USER MANUAL

SHDTU03-ET10R

SHDSL Router With
1-Port Ethernet Switch

SHDTU03-ET10RS

SHDSL Router With
4-Port Ethernet Switch

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Building
Neihu Technology Park
8F, No. 60 ZhouZi St.
Neihu, Taipei, 114
Taiwan

SHDTU03-ET10R SHDSL Router With 1-Port Ethernet Switch, SHDTU03-ET10RS SHDSL Router With 4-Port Ethernet Switch, Installation and Operation Manual
Version 3.0

Revision Marks

Revision	Date	Notes
V 2.0	**N/A**	**Software: Version: 1.5X7001r-XAT0**
V 3.0	**June 6, 2003**	**Software Version: 1.70XAF0.M2R (1.70XAF0.M2R-H62.3003-FR17-276B4WK0L0 23/Jan/2003 11:00**

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1.1 General

You are about to join the new ranks of G.SHDSL technology. Your new G.SHDSL Router is an external Single-Pair High-Speed Digital Subscriber Line (SHDSL) Router, which conveniently connects with a Switch, Hub or computer. The Router connects directly to telephone line via a standard RJ-11 connector.

The SHDSL (Single-Paired High Speed Digital Subscriber Line) router complies with G.992.2 standard and connects to any Ethernet LAN utilizing 10/100 Base-T auto-negotiation. It provides business-class, multi-range 192Kbps to 2.304Mbps payload rates over exiting single-pair copper wire. The SHDSL router is designed not only to optimize the service bit rate from central office to customer premises but also integrates high-end Bridging/Routing capabilities with advanced functions of Multi-DMZ, virtual server mapping and VPN pass-through.

The SHDSL router provides not only advanced functions like Multi-DMZ, virtual server mapping and VPN pass-through but advanced firewall functions, SPI, NAT, and DoS protection, to protect the internal LAN network from outside intruders.

The 4-port switching HUB on the "S" model supports four 10Base-T /100Base-T auto-negotiation and auto-MDIX switching ports to meet enterprise needs.

The SHDSL router allows customers to leverage the latest in broadband technologies to meet their growing data communication needs. Through the power of SHDSL products, you will have access to superior manageability and reliability.

1.2 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
- Build-in advanced SPI firewall (Firewall routers)
- 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 just one IP address
- Full ATM protocol stack implementation over G.SHDSL
- PPPoA and PPPoE support user authentication with PAP/CHAP/MS-CHAP
- SNMP management with SNMPv1/SNMPv2 agent and MIB II
- Get enhancements and new features via Internet download and software upgrade

1.3 Specifications

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 (Application Level Gateway) for ICQ/Netmeeting/MSN/Yahoo Messenger
- DNS relay and caching (RFC1034/1035)
- DHCP server (RFC2131/2132)

Bridging

- IEEE 802.1D transparent learning bridge

Security

- DMZ host/Multi-DMZ/Multi-NAT function
- Virtual server mapping (RFC1631)
- VPN pass-through for PPTP/L2TP/IPSec tunneling
- Natural NAT firewall

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/SNMPv2c (RFC1157/1901/1905) agent and MIB II (RFC1213/1493)
- Software upgrade via web-browser/TFTP server

ATM

- Up to 8 PVCs
- UBR/CBR/VBR traffic shaping
- OAM F5 AIS/RDI and loop back
- AAL5

AAL5 Encapsulation

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

PPP

- PPP over Ethernet (RFC 2516)
- PPP over ATM (RFC 2364)
- User authentication with PAP/CHAP/MS-CHAP

WAN Interface

- SHDSL: ITU-T G.991.2 (Annex A, Annex B)
- Encoding scheme: 16-TCPAM
- Data Rate: N x 64Kbps (N=1~36)
- Impedance: 135 ohms

LAN Interface

- 1-port (SHDTU03/ET10R) /
  4-ports switching hub (SHDTU03/ET10RS)
- 10 Base-T and 100 Base-TX auto-negotiation
- Auto-MDIX (4-port router)

Hardware Interface

- WAN: RJ-11
- LAN: RJ-45 x 4 (4-port router with or without firewall) or RJ-45 x 1 (1-port router with or without firewall)
- Console port: RS232

Indicators

- General: Power
- G.SHDSL: Link, Active
- Ethernet: 10M, 100M, Alarm (1-port router with or without firewall)
- Ethernet: 1, 2, 3, 4, Alarm (4-port router with or without firewall)

Physical/Electrical

- Dimensions: 18.7 x 3.3 x 14.5cm (WxHxD)
- Power: 100~240VAC (via power adapter)
- Power consumption: 6 watts
- Temperature: 0~45 C
- Humidity: 0%~95%RH (non-condensing)

Memory

- 2MB Flash Memory, 4MB SDRAM

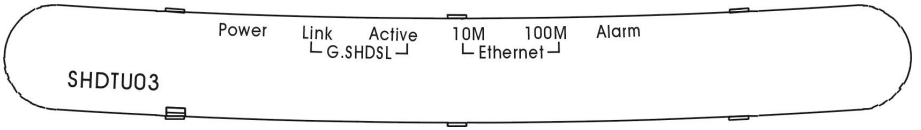
Products' Information

SHDTU03/ET10R: G.SHDSL router/bridge with 1-port LAN

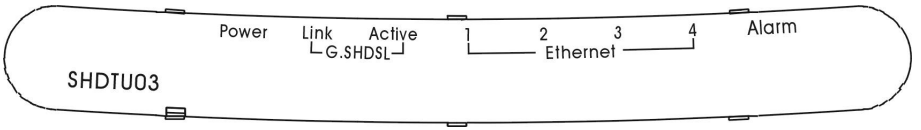
SHDTU03/ET10RS: G.SHDSL router/bridge with 4-port switching hub LAN

1.4 Front Panel

The front panel displays LED status



Front Panel of SHDTU03/ET10R



Front Panel of SHDTU03/ET10RS

LED status of 4-port router

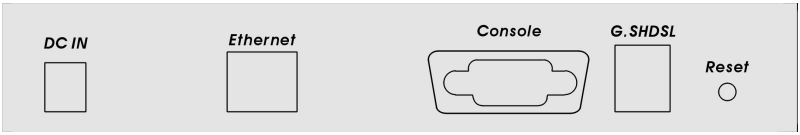
LEDs		*Active*	*Description*
Power		On	Power adaptor is connected to the router
G.SHDSL	Link	On	SHDSL line connection is established
	Active	On	Transmit or received data over SHDSL link
Ethernet	1	On	Transmit or received data over LAN Port 1
	2	On	Transmit or received data over LAN Port 2
	3	On	Transmit or received data over LAN Port 3
	4	On	Transmit or received data over LAN Port 4
Alarm		On	SHDSL line connection is dropped

Different LED status of 1-port router

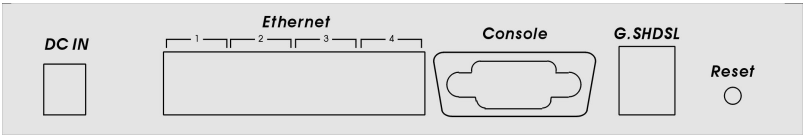
Ethernet	10M	On	LAN port acts in 10M
	100M	On	LAN port acts in 100M

1.5 Rear Panel

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



Rear Panel of SHDTU03/ET10R router with or without firewall



Rear Panel of SHDTU03/ET10RS router with or without firewall

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

Connectors Description of 1-port router

DC IN	Power adaptor inlet: Input voltage 9VDC
Ethernet	Ethernet 10BaseT for LAN port (RJ-45)
Console	RS- 232C (DB9) for system configuration and maintenance
G.SHDSL	SHDSL interface for WAN port (RJ-11)
Reset	Reset button for factory default

Connectors Description of 4-port router

DC IN	Power adaptor inlet: Input voltage 9VDC
Ethernet (1,2,3,4)	10/100BaseT auto-sensing and auto- MDIX for LAN port (RJ-45)
Console	RS- 232C (DB9) for system configuration and maintenance
G.SHDSL	SHDSL interface for WAN port (RJ-11)
Reset	Reset button for factory default


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

1. When you want to change the SHDTU03's configuration but you forgot the user name or password, press the Reset Button for three or four seconds with a paper clip or sharp pencil. Pressing the Reset Button in this way will cause the SHDTU03 to load the factory default settings and lose all of your configuration.

2. If the SHDTU03 is having problems connecting to the Internet and you want to configure it again by clearing all configurations, momentarily press the Reset Button with a paper clip or sharp pencil. Pressing the Reset Button in this way will cause the SHDTU03 to load the factory default configuration.

2.1 Configuration of the Router

This guide is designed to lead users through Web Configuration of SHDTU03/ET10R 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 to step 3.

For Serial Console Configuration, you can skips step 1 and 3.

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 confirm that the TCP/IP protocol has been installed.

Step 2: Check the Terminal Access Program

For Serial Console and Telnet Configuration, users need to setup the terminal access program with VT100 terminal emulation. If your PC or Notebook uses MS-Windows®, it is recommended that the Hyper Terminal™ Program be utilized for terminal configuration.

Step 3: Check the Web Browser in PC or NB

For Web Configuration, the PC or NB must have installed a Web Browser such as IE or Netscape.

Note: The Browser must support "Frames". Therefore it is recommended that for Web configuration the browsers IE5.0, Netscape 6.0 or above and 800x600 resolutions or above be used.

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	Bridged Ethernet over ATM
RFC1577	Classic Internet Protocol over ATM
RFC2364	Point-to-Point Protocol over ATM
RFC2516	Point-to-Point Protocol over Ethernet

The different Protocols need to setup different WAN parameters. Once knowing the Protocol provided by your ISP, you will need the following necessary WAN parameters.

