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)
-----
```

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

minutes.

Most of the ISP use dynamic IP for PPP connection but some of the ISP use static IP. Configure the IP type, dynamic or fixed, via `ip_type` command.

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

## 14.16.4 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:

```
-----
>> add          Add static MAC entry
   delete       Delete static MAC entry
   modify       Modify static MAC entry
   list        Show static bridging table
-----
```

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
   list        Show static bridging table
-----
```

## 14.16.5 VLAN

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

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

Move the cursor “>>” to **vlan** and press enter.

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

To 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.

## 14.16.6 802.11Q 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): 11001
-----
```

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.

### 14.16.7 STP

IEEE 802.1d to implement this feature for avoiding a storm in a redundant network environment 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.

It will send BPDU, a hello packet to make sure if the network is still stable. Once it can't receive the hello packet over the max. 20 sec., it will restart to process the above 4 steps.

### 14.16.8 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
   auth       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.

### 14.16.9 LAN

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

```
-----
>> address      LAN IP address and subnet mask
   attrib       NAT network type
-----
```

### 14.16.10 IP share

You can configure Network Address Translation (NAT), Port Address Translation (PAT) and Demilitarized Zone parameters in **ip\_share** menu. Move the cursor ">>" to **ip\_share** then press enter.

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

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.

### 14.16.11 NAT

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 address 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 entry via **range** command.

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

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

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.

## 14.16.12 PAT

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.

### 14.16.13 DMZ

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

---

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

---

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

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

---

```
Command: setup ip_share dmz address <ip> <1~10>
Message: Please input the following information.
```

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

---

### 14.16.14 Firewall

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_protection Configure DoS protection
-----

```

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.

### 14.16.15 Packet Filtering

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

```

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

```

To enable the packet filtering function, you can use **active** command.

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
-----

```

### 14.16.16 DoS Protection

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

```

-----
>> syn_flood      Enable protection SYN flood attack
  icmp_flood      Enable protection ICMP flood attack
  udp_flood       Enable protection UDP flood attack
  ping_death      Enable protection ping of death attack
  land_attack     Enable protection land attack
  ip_spooff       Enable protection IP spoofing attack
  smurf_attack    Enable protection smurf attack
  fraggle_attack  Enable protection fraggle attack
-----

```

A SYN flood 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 sender transmits a volume of requests for UDP diagnostic services which cause all CPU resources to be consumed serving the phony requests.

A ping of death attack attempts to crash your system by sending a fragmented packet, when reconstructed is larger than the maximum allowable size. Other known variants of the ping of death include teardrop, bonk and nestea.

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 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.

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.

### 14.16.17 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
-----
```

You can enable the IPQoS function via **active** command.

The add parameters of IPQoS can be configured via **add** command

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

The port type is configured by **protocol** command.

The local ip range is configured by **local\_ip** command.

The remote ip range is configured by **remote\_ip** command.

The port range is configured by **port** command.

To define the description of policy is configured by **description** command.

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

To define the priority of the policy is configured by **precedence** command

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

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

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

## 14.16.18 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      Configure generic DHCP parameters
    fixed       Configure fixed host IP address list
    list        Show DHCP configuration
-----
```

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

```
-----
>> active      Tigger DHCP 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
-----
```

Active the DHCP function with **active** command.

Set the default gateway via **gateway** command.

The subnet mask for DHCP client is configured by **netmask** command.

**ip\_range** command is to configure dynamic assigned IP address range.

The dynamic IP maximum lease time is configured by **lease\_time** command.

You can setup 3 domain name servers via **name\_server** commands.

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

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

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

## 14.16.19 DNS proxy

You can setup three DNS servers in the product. The number 2 and 3 DNS servers are option. 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:  
-----
```

## 14.16.20 Host name

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  
-----
```

## 14.16.21 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  
-----
```