User Manual

G.SHDSL .bis Router

CTC UNION TECHNOLOGIES CO., LTD.

Table of Contents

This page is intentionally left blank.

1 Descriptions

CTC SHDTU04b Series 2/4-Wire SHDSL.bis EFM Bridges/Routers comply with the latest G.SHDSL.bis technology standards and supports symmetric data rate up to 15.3Mbps/Pair under TC-PAM 128. It provides a secure and symmetrical high-speed connectivity over existing copper-line infrastructure that is ideal for service providers as well as SOHO and SME users.

SHDTU04b supports back to back connectivity for long reach Ethernet extension. Users can make a direct connection between two SHDSL.bis routers by using a standard telephone cable, and configure one as CO and the other as CPE. The connection offers a cost effective solution for service providers and SME users who need high-speed dedicated network applications.

The SHDSL.bis EFM routers are integrated with high-end Bridging/Routing capabilities that support flexible traffic management policies and Quality of Service, enabling business-class Ethernet services with flexibility of mapping user traffic into Ethernet flows. The unit can be managed by different ports and applications including comprehensive command-line interface (CLI), Telnet, user-friendly GUI-based Web Browser Interface and SNMP.

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

1.1 Features

- ✓ Symmetrical high-speed Ethernet service with SHDSL.bis, backward compatible with SHDSL
- ✓ Support both EFM mode and ATM mode(1 PVC)
- ✓ Support point to point connectivity
- ✓ Support dying gasp

1.2 Specification

WAN Interface

- SHDSL.bis: ITU-T G.991.2 (2004) Annex A/B/F/G supported
- Support EFM Bonding and SHDSL M-Pair mode
- Encoding scheme: TC-PAM 16/32/64/128
- Data Rate:

N x 64 Kpbs (N=3~89) using TC-PAM 16/32
Max. 5.696Mbps (1-Pair)
Max. 11.392Mbps (2-Pair)

N x 64 Kbps (N=3~239) using TC-PAM 64/128
Max. 15.296 Mbps (1-Pair)
Max. 30.592 Mbps (2-Pair)

Impedance: 135 ohms.
Compliant with IEEE 802.3ah

LAN Interface

- 4-Ports 10/100M Switch, Auto-negotiation for 10/100Base-TX and Half/Full Duplex, Auto-MDIX Supported.

Bridging

- Up to 1024 MAC address learning bridge
- IEEE 802.1D transparent learning bridge
- IEEE 802.1Q/1P VLAN Port-based/Tagging
- QoS Class-based (Prioritization/Traffic/DSCP Mark), Rate Limiting, Up to 8 priority queues

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)
- DHCP server, client and relay (RFC2131/2132)
- DNS relay/proxy and caching (RFC1034/1035)
- Dynamic DNS
- IP precedence (RFC 791)

ATM

- Multiple Protocols over AAL5
- Ethernet over ATM (RFC 2684/1483)
- 1 PVC

EFM

- EFM mode compliant to IEEE 802.3,
- PPP over Ethernet (RFC2516)
- Support of OAMPDU information and functionality (ITU-T Y.1731)
- OAMPDU Event Notification, Variable Request, Variable Response, Loopback Control

- VLAN base QOS (802.1P/Q), Priority Queue

Network Protocol

- VoIP(SIP) pass-through
- IPv4 (ARP/RARP, TCP/UDCP, ICMP)
- SNTP (Time Zone/ Daylight Savings)

Security

- Natural NAT/PAT firewall
- DMZ host
- Virtual server mapping (RFC1631)
- Advanced stateful packet inspection (SPI) firewall Denial of Service (DoS)
- Application level gateway for URL and keyword blocking (Content Filter)
- Access Control List (ACL)
- Support PAP/CHAP/MS-CHAP client

Management

- Web-based GUI for quick setup, configuration and management
- Command-line interface (CLI) for local console and Telnet/SSH access
- Password protected management and access control list for administration
- Remote management via WWW/SSH/Telnet local/remote
- Real-time system log logging
- SNMP SNMPv1/SNMPv2 (RFC 1157/1901/1905) and MIB-II (RFC 1213/1493)
- Software upgrade via Web-browser/CLI, supported TFTP/FTP
- Dying Gasp

Diagnostics/Monitoring

- Routing Table
- Packet Statistics

Hardware Interface

- WAN: RJ-45 x 1
- LAN: RJ-45 x 4
- Console Port: RS232 female
- Reset Button: Load factory default
- Power Jack