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)

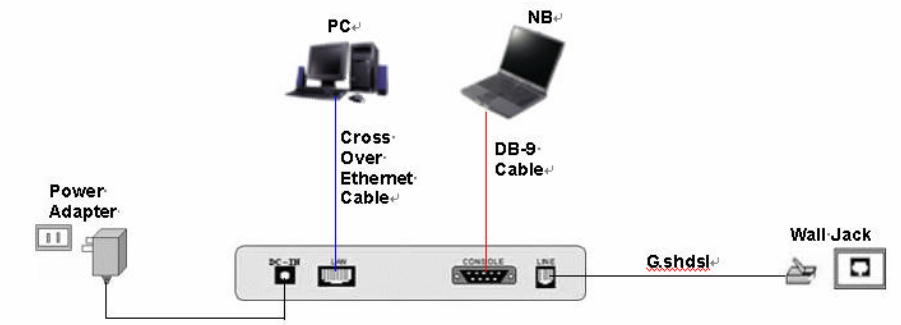
Step 5: Install the SHDSL Router

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

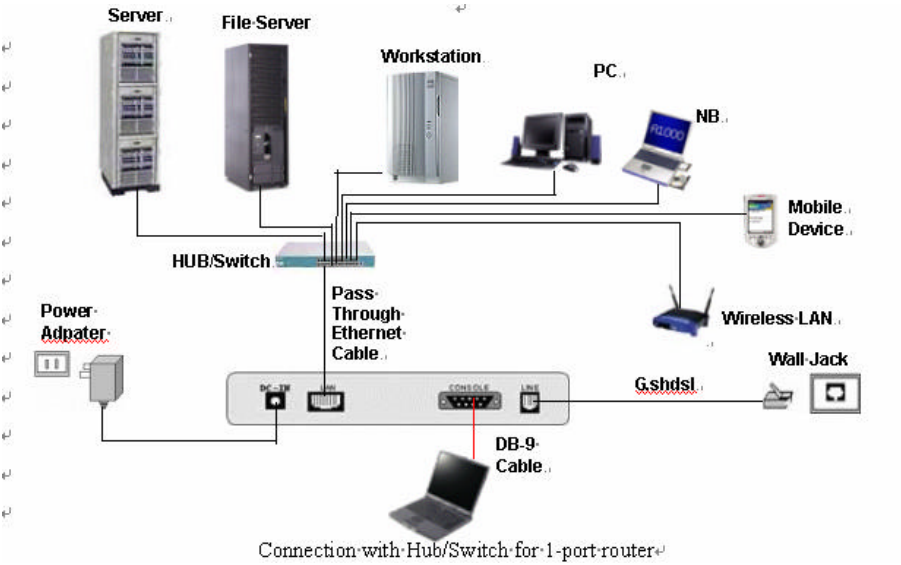
- Connect the power adapter to the port labeled DC-IN on the rear panel of the product.
- Connect the Ethernet cable.

If the 1-port router is directly connected to PC or NB, the Ethernet cable must use a cross over cable. If the 1-port router is connected to hub or switch, be sure that the hub or switch supports auto-sensing. If the HUB or Switch supports auto-MDIX, then both cross over and non cross over Ethernet cables are suitable. Otherwise, only straight through Ethernet cables may be used. The 4-port router has its own auto-MDIX switching hub so both straight through and cross-over Ethernet cables may be used.

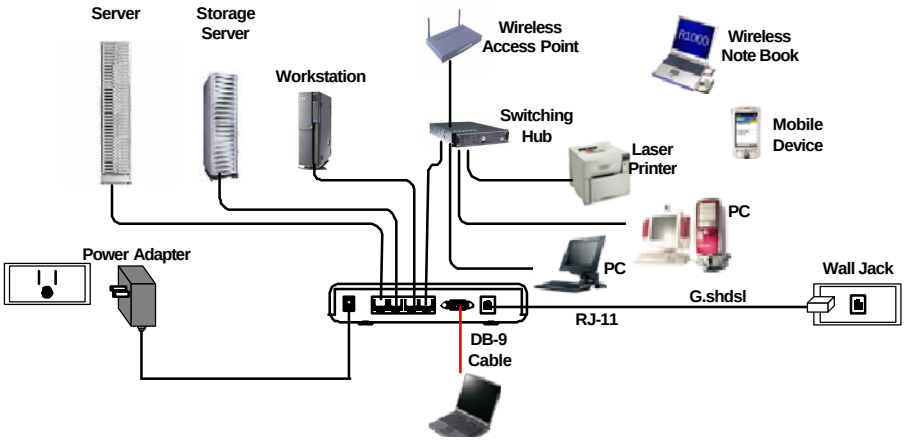
- Connect the phone cable to the SHDTU03 and the other side of phone cable to wall jack.
- Connect the power adapter to power source.
- Turn on the PC or NB which is used for configuration of the Router.



Direct Connection with PC or NB for 1-port router



Connection with Hub/Switch for 1-port router



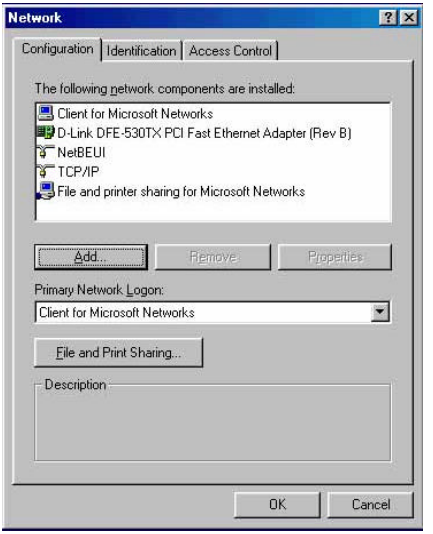
4-port router with complex network topology

2.2 Configuration via Web Browser

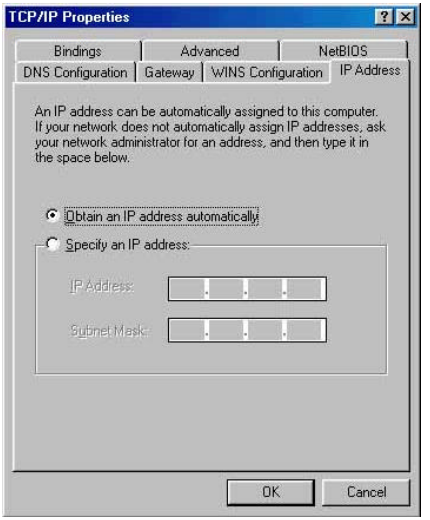
For Win85, 98 and Me, click the **start** button.
Select **setting** and **control panel**.

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 the **properties** button.



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



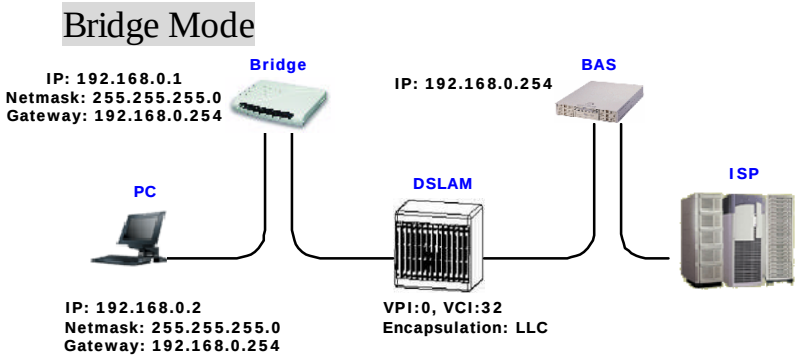
The window will ask you to restart the PC. Click the **Yes** button.
When the PC has restarted, Open Internet Explorer or Netscape Browser to connect to the Router. Type http://192.168.0.1
The default IP address and sub net-mask of the Router is 192.168.0.1 and 255.255.255.0. Because the router acts as DHCP server in your network, the router will automatically assign an IP address for the PC or NB on the network.

Type User Name root and Password root and then click OK.
The default user name and password are both *root*. For system security, it is recommended to change them after configuration.

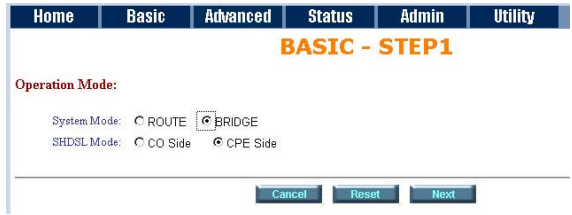
Note: After changing the User Name and Password, it is strongly recommend that you write the information in a safe place. If you forget the user/password setting the router must be factory Reset and all Configuration Settings will be lost.

3.1 Basic (Quick Setup)

The Basic Setup contains Bridge and Route operation modes. Follow this example to set Bridge mode Click Basic for basic installation.

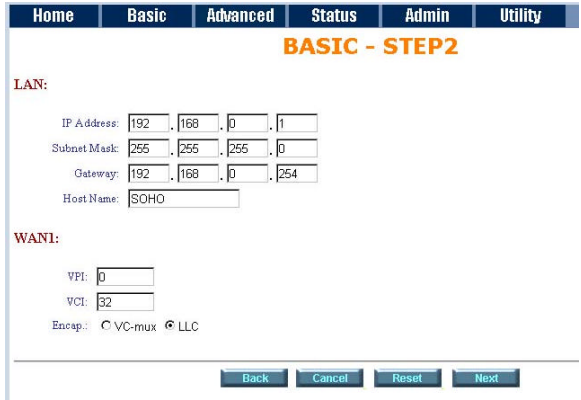


Click Bridge and CPE Side to setup Bridging mode of the Router and then click Next for the next setting.



LAN Parameters
Enter IP: 192.168.0.1
Enter Subnet Mask: 255.255.255.0
Enter Gateway: 192.168.0.254
Enter Host Name: SOHO

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

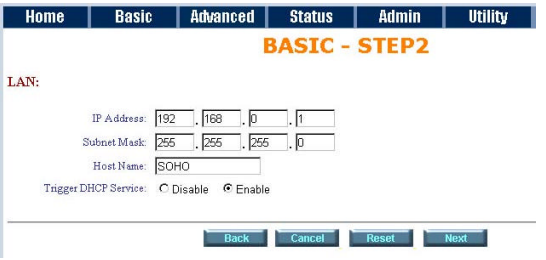


The screen will prompt with the new configuration parameters. Check the parameters and Click Restart The router will reboot with the new settings or Continue to configure other parameters.

Routing Mode

Routing mode contains settings for DHCP server, Point-to-Point Protocol over ATM and Ethernet, IP over ATM and Ethernet over ATM. You need to clarify which Internet protocol is provided by your ISP. Click ROUTE and CPE Side then press Next.

Type LAN parameters:
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: Enable
The default setup will Enable the DHCP server. If you want to turn off the DHCP service, choose Disable.



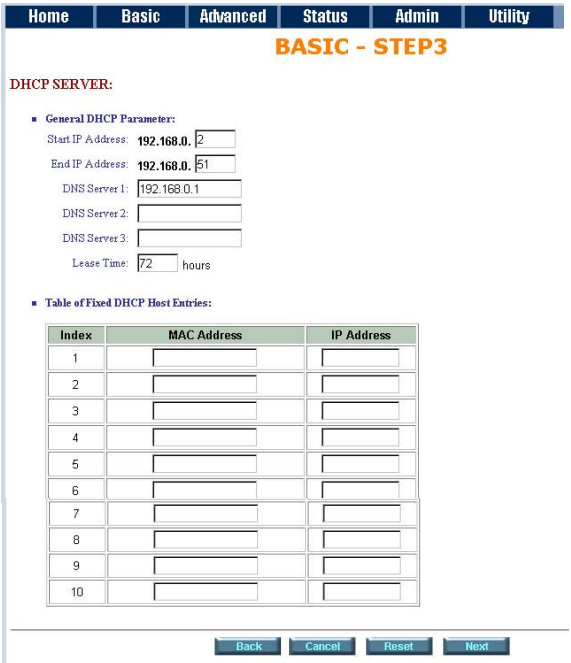
DHCP Server

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

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

If the DHCP server is Enabled, you will need to setup the following parameters for processing by the DHCP server.

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

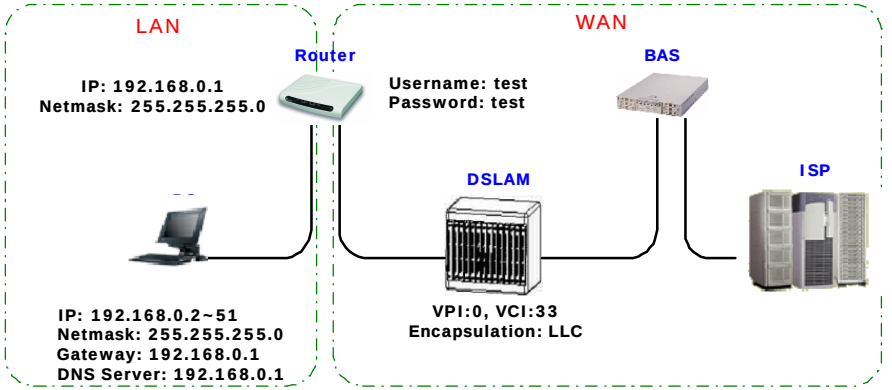


For this example: If the LAN IP address is 192.168.0.1, the IP range of LAN is 192.168.0.2 to 192.168.0.51. The DHCP server assigns the IP from Start IP Address to End IP Address. The legal IP address range is from 0 to 255, but 0 and 255 are reserved for broadcast so the useable IP address range is from 1 to 254. You may NOT assign an IP greater than 254 or less then 1. Lease time of 72 hours indicates that the DHCP server will not reassign the IP information to any new device for 72 hours.

Press Next to setup WAN parameters.

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 customer's modem or similar devices. PPPoE and PPPoA can be used in connections to offices or buildings. Users may 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.



Key in the WAN1 parameters:

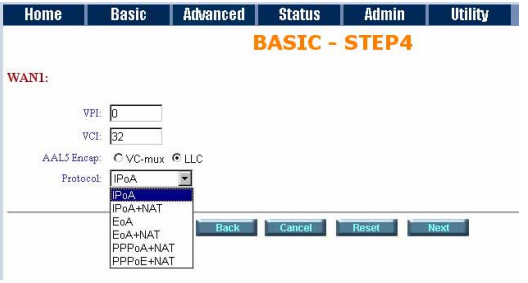
VPI: 0

VCI: 33

AAL5 Encap: LLC

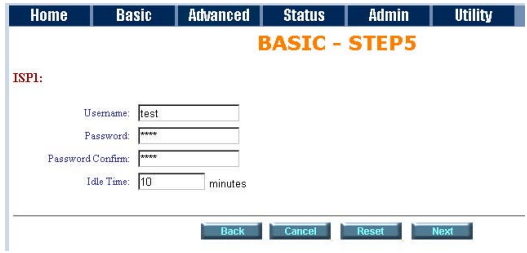
Protocol: PPPoA + NAT or PPPoE + NAT

Click Next to setup username and password.



For more understanding about NAT, review NAT/DMZ in page 3-15.

Type the ISP1 parameters.



Username and password are provided by your ISP.

Username: test

Password: test

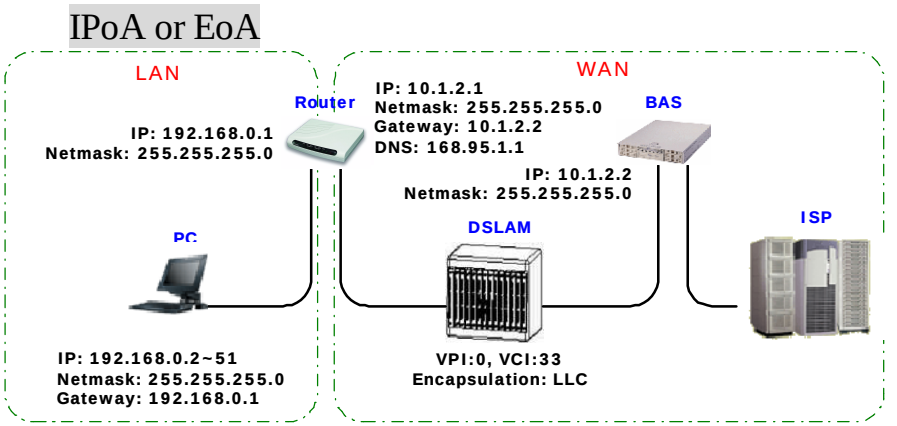
Password Confirm: test

Idle Time: 10

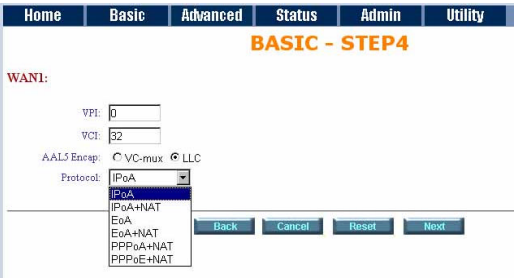
Click Next.

For security, the password will be displayed with star symbols.

The screen will prompt with the parameters to be written in Flash. Check the parameters before writing to Flash. Press Restart to restart the router with the new configuration or press continue to setup other parameters.

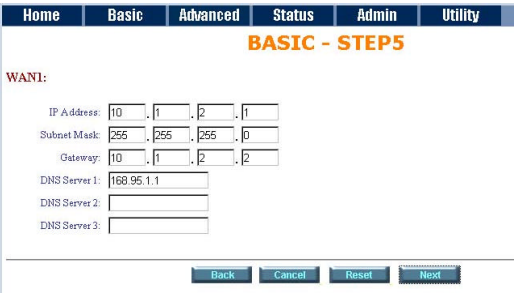


Type the Wan Parameters;
VPI: 0
VCI: 33
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT
Click Next to setup the IP parameters.



For more understanding about NAT, review NAT/DMZ in page 3-15.

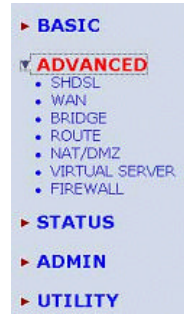
IP Address: 10.1.2.1
Subnet mask: 255.255.255.0
Gateway: 10.1.2.2
DNS Server 1: 168.95.1.1
Click Next



The screen will prompt with the parameters to be written to Flash. Check the parameters before writing to Flash. Press Restart to restart the router with the new configuration or press continue to setup other parameters.

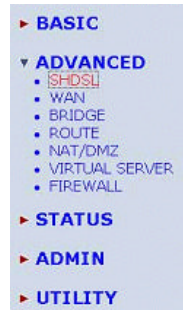
Congratulation! You are done. Your SHDSL Internet connection is established.

3.2 Advanced Set-Up

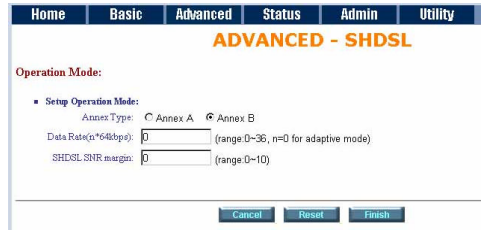


Advanced setup contains the configuration steps for SHDSL, WAN, Bridge, Route, NAT/DMZ, Virtual server and firewall parameters.

SHDSL



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

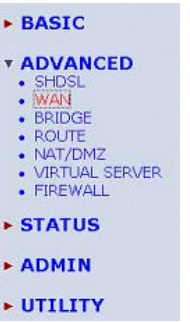


Annex Type: There are two Annex types supported, Annex A and Annex B, in SHDSL.
Data Rate: you can setup the SHDSL data rate in multiples of 64kbps.
SHDSL SNR margin: the margin range is from 0 to 10.

: Generally, the SNR margin does not require changing because it will affect the data rate.

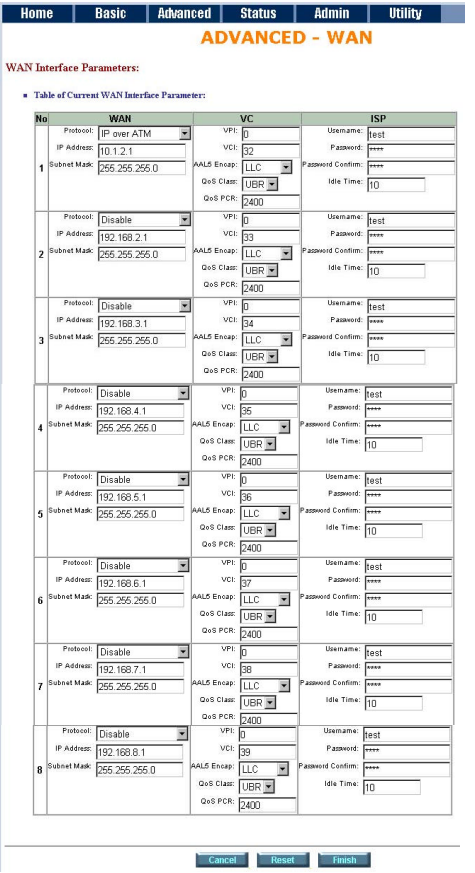
The screen will prompt with the parameters that will be written to Flash. Check the parameters before writing to Flash. Press Restart to restart the router with the new configuration or press continue to setup other parameters.

WAN



The SHDSL router supports up to 8 PVCs. The parameters are setup under WAN.

The WAN Number 1 will be the parameters setup in Basic Setup. If you want to setup another PVC, you may configure them in WAN 2 to WAN 8.
Enter the parameters.



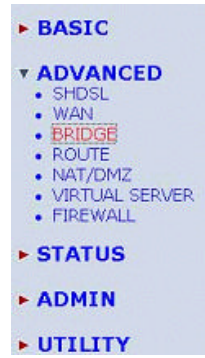
Press Finish to finish setting.

The screen will prompt with the parameters that will be written to Flash. Check the parameters before writing to Flash. Press Restart to restart the router with the new configuration or press continue to setup other parameters.

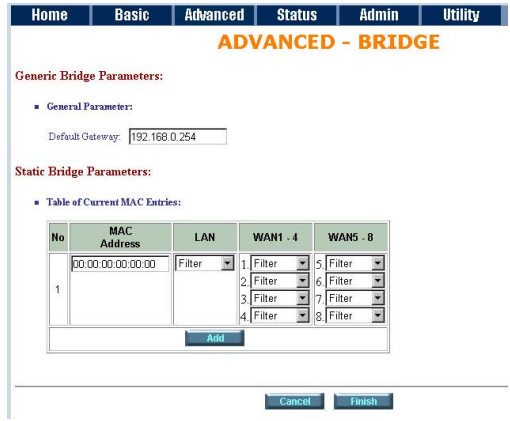
Bridge

The bridge mode can be setup with static bridge parameters.

Click Bridge to setup.



Press Add to add the static bridge information.



The screen will prompt with the parameters that will be written to Flash. Check the parameters before writing to Flash.

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

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.