Indicators

- System: PWR, ALM
- WAN 1~4: LNK/ACT
- LAN 1~4: LINK/ACT

Physical / Electrical

- Dimensions: 18.7 x 3.3 x 14.5cm (WxHxD)
- Power: 100~240VAC (via power adapter)
- Power Consumption: 9 watts Max
- Operating Temperature: 0~45°C
- Storage Temperature: -20°C~70°C

- Humidity: 0%~95%RH (non-condensing)

Memory

- 128MB Flash Memory, 64MB DDR2 DRAM

Regulatory

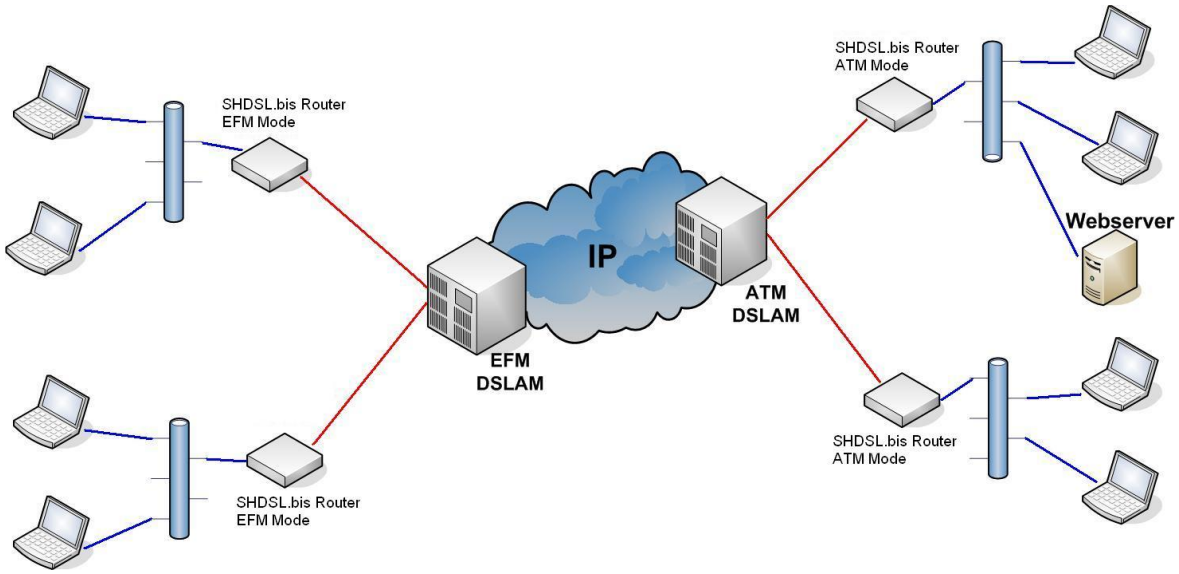
- CE
- FCC Part 15 Class A
- VCCI
- EN60950

*__CTC reserves the right to change specifications without prior notice.__

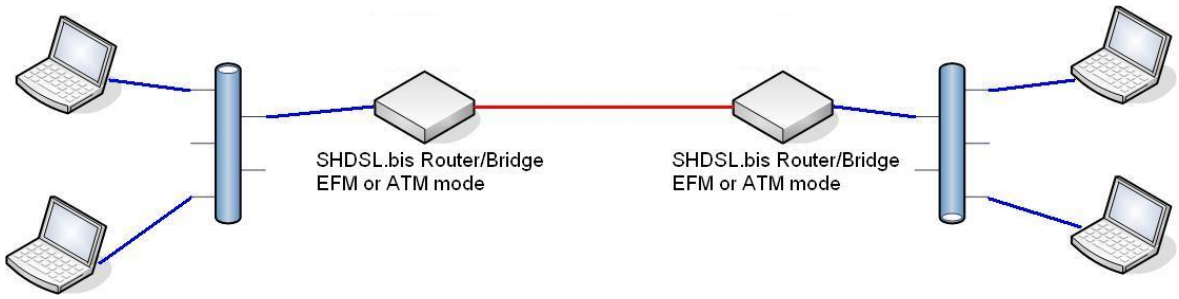
Order Information

SHDTU04bF-ET10RS	2-Wire G.SHDSL.bis EFM Router with 4 LAN Port
SHDTU04bFA-ET10RS	4-Wire G.SHDSL.bis EFM Router with 4 LAN Ports