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

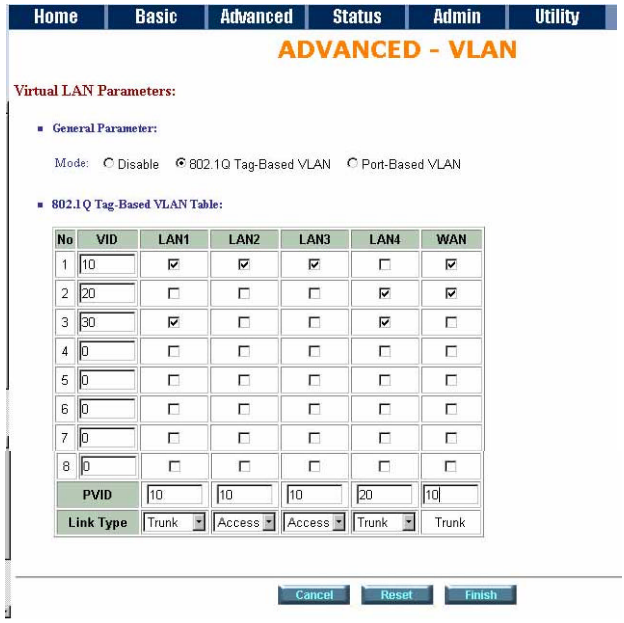
The specifications of VLAN functions are as follows:

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 to.
9. If VID and source address look up fails, the source address will be learned.

Click VLAN to configure VLAN.

The SHDTU03 supports two types of VLAN, 802.1Q and Port-Based. The user can configure either one of them in the router.

For setting 802.1Q VLAN click the 802.1Q Tag-Based VLAN. The screem will prompt as follows.



VID: Virtual LAN ID. Is a defined number, an ID which numbers from 1 to 4094.

PVID: Port VID is an untagged member of default VLAN.

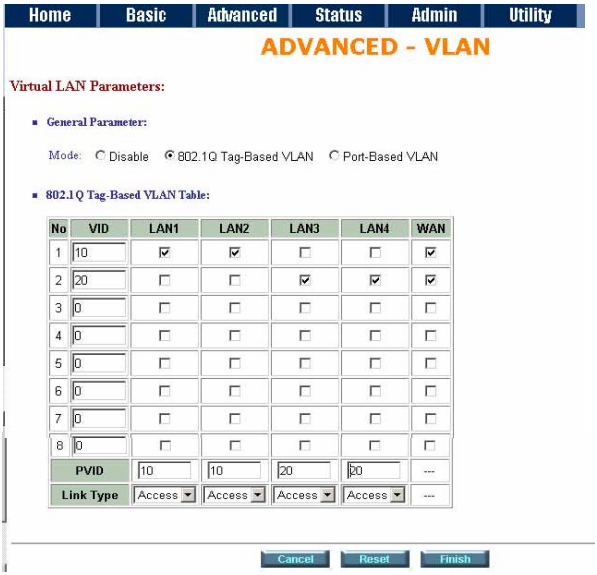
Link Type: Access means the port can send or receive untagged packets.

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

The Link Type of the WAN is assigned automatically depending on which mode the SHDTU03 is configured.

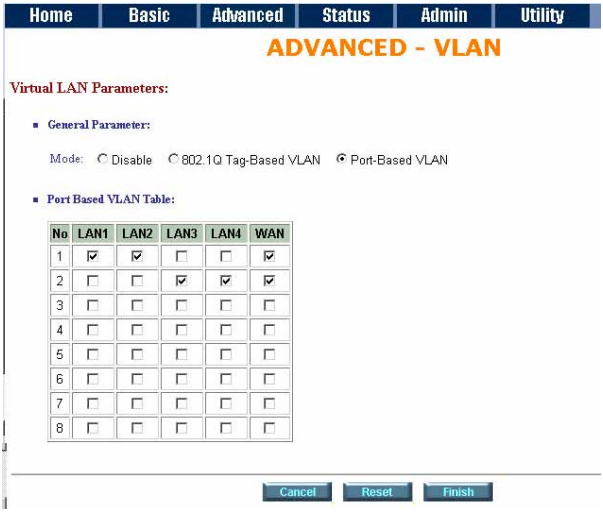
If the SHDTU03 works in bridge mode, the Link type of WAN will be Trunk, tagged port, and you can assign any PVID to WAN except 0 and leaving blank.

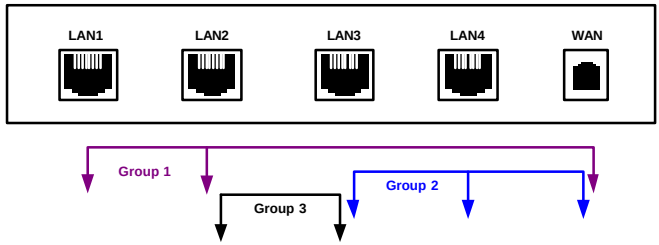
When the SHDTU03 works under routing mode, the Link Type of WAN will be Access mode, un-tagged port.



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.



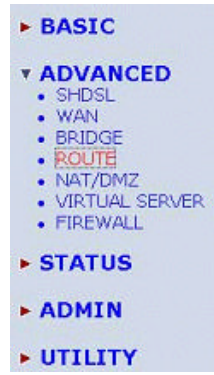


No	LAN1	LAN2	LAN3	LAN4	WAN
1	?	?	?	?	?
2	?	?	?	?	?
3	?	?	?	?	?
4	?	?	?	?	?
5	?	?	?	?	?

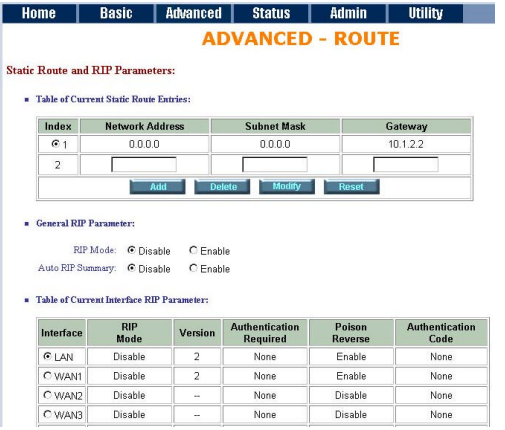
Route

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.

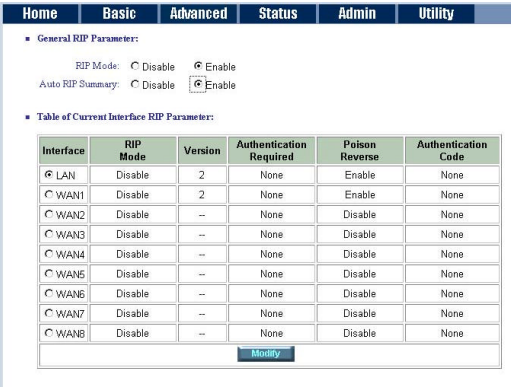
With Dynamic Routing, you can enable the Router to automatically adjust to the physical changes in the network's layout. The SHDTU03 G.SHDSL Firewall Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.



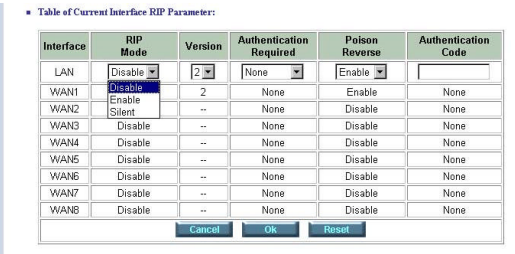
Click Route to modify the routing information.



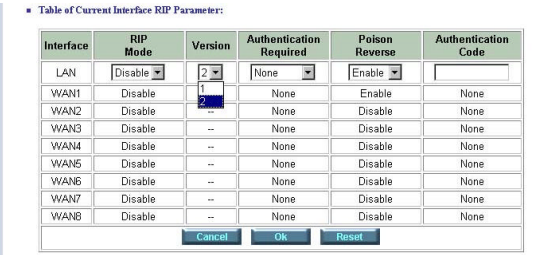
To modify the RIP (Routing information protocol) Parameters:
RIP Mode: Enable
Auto RIP Summary: Enable
Press Modify



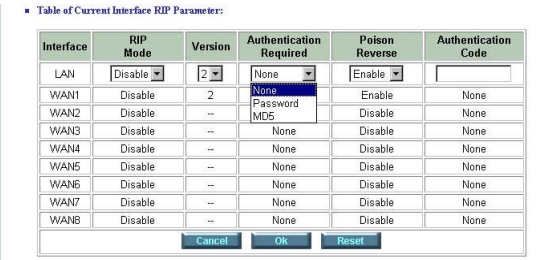
RIP Mode: this parameter determines how the product handles RIP (Routing information protocol). RIP allows it to exchange routing information with other routers. If set to Disable, the gateway does not participate in any RIP exchange with other routers. If set to Enable, the router broadcasts the routing table of the router on the LAN and incoporates RIP broadcast by other routers into it's routing table. If set silent, the router does not broadcast the routing table, but it accepts RIP broadcast packets that it receives.



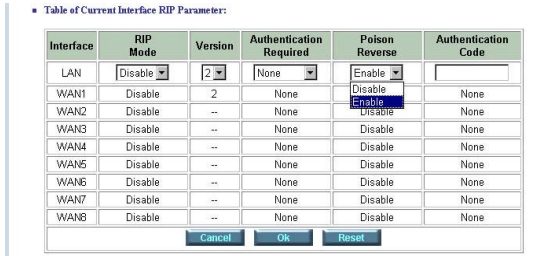
RIP Version: This determines the format and broadcasting method of any RIP transmissions by the gateway.
RIP v1: it only sends RIP v1 messages only.
RIP v2: it send RIP v2 messages in multicast and broadcast format.



Authentication required.
None: for RIP, there is no need for an authentication code.
Password: the RIP is protected by password, authentication code.
MD5: The RIP will be decoded by MD5 then protected by password, authentication code.

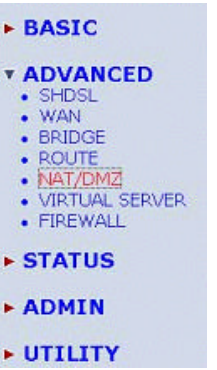


Poison Reserve is for the purpose of promptly broadcasting or multicasting RIP when the route is changed. (ex shutting down one of the routers in routing table)
Enable: the gateway will actively broadcast or multicast the routing information.
Disable: the gateway will not broadcast or multicast the information.



After modifying the RIP parameters, press finish.
The screen will prompt with the modified parameters. Check the parameters and press Restart to restart the router or press Continue to setup other parameters.

NAT/DMZ

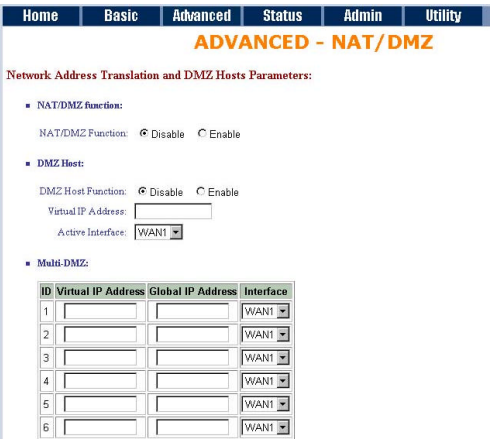


NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated as the inside network (private) and the other as the outside network (public). Typically, a company maps its local inside network addresses to one or more global outside IP addresses and reverses the global IP addresses of incoming packets back into local IP addresses. This ensures 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 allows the company to use a single IP address for its communication in the Internet world.

DMZ (demilitarized zone) is a computer host or small network inserted as a " neutral zone" between a company's 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.

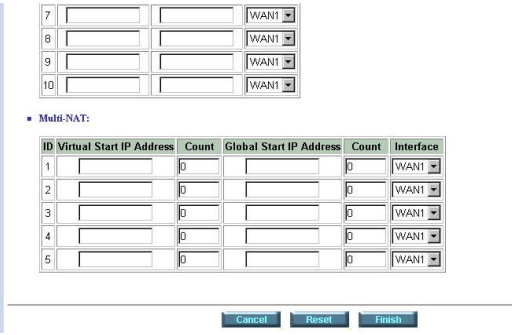
If you want to enable the NAT/DMZ functions, click Enable. Enable the DMZ host Function will use the IP address assigned to the WAN for enabling DMZ function for the virtual IP address.

Multi-DMZ: Some users who have two or more global IP addresses assigned by ISP can use the multi DMZ function. The table is for the mapping of global IP address and virtual IP address.

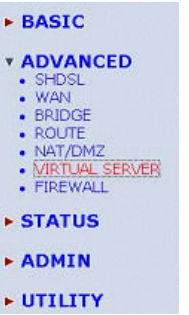
Multi-NAT: Some of the virtual IP addresses (eg: 192.168.0.10 ~ 192.168.0.50) collectively use two of the global IP addresses (eg: 69.210.1.9 and 69.210.1.10). The Multi-NAT table will be setup as;
Virtual Start IP Address: 192.168.0.10
Count: 40
Global Start IP Address: 69.210.1.9
Count: 2

Press Finish to continue.

The screen will prompt for the parameters that will be written to Flash. Check the parameters before writing to Flash. Press Restart to restart the router with the new configuratioin or Continue to configure other parameters.



Virtual Server



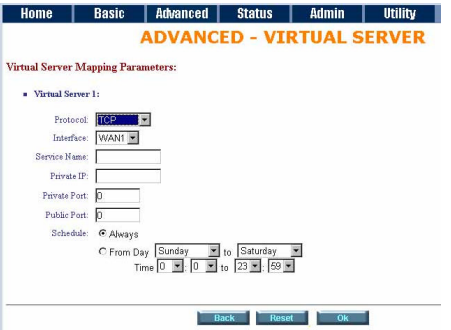
For example: Specific ports on the WAN interface are re-mapped to services inside the LAN. As an example, only 69.210.1.8 (e.g., assigned to WAN from ISP) is visible to the Internet, but does not actually have any services (other than NAT of course) running on gateway. It is said to be a virtual server. 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.

Type the necessary parameters then click Finish.



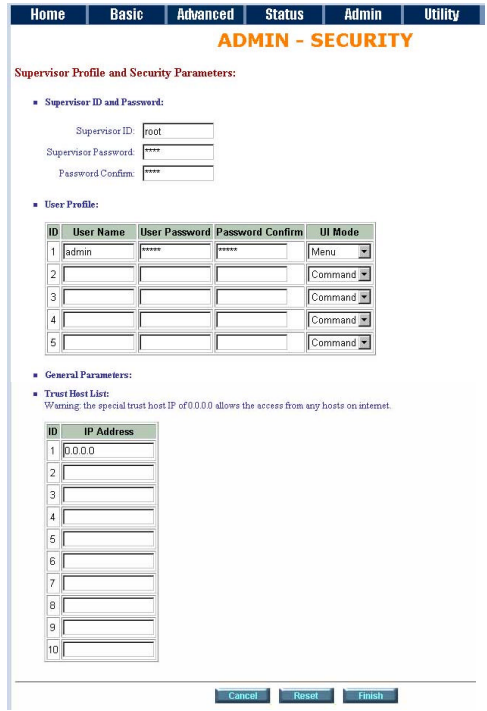
Press Restart to restart the router or press continue to setup other functions.

Chapter 4. Administration

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

Security

For system security, it is suggested to change the default user name and password after the first setup, otherwise unauthorized persons may gain access to 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's password for the gateway. If you do not change it, all users on your network will be able to access the gateway using the default IP and Password root.

You may authorize five legal users to access the router via telnet or console. There are two UI (user interface) modes, menu driven mode and command mode to configure the router.

Legal address pool will setup the legal IP addresses from which authorized persons can configure the gateway. This is a more secure function for the network administrator to setup the legal address of configuration.
Configuring as 0.0.0.0 will allow all hosts on the Internet to access the router.

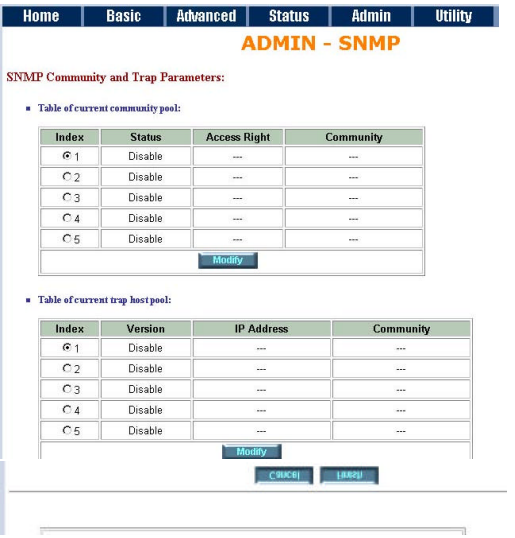
Click Finish to finish the setting.
The browser will prompt with the configured parameters. Check them before writing to Flash. Press Restart to restart the gateway with the new parameters and press Continue to setup other parameters.

SNMP

Simple Network Management Protocol (SNMP) is the protocol not only governing network management, but also for 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 II.

Click SNMP to configure the parameters.



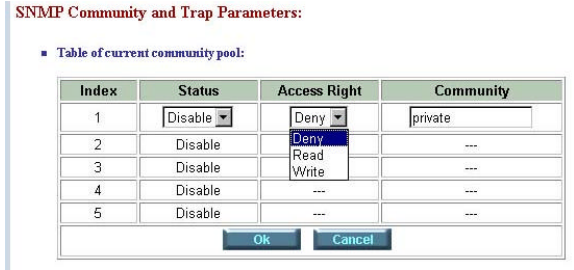
In the table of current community pool, you can setup the access authority.

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

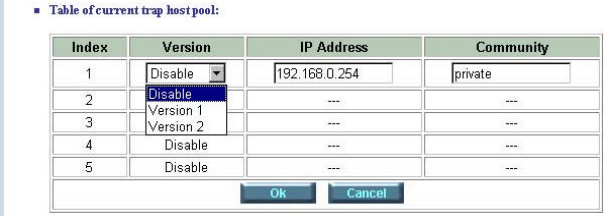
Press Modify to modify the community pool.

SNMP status: Enable

Access Right: Deny for deny all access
Access Right: Read for access read only
Access Right: Write for access read and write.
Community: it serves as password for access right.
After configuring the community pool, press OK.



Click Modify to modify the trap host pool.
Version: select version for trap host.
IP: type the trap host IP
Community: type the community password.
Press OK to finish the setup.



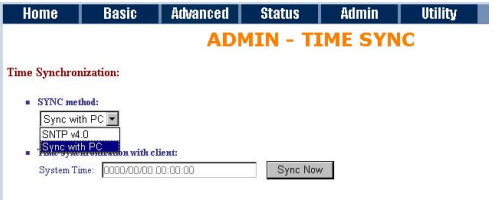
The browser will prompt with the configuration parameters. Check them before writing to Flash.

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

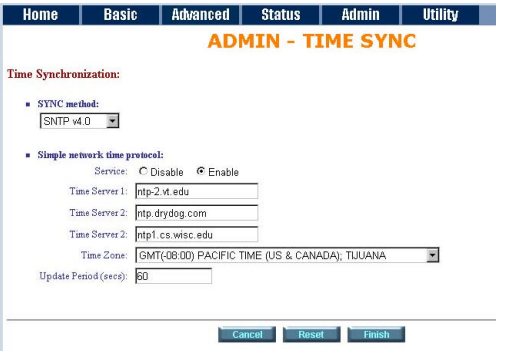
Time Sync

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

Click TIME SYNC.



There are two synchronization modes: Sample Network Time Protocol (SNTP) and 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 is required.

For SNTP, select SNTP v4.0.
SNTP service: Enable
Time Server: Any of the time servers around the world can be used but it is suggested to use a time server physically nearby.
Time Zone: you have to choose the right time zone.

Press Finish to finish the setup. The browser will prompt with the configuration parameters. Check them before writing to Flash.

Chapter 5. Utility

This section describes the utility to display the system information, load the factory default configuration, upgrade the firmware and restart the gateway.

System Info

Click System Info to review the system information.

The browser will prompt for the system information.

Config Tool

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

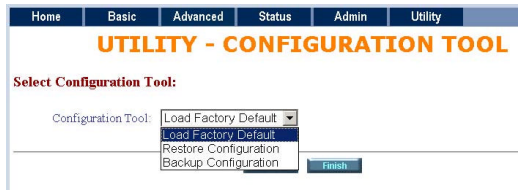
Press Config Tool.

Choose the function you wish to perform and then press finish.

- Load Factory Default function: this will load the factory default parameters to the gateway.

: All of the settings will be changed to factory default. Therefore, you will lose all the configured parameters.

- Restore Configuration: Sometimes the configuration will become corrupt unintentionally. Restore configuration will help you to recover the backup configuration easily.
- Click Finish after selecting the Restore Configuration.
- Browse the location of the backup file then press finish. The router will automatically restore the saved configuration.
- Backup Configuration: After configuration, it is recommended to use this function to backup your router parameters in the PC.
- Select the Backup Configuration and then press Finish.
- Browse to the location to backup the file named "backup". Press Finish. The router will automatically backup the configuration.



Upgrade

You can upgrade the gateway using the upgrade function.

Press Upgrade.

Browse to the file and press the OK button to upgrade. The system will reboot automatically after finishing. Do not allow any power disruption during the upgrade process.

Logout

To logout of the router, press logout.

Restart

For restarting the router, click the Restart item under UTILITY.

Press Restart to reboot the router.

This page was left blank intentionally.