1.3 Applications



Combination with EFM or ATM DSLAM



Point-to-point connection

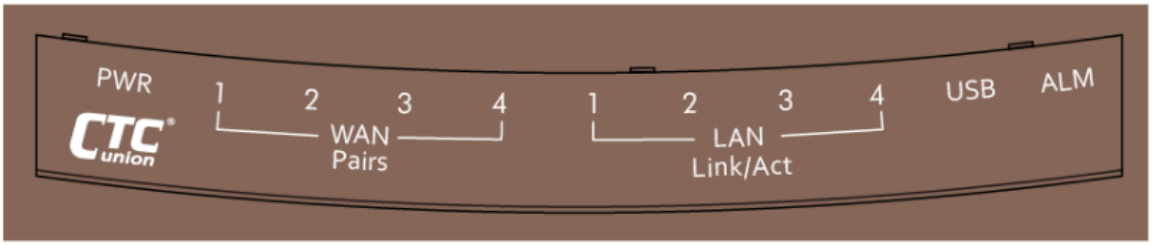
.

2 Getting to know about the router

This chapter introduces the main features of the router.

2.1 Front Panel

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

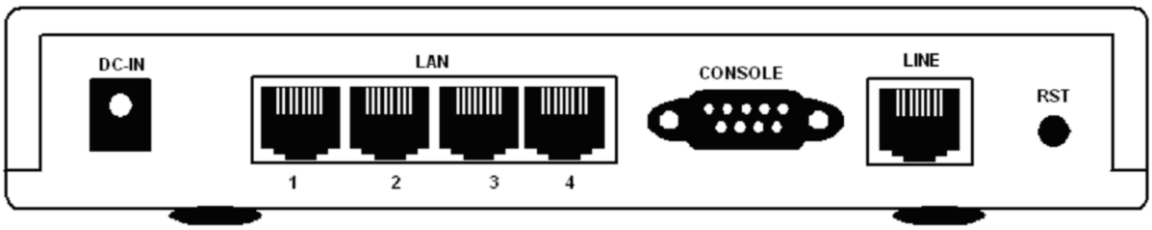


LED status of SHDSL.bis Router

LEDs		Active	Description
PWR		On	The power adaptor is connected to this device
DSL	LINK 1	On	SHDSL.bis line 1 connection is established
		Blink	SHDSL.bis line 1 handshake Transmit or received data over SHDSL.bis link 1
	LINK 2	On	SHDSL.bis line 2 connection is established
		Blink	SHDSL.bis line 2 handshake Transmit or received data over SHDSL.bis link 2
	LINK 3	On	SHDSL.bis line 3 connection is established
		Blink	SHDSL.bis line 3 handshake Transmit or received data over SHDSL.bis link 3
	LINK 4	On	SHDSL.bis line 4 connection is established
		Blink	SHDSL.bis line 4 handshake Transmit or received data over SHDSL.bis link 4
LAN	LINK/ACT1	On	Ethernet cable is connected to LAN 1
		Blink	Transmit or received data over LAN 1
	LINK/ACT2	On	Ethernet cable is connected to LAN 2
		Blink	Transmit or received data over LAN 2
	LINK/ACT3	On	Ethernet cable is connected to LAN 3
		Blink	Transmit or received data over LAN 3
	LINK/ACT4	On	Ethernet cable is connected to LAN 4
		Blink	Transmit or received data over LAN 4
ALM		On	SHDSL.bis line connection is dropped
		Blink	SHDSL.bis self-test
		Off	No Alarm

2.2 Rear Panel

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



Connectors Description of SHDSL.bis Router

DC-IN	Power adaptor inlet: Input voltage 12VDC
LAN (1,2,3,4)	Four Ethernet10/100BaseT auto-sensing and auto-MDI/MDIX for LAN ports (RJ-45)
CONSOLE	RS- 232C (DB9) for system configuration and maintenance
LINE	SHDSL.bis interface for WAN port (RJ-45)
RST	Reset button for reboot or load factory default