Chapter 6. Status

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

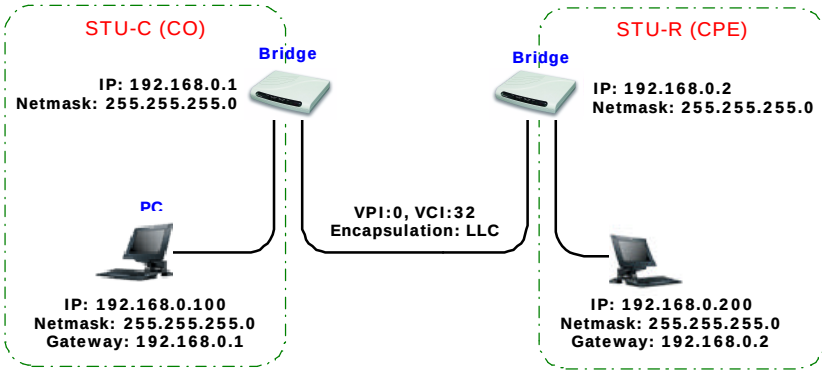
LAN status will display the MAC address, IP address, Subnet mask and DHCP client table.

WAN status will display the WAN interface information.

You can view the routing table from the "ROUTE" status.

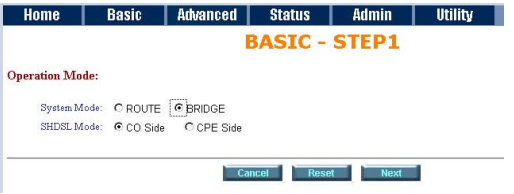
"INTERFACE" status includes LAN and WAN statistics information.

LAN-to-LAN connection with bridge Mode



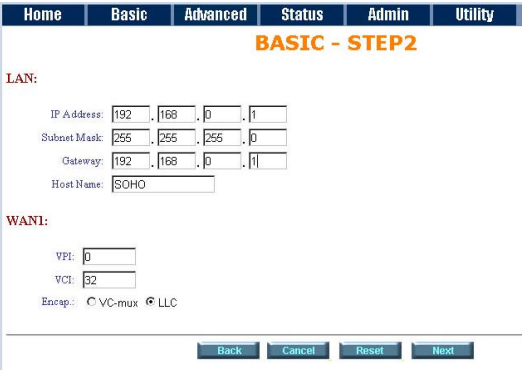
CO side

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



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

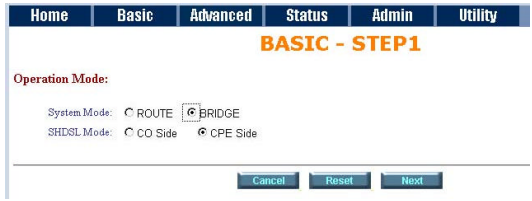
WAN1 Parameters
Enter VPI: 0
Enter VCI: 32
Click LLC
Click Next



The screen will prompt with the new configuration parameters. Check the parameters and Click Restart. The router will reboot with the new settings.

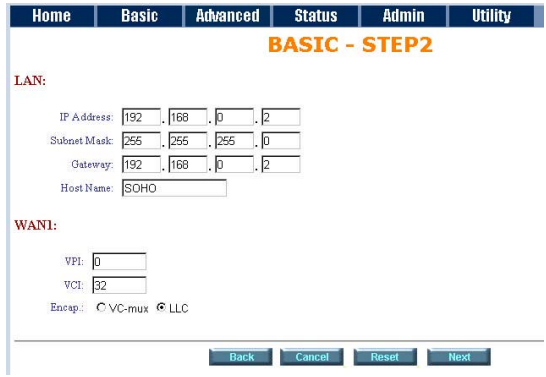
CPE Side

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



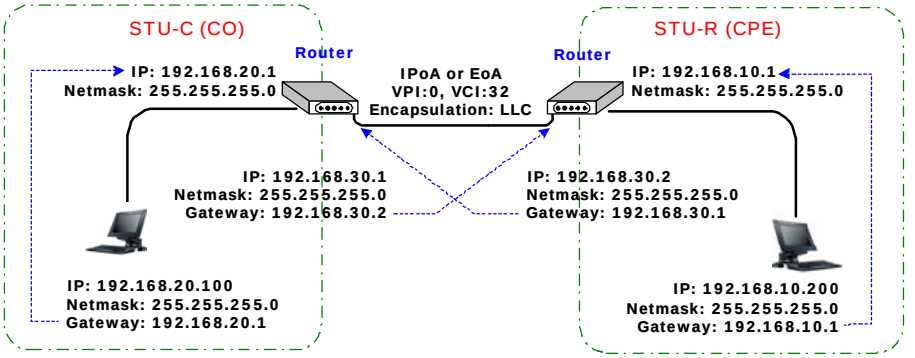
LAN Parameters
Enter IP: 192.168.0.2
Enter Subnet Mask: 255.255.255.0
Enter Gateway: 192.168.0.2
Enter Host Name: SOHO

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



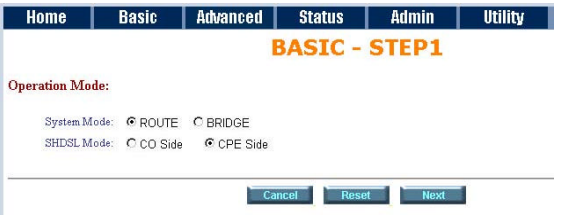
The screen will prompt with the new configuration parameters. Check the parameters and Click Restart The router will reboot with the new settings.

LAN-to-LAN connection in routing mode

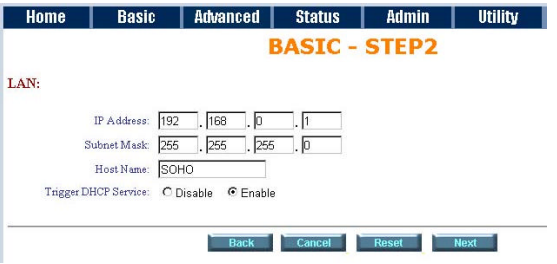


CO side

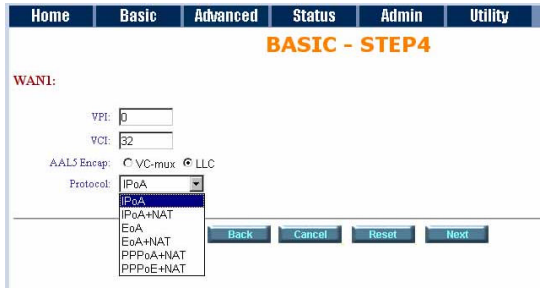
Click ROUTE and CO Side then press Next.



Type LAN parameters:
IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: For more DHCP service, review DHCP Service.

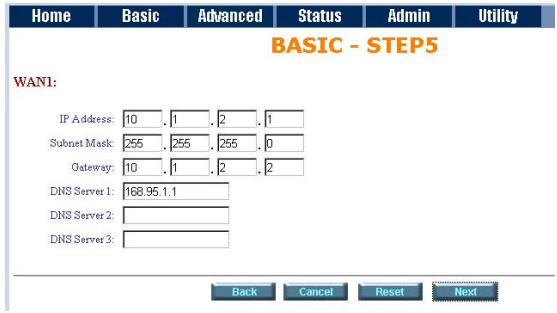


Type the Wan Parameters;
VPI: 0
VCI: 32
AAL5 Encap: LLC
Protocol: IPoA , EoA , IPoA + NAT or EoA + NAT
Note: The Protocol used in CO and CPE have to be the same.
Click Next to setup the IP parameters.



For more understanding about NAT, review NAT/DMZ in page 19.

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

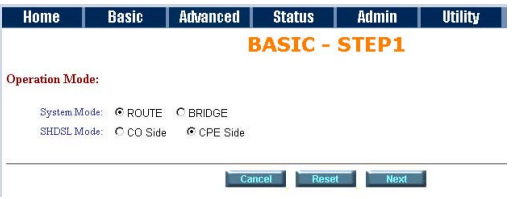


The screen will prompt with the parameters that will be written in Flash. Check the parameters before writing to Flash.

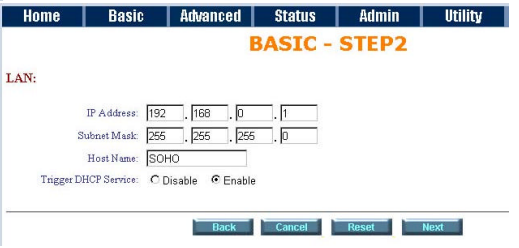
Press Restart to restart the router working with new parameters or press continue to setup another parameter.

CPE side

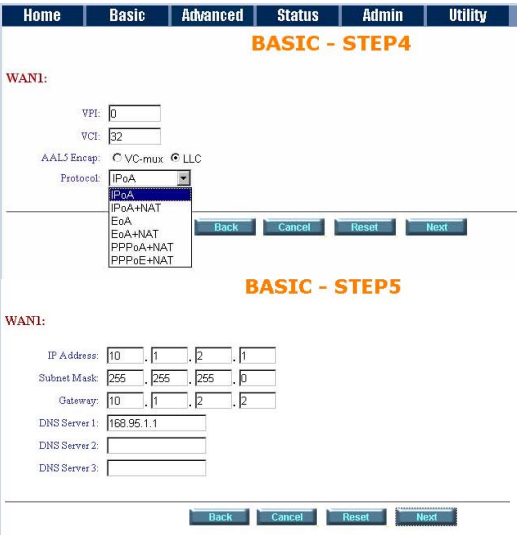
Click ROUTE and CPE Side then press Next.



Type LAN parameters:
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: For more DHCP service, review DHCP Service.



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 of NAT, review the NAT/DMZ section in this manual.



IP Address: 192.168.30.2
Subnet mask: 255.255.255.0
Gateway: 192.169.30.1
Click Next

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

Congratulation! You are done. Your SHDSL LAN-to-LAN connection is established.

Chapter 7. Serial Console or Telnet Mode

Serial Console

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

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

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

Telnet

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

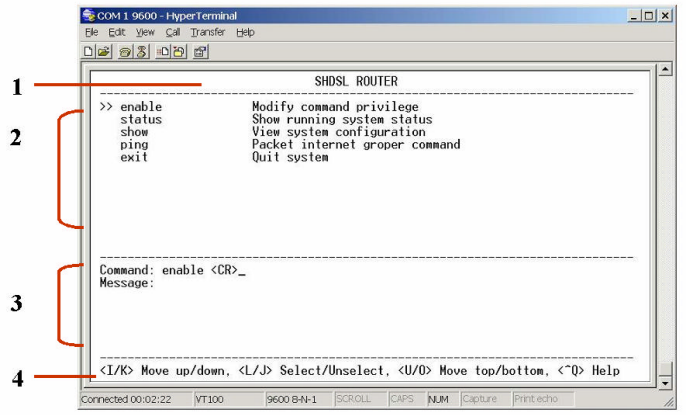
```
User:admin
Password: *****
```

Note: If you have not set any LAN IP of the Router, the default IP address is 192.168.0.1.