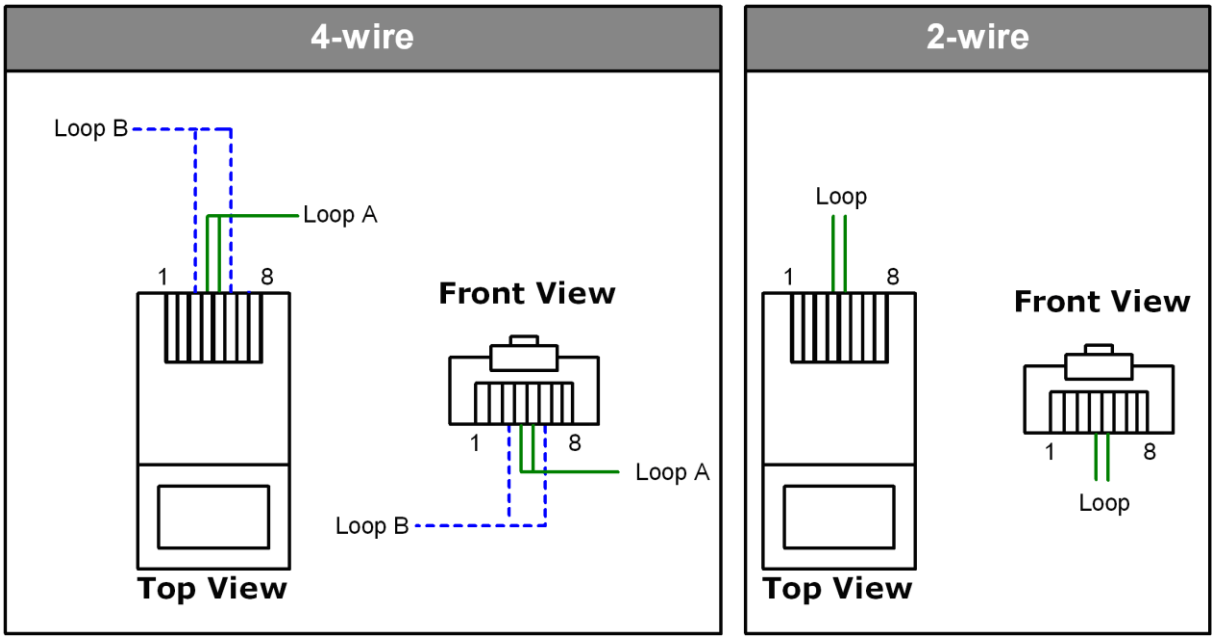
The reset button can be used only in one of two ways.

(1) Press the Reset Button for 1 second to make the system reboot.

(2) Pressing the Reset Button for 4 seconds will make the system load the factory default settings and lose your existing configuration. When you want to change its configuration but forget the user name or password, or if the product is having problems connecting to the Internet and you want to configure it again by clearing all configurations, press the Reset Button for 4 seconds with a paper clip or sharp pencil.

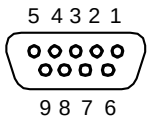
2.3 SHDSL.bis Line Connector

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



2.4 Console Cable

Below figure show the cosole cable pins asignment:

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

3 Install the Router

This chapter will guide you to install the SHDSL.bis Router via Web Configuration and Serial Console. Please follow the instructions carefully.

Note: There are three methods to configure the router: Serial console, Telnet or Web Browser. Only one configuration method is used to setup the Router at any given time. Users have to choose one method to configure it.

For Web configuration, you can skip item 3.
For Serial Console Configuration, you can skip item 1 and 2.

3.1 Check List

(1) Check the Ethernet Adapter in PC or NB

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

(2) Check the supported Web Browser in PC or NB

In order to set up the routeter by Web Configuration, your PC or notebook computer needs to install the supported web browser

(3) Check the Terminal Access Program

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

(4) Determine Connection Setting

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

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

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

Bridge EoA

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

Route EoA

VPI:_
VCI:__
Encapsulation:
IP Address:
Subnet Mask:
Gateway:
DNS Server:_

IPoA

VPI:_
VCI:__
Encapsulation:
IP Address:
Subnet Mask:
Gateway:
DNS Server:_

PPPoA

VPI:_
VCI:__
Encapsulation:
User Name:
Password:
DNS Server:_
Host Name: (if applicable)