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 with a simple interface, which is better than working with script files. The menu driven interface is a user-friendly interface for general configuration 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 can scroll up/down by pressing key I / K, select one command by key L, and go back to a higher level of menu by key J. For example, to show the system information, just logon to the ROUTER, move down the cursor by pressing key K twice and select " show" the command by key L. You will see a submenu and can select the " system" command in this submenu. The system will then show you the general information.



Window structure

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

1. Product name
2. Menu field: Menu selection items are prompted on this field. The "**>>**" symbol indicates the cursor position.
3. Configuration field: You will configure the parameters in this field. **< parameters >** indicates the parameters you can choose and **< more...>** indicates that there is another submenu in the title.
4. Operation command for help

The following table shows the parameters in the brackets.

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

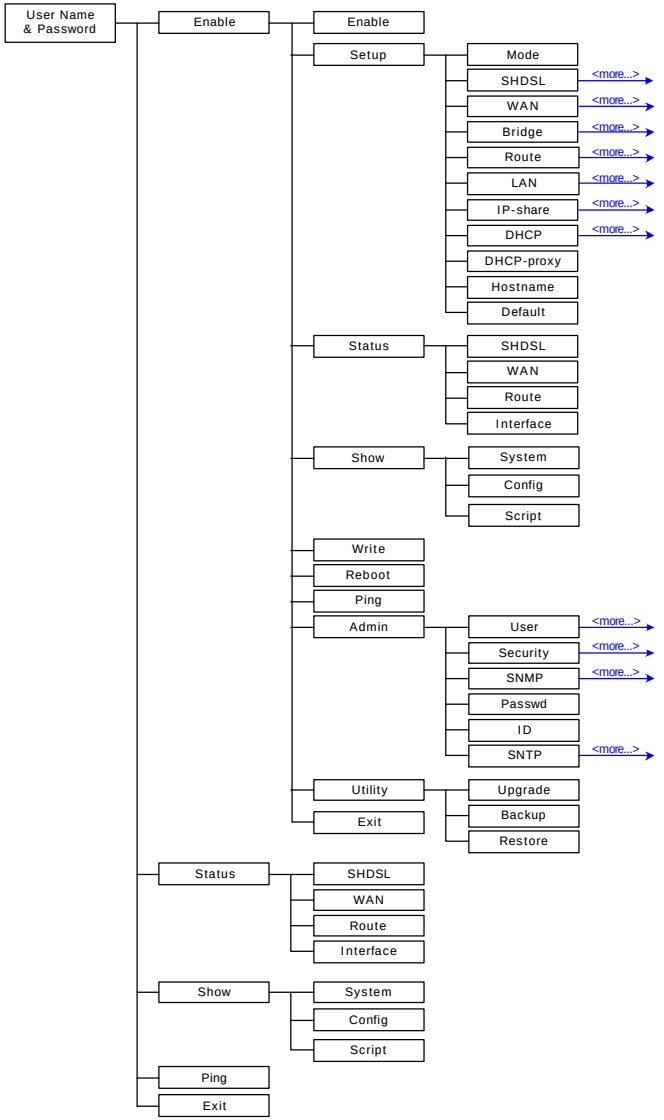
Menu Driven Interface Commands

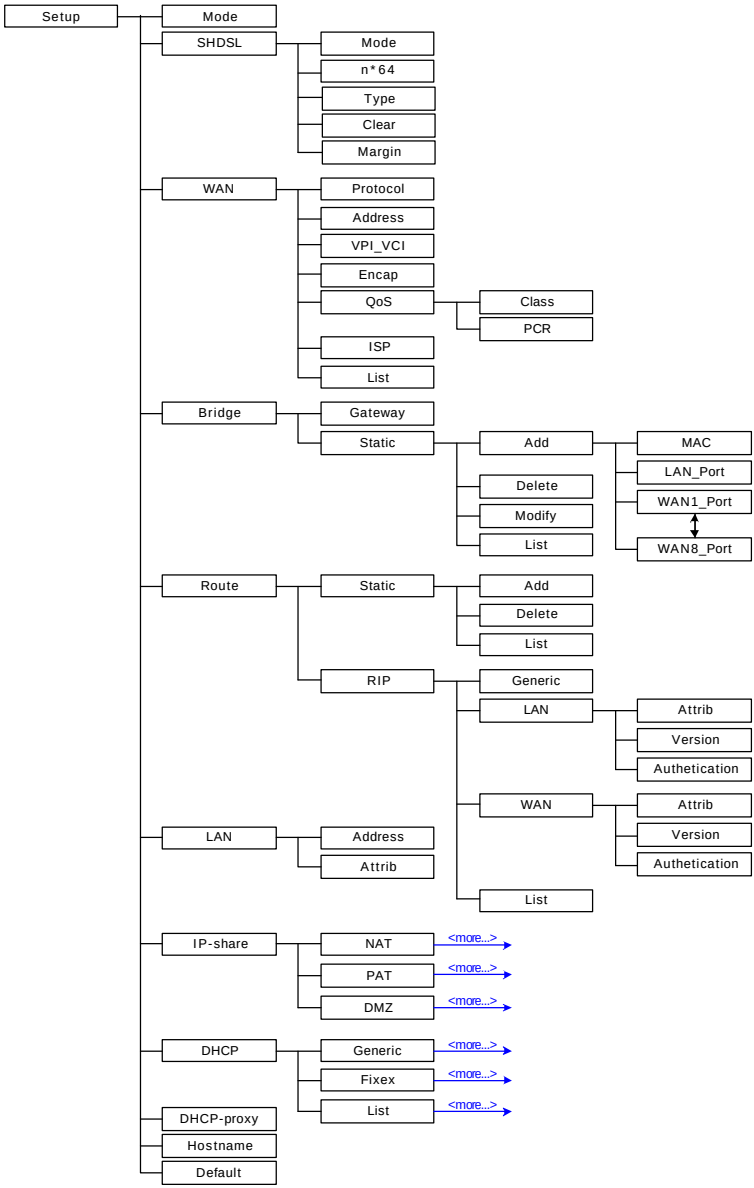
Before changing the configuration, familiarize yourself with the navigation keys listed in the following table. The operation list will be shown on the window.

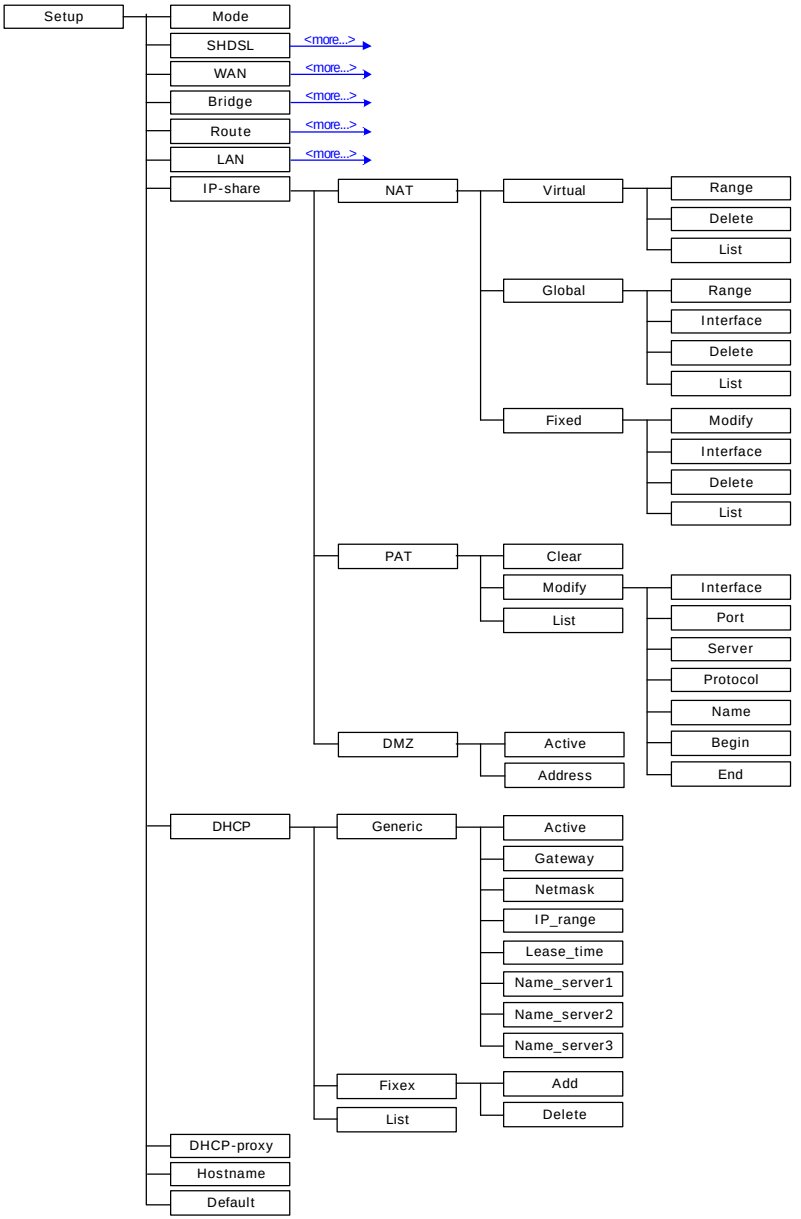
Keystroke	Description
[UP] or I	Move to field above in the same level menu.
[DOWN] or K	Move to field below in the same lever menu.
[LEFT] or J	Move back to previous menu.
[RIGHT] or L	Move forward to submenu.
[ENTER]	Move forward to submenu.
[TAB]	To choose another parameters.
Ctrl + C	To quit the configuring item.
Ctrl + Q	For help

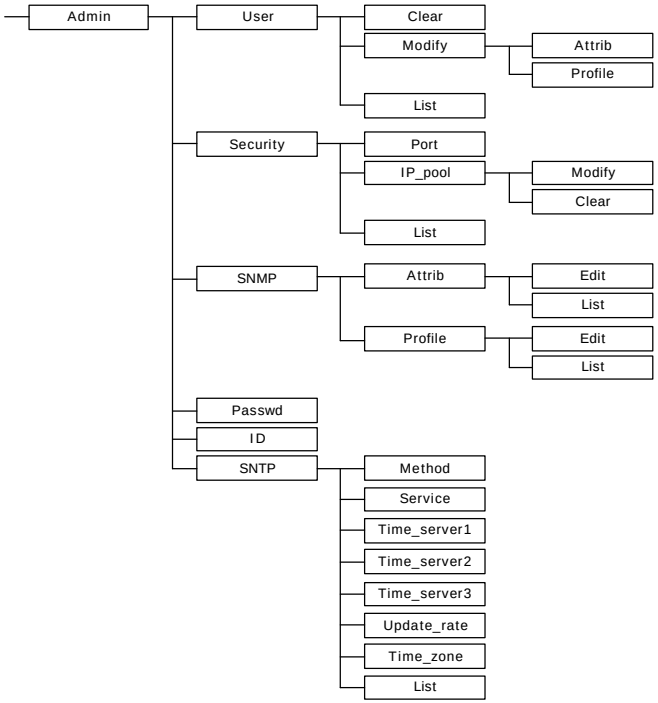
Menu Tree

All of the configuration commands that are placed in the subdirectories of Enable are protected by supervisor password.