PPPoE

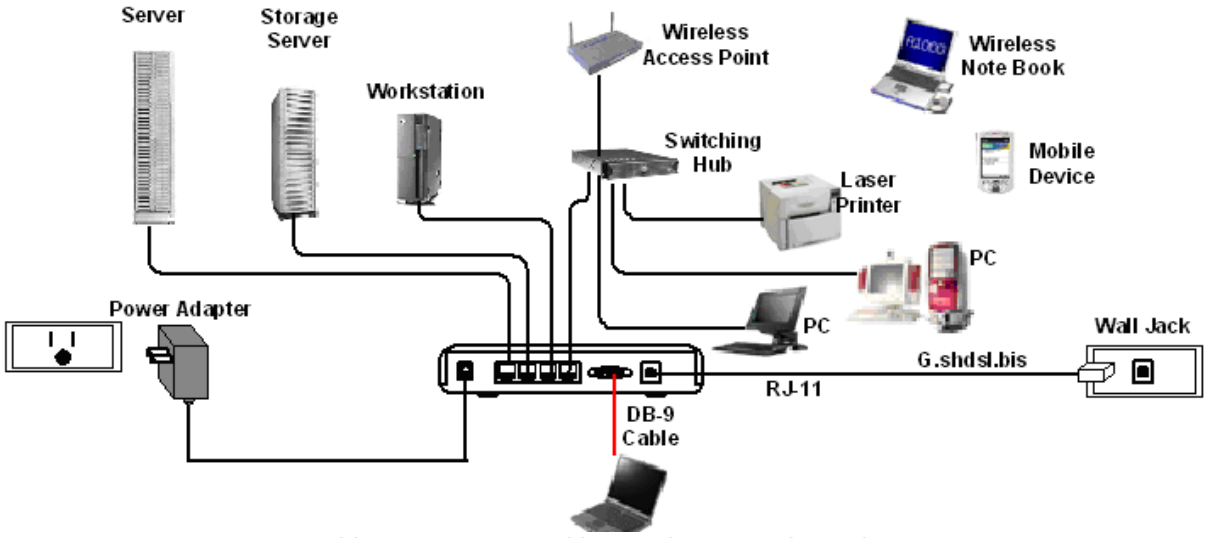
VPI:_
VCI:__
Encapsulation:
User Name:
Password:
DNS Server:_
Host Name:(if applicable)

3.2 Install the SHDSL.bis Router

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

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

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



SHDSL.bis 4-ports router with complex network topology

4 Configuration via Web Browser

OVERVIEW

The web configuration is an HTML-based management interface for quick and easy set up of the SHDSL.bis Routers by using an Internet browser.

After properly connecting the hardware of SHDSL.bis router as previously explained. Launch your web browser and enter http://192.168.1.1

The default IP address and sub net-mask of the Router are 192.168.1.1 and 255.255.255.0. Because the router acts as DHCP server in your network, the router will automatically assign IP address for PC or NB in the network.

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

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

Function Listing

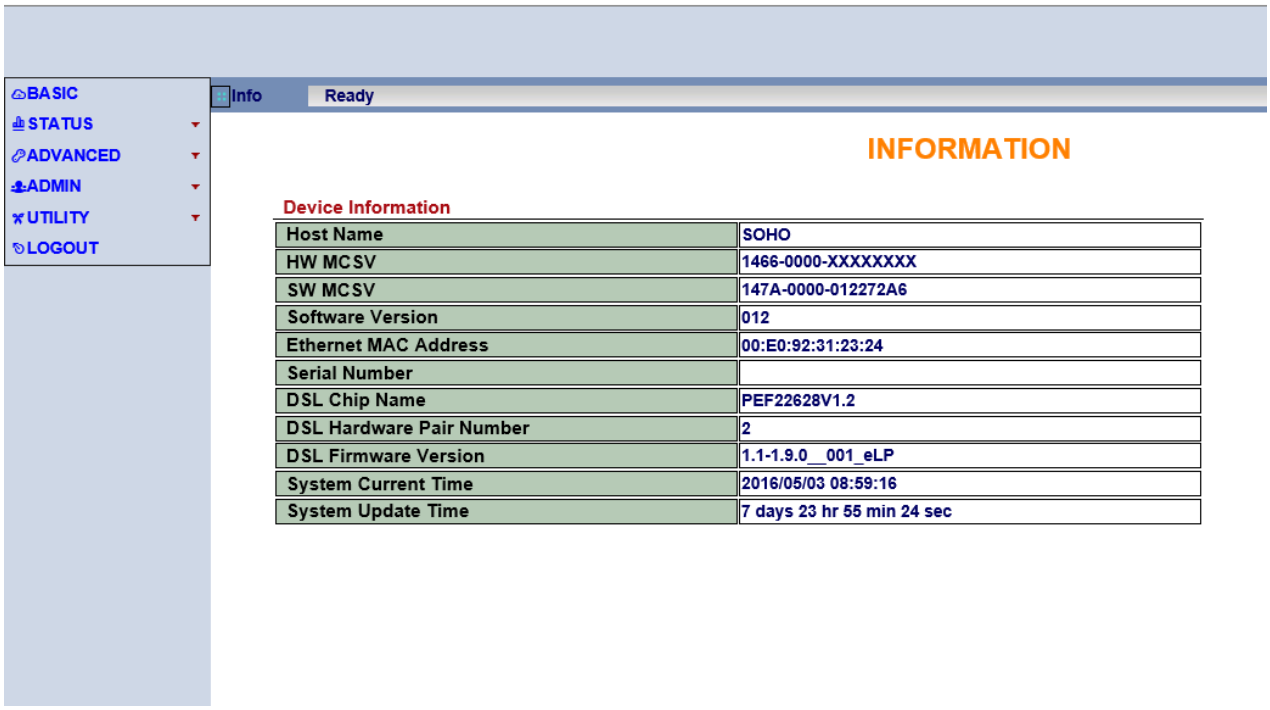
Below is the full function list of G.SHDSL.bis router

- **BASIC**
- **STATUS**
  - Information
  - Networking
  - Packet Statistics
  - G.SHDSL
- **ADVANCED**
  - SHDSL.bis
  - WAN
  - LAN
  - DNS
  - DHCP
  - VLAN
  - QoS
  - RIP
  - NAT/DMZ
  - Virtual Server
  - DDNS
  - Firewall
  - Content Filter
  - IGMP
  - SNTP
- **ADMIN**
  - SECURITY
  - MGMT
- **UTILITY**
  - SYSTEM LOG
  - SYSTEM TOOL
  - UPGRADE
  - RESTART
- **LOGOUT**

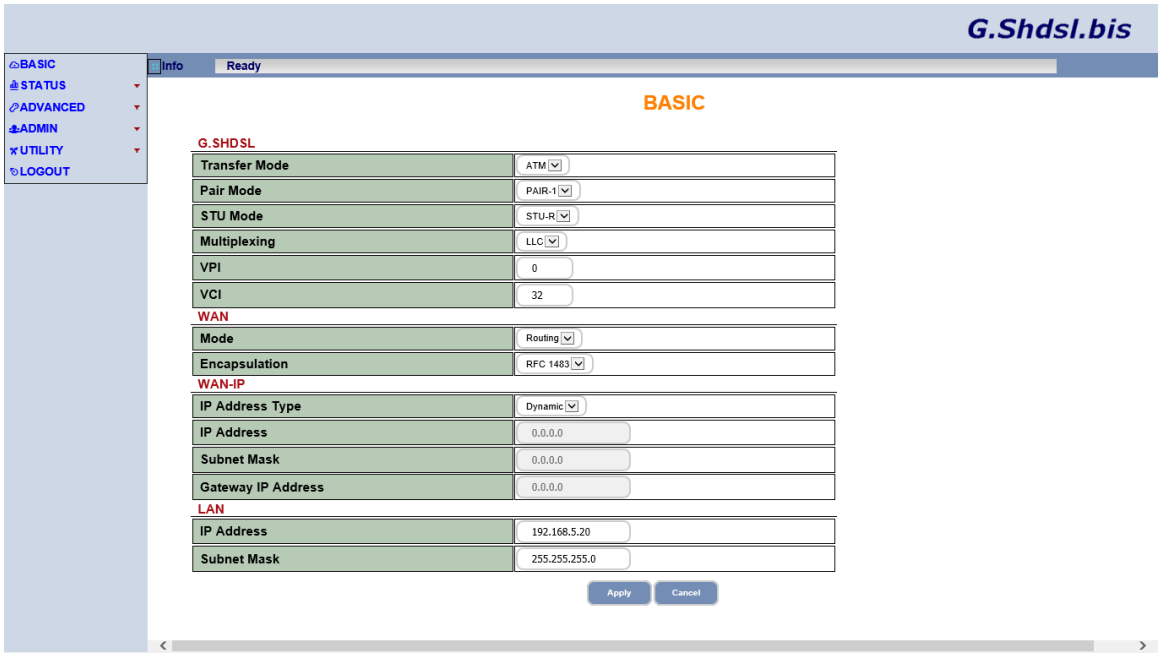
4.1 Basic Setup

OVERVIEW

Basic setup includes Bridge and Routing operation modes. User can use it to setup the SHDSL.bis router quickly. After completing it successfully, you can access Internet or use a pair of SHDSL.bis Routers as LAN extenders. This is the easiest and quickest way to setup the router.



Click BASIC for basic installation.