Setup
Mode
SHDSL
Mode
n*64
Type
Clear
Margin
WAN
Protocol
Address
VPI_VCI
Encap
QoS
Class
PCR
ISP
List
Bridge
Gateway
Static
Add
MAC
LAN_Port
WAN1_Port
WAN8_Port
Delete
Modify
List
Route
Static
Add
Delete
List
RIP
Generic
LAN
Attrib
Version
Authetication
WAN
Attrib
Version
Authetication
List
LAN
Address
Attrib
IP-share
NAT
PAT
DMZ
<more...>
DHCP
Generic
Fixex
List
DHCP-proxy
Hostname
Default


Setup
Mode
SHDSL
<more...>
WAN
<more...>
Bridge
<more...>
Route
<more...>
LAN
<more...>
IP-share
NAT
Virtual
Range
Delete
List
Global
Range
Interface
Delete
List
Fixed
Modify
Interface
Delete
List
PAT
Clear
Modify
Interface
Port
Server
Protocol
Name
List
DMZ
Active
Begin
Address
End
DHCP
Generic
Active
Gateway
Netmask
IP_range
Lease_time
Name_server1
Name_server2
Name_server3
Fixex
Add
List
Delete
DHCP-proxy
Hostname
Default


Admin
User
Clear
Modify
Attrib
Profile
List
Security
Port
IP_pool
Modify
Clear
List
SNMP
Attrib
Edit
List
Profile
Edit
List
Passwd
ID
SNTP
Method
Service
Time_server1
Time_server2
Time_server3
Update_rate
Time_zone
List

This page was left blank intentionally.

Chapter 8. Configuration Commands

To setup the router, move the cursor " **>>**" to **enable** and press the enter key. When the screen appears, type the supervisor password. The default supervisor password is **root**. The password will be written on screen 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 system security, it is recommended to change the default user name and password after completing these settings. After changing the User Name and Password, it is strongly recommend you write the user name/password down and save it, since they will be required the next time you login to the Router.

For any changes to the configuration, you must write the new configuration to Flash and reboot the router to activate the new settings.
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 comm and
   admin           Setup management features
   utility         TFTP upgrade utility
   exit            Quit system
```

Chapter 8. Configuration Commands

Status

You can view the running system status of SHDSL, WAN, route and interface via the **status** command.

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

```
>> shdsl          Show SHDSL status
   wan            Show WAN interface status
   route          Show routing table
   interface      Show interface statistics status
```

Show

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

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

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

Write

For any changes to the configuration, you must write the new configuration to Flash using the **write** command and reboot the router to activate the configuration.

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

```
-------------------------------------------------------------------------
Command: write <CR>
Message: Please input the following inf ormation.

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

Reboot

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

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

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

Ping

Ping command will be used to test the connection of the router. Move the 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):  1~65534
Data size [1~1999]: 32
-------------------------------------------------------------------
```

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 of 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
```

User Profile

You can use the **user** command to clear, modify and list all the user profiles. You can setup up to five users to access the router via console port or Telnet in the 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 the **clear** command. If you do not know the user number, you can use the **list** command to check it. The **Modify** command is used to modify 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 modes, command line and menu mode, to setup the SHDTU03. We will not discuss the command line interface (CLI) in this manual.

Security

Security command can be used to configure ten legal IP address for Telnet access and port number.

Move the cursor " **>>** " to **security** and press enter. The default legal address is 0.0.0.0. which 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
```

SNMP

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

The router can generate SNMP traps to indicate alarm conditions, and it relies on the SNMP community strings to implement SNMP security. This router support MIB 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 numb er <1~5> : 2
------------------------------------------------------------------------
```

The screen will prompt as follows:

```
>> 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 follows:

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

Supervisor Password and ID

The supervisor password and ID are the last door for security but the most important. Users who access the router via web browser, console port or Telent have to use the ID and password to configure the router. It is strongly suggested to change the ID and password.

SNTP

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

There are two methods to synchronize time, synchronize with PC or SNTPv4. If you choose to synchronize with a PC, the router will synchronize with a PC. If you choose SNTPv4, the router will use the protocol to synchronize with an Internet time server.

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

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

To configure SNTP v4 time synchronization, follow the procedures below.
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 <Dis able|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 server 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.

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
```

Exit

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

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           Configure SHDSL 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 defau lt setting
```

Mode

The SHDTU03 can act in either routing mode or bridging mode. The default setting is routing mode. You can change the system operation mode by using the 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
```

SHDSL

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

```
>> mode            Configure SHDSL mode
   n*64            Configure SHDSL data rate
   type            Configure SHDSL annex type
   clear           Clear current CRC error  count
   margin          Configure SHDSL SNR margin
```

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

You can setup the data rate in multiples of 64Kbps where n is from 0 to 32. If you configure n as 0, the SHDTU03 will perform in adaptive mode.

There are two types of SHDSL Annex types, Annex-A and Annex-B.

Clear command can clear the CRC error count.

Generally, you do not need to change the SNR margin, whose range is from 0 to 10. The SNR margin is an index of line connection. You can see the actual SNR margin in STATUS SHDSL. The larger the SNR margin, the better the line connection. If you set SNR margin in the field as 2, the SHDSL 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.

WAN

The router supports 8 PVC, private virtual circuit, and so you can setup eight WANs; 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 idl e time
   ip_type         Configure IP type in PPPoA and PPPoE
   list            WAN interface configuration
```

There are four types of connection protocols, IPoA, EoA, PPPoA and PPPoE, which may or may not be supported by your ISP. For PPPoA and PPPoE, you do not need to setup any IP addresses and subnet masks. However, a valid username/password must be provided by your ISP for the PPP authentication.
There is a 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 methods; VC-Mux and LLC.

You can setup virtual circuit quality of service, VC QoS, using the qos command. There are two QoS classes; UBR and CBR. The peak cell rate can be configured from 64kbps to 2400kbps.

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

The ISP command can configure the account name, password and idle times. Idle times are from 0 minute to 300 minutes.
You can review the WAN interface configuration via the list command.

Bridge

You can setup the bridge parameters using the bridge command. If the product is configured as a router, you do not need to setup the bridge parameters. Move the cursor " **>>** " to **bridge** and press enter.

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

You can setup the default gateway IP via the 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 entering the add menu, the screen will prompt as follows

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

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.

The specification of VLAN function is as follow:

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 to.
9. If VID and source address look up fails, the source address will be learned.

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

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

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

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

802.11Q VLAN

Follow the steps to configure 802.11Q VLAN.

```
-------------------------------------------------------------------------
Command: setup vlan active <Disable|80 21Q|Port>
Message: Please input the following information.

Trigger 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 in the range 1~4095.

VLAN port status is a 5-digit binary number whose bit-1 location indicates the VLAN port membership in which 4MSBs and 1MSB 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 represents WAN. VID value is the group at which you want to assign the PVID of the port.

```
-------------------------------------------------------------------------
Command: setup vlan pvid <1~5> <1~4094>
Message: Please input the following information.

Port index <1~1>: 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 <1~4> <Access|Trunk>
Message: Please input the following information.

Port index <1~4>: 1
Port link type (Tab select) <Trunk >: Access

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

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

Route

You can setup the routing parameters using the route command. If the SHDTU03 is configured as a bridge, you do not need 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 routes 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 SHDTU03 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 follows:

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

You can add 20 sets of static route entries by using the **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 the **delete** command.
You can review the static route entries by using the **list** command.

To configure Routing Information Protocol (RIP), you can use the **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 paramete rs
   wan              Configure WAN interface RIP parameters
   list             Show RIP configuration
```

The **generic** command can be used to setup RIP mode and auto summary mode.
If there are any routers in your LAN, you can configure LAN interface RIP parameters via **lan** command.

The SHDTU03 supports 8 PVCs and you can configure the RIP parameters of each WAN via the **wan** command. Move the cursor " **>>** " to **wan** and press enter.

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

Active interface number <1~8>:  1

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

The screen will prompt as follows:

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

Attrib command can configure RIP mode, authentication type and Poison reverse mode.
Version command can configure RIP protocol version.
Authe command can configure the authentication code.
You can review the list of RIP parameters via the **list** command.

LAN

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

IP share

You can configure Network Address Translation (NAT), Port Address Translation (PAT) and Demilitarized Zone parameters in the **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 (private) network and the other is the outside (public) network. 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 ensures 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 allows the company to use a single IP address for its communication to 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.

NAT

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

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

The **virtual** menu contains a range of virtual IP 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 with the **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 the **delete** command.

You can view the virtual IP address range via the **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 of the global IP address range, You can bind the address pool to a specific interface via the **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 the **delete** command.
You can view the global IP address range via the **list** command.

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

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

You can create up to 10 fixed NAT mapping entries via the **range** command.

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

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

After configuration of fixed IP address entries, you can bind the entry to specific interface via the **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 entries- from 1 to 5- by using the **delete** command.

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

PAT

To configure Port Address Translation, move the cursor " **>>**" to the **pat** command 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 entries- from 1 to 10- by using the **clear** command.

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

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

Virtual server entry number <1~10>:  1

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

After keying 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 the **interface** command.
You can configure the global port number by using the **port** command.
The local server, host, IP address and port number are configured via the **server** command.
The authorized access protocol is setup via the **protocol** command.
The **Name** command can be used to configure the service name of the host server.
Begin and **end** commands are used to setup the local server schedule to access.
You can view the fixed NAT mapping entries via the **list** command.

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 the **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 defaul t) <1>: 1

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

DHCP

Dynamic Host Configuration Protocol (DHCP) is a communication protocol that allows network administrators the ability 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 the DHCP server, move the cursor to **dhcp** and press enter.

```
>> generic          Configure generic DHCP parameter s
   fixed            Configure fixed host IP address list
   list             Show DHCP configuration
```

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

```
>> active            Trigger DHCP function
   gateway           Default gateway for DHCP clie nt
   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
```

Activate the DHCP function with the **active** command.
Set the default gateway via the **gateway** command.
The subnet mask for DHCP client is configured by the **netmask** command.
The **Ip_range** command is used to configure the dynamic assigned IP address range.
The dynamic IP maximum lease time is configured by the **lease_time** command.
You can setup 3 domain name servers via the **name_server** command.
The Fixed Host IP Address list is setup via the **fixed** command.

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

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

DNS proxy

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

Host name

Enter the local host name via the 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

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

Default

If you want to restore to the 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
------------------------------------------------------- -------------
```

Transmission Units

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Building
(Neihu Technology Park)
8F, No. 60, ZhouZi St., Nei-Hu, Taipei, Taiwan
Phone:(886) 2.2659.1021 Fax:(886) 2.2799.1355
E-mail: info@ctcu.com http://www.ctcu.com