G.SHDSL

Item	Description
Transfer Mode	Click on the drop-down list and select Transfer Mode as ATM(Asynchronous Transfer Mode) or PTM(Packet Transfer Mode). ATM uses asynchronous time-division multiplexing, and encodes data into small, fixed-sized packets called cells. SHDSL interfaces support Packet Transfer Mode (PTM). In PTM, packets (IP, PPP, Ethernet, MPLS, and so on) are transported over DSL links as an alternative to using Asynchronous Transfer Mode (ATM). PTM is based on the Ethernet in the First Mile (EFM) IEEE 802.3ah standard.
Pair Mode	Click on the drop-down list and select Pair Mode as Pair-1, Pair-2 or Pair-4. Pair-1 for 2-Wire SHDSL.bis Router Pair-2 for 4-Wire SHDSL.bis Router
STU Mode	Click on the drop-down list and select STU Mode as STU-C or STU-R STU-C means the terminal of central office and STU-R means customer premise equipment. For point to point application, STU-C is the server/master unit while STU-R is the client/slave unit.
Multiplexing	Click on the drop-down list and select Multiplexing used by your ISP as VC or LLC. VC-mux (VC-based Multiplexing): Each protocol is assigned to a specific virtual circuit. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical. LLC (LLC-based Multiplexing): One VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol. *This is available only when you select ATM as Transfer Mode.
VPI	Enter the VPI(Virtual Path Identifier) range from 0 to 255. *This is available only when you select ATM as Transfer Mode.
VCI	Enter the VCI(Virtual Channel Identifier) range from 32 to 65535. *This is available only when you select ATM as Transfer Mode.

WAN

Item	Description
Mode	Click on the drop-down list and select Mode as Routing or Bridge Choose Routing if your ISP provides you with only one IP address and you need several computers to use the same Internet account. Choose Bridge when your ISP provides you with more than one IP address and you need several computers to get individual IP address from your ISP's DHCP server. When Bridge is selected, NAT, DHCP server and Firewall become unavailable.
Encapsulation	Click on the drop-down list and select Encapsulation used by your ISP as PPPoE or RFC1483

WAN-IP

Item	Description
IP Address Type	Click on the drop-down list and select IP Address Type as Static or Dynamic A static IP address is a fixed IP provided by your ISP. A dynamic IP address is different every time when you connect to the Internet.
IP Address	Enter IP address for WAN when select Static IP address Type.
Submask	Enter a subnet mask in dotted decimal notation when select Static IP address Type.
Gateway IP Address	Enter a gateway IP address provided by your ISP when select Static IP address Type.

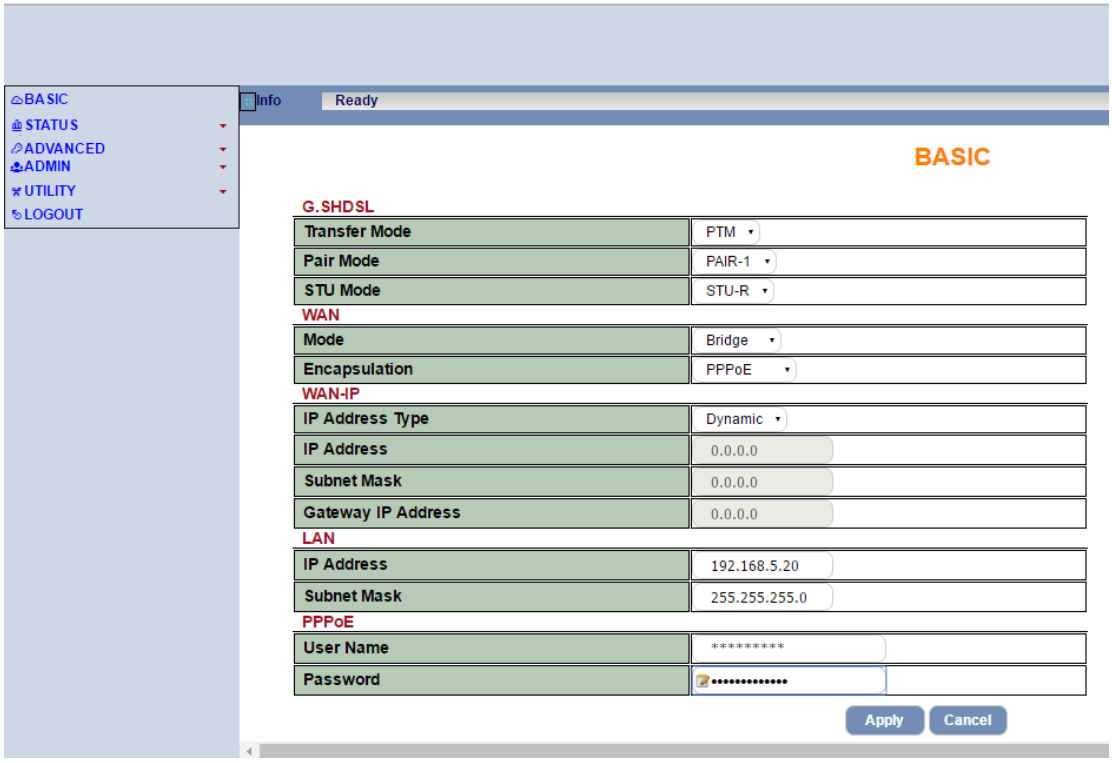
LAN

Item	Description
IP Address	Enter IP address for LAN
Subnet Mask	Enter a subnet mask in dotted decimal notation when select Static IP address Type.

When select PPPoE as Encapsulation, you are required to enter the User Name and Password provided by your ISP.

PPPoE

Item	Description
User Name	Enter User Name provided by the ISP for PPPoE
Password	Enter Password provided by the ISP for PPPoE

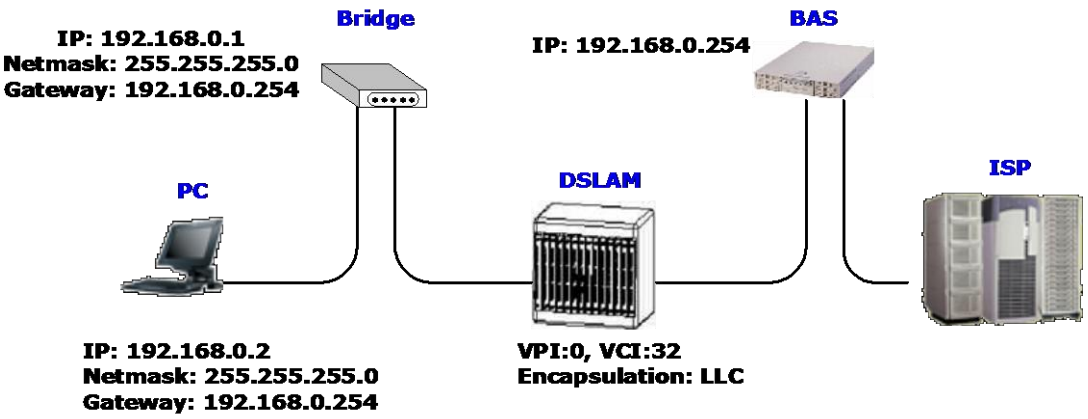


Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.1.1 Reference diagram

Bridge mode

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

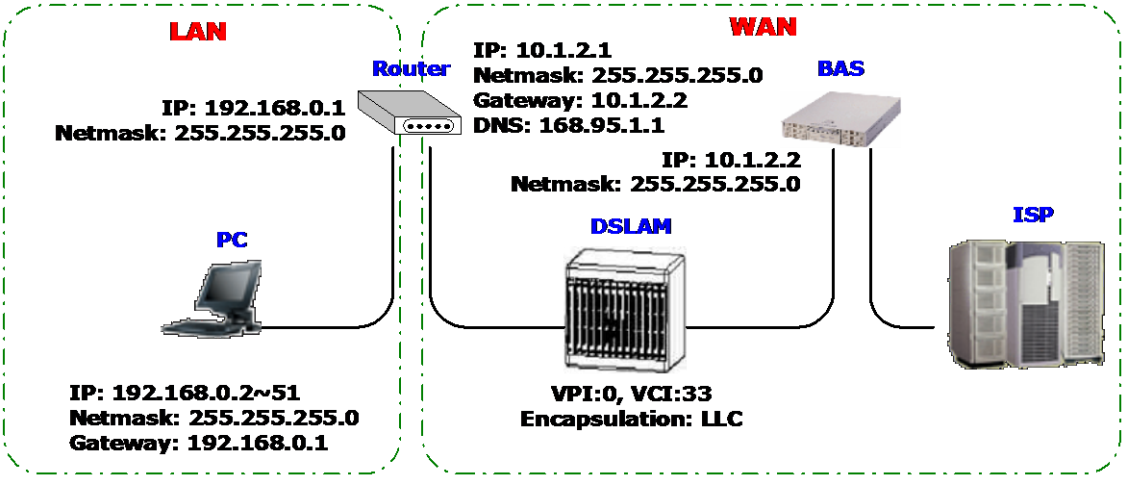


IPoA or EoA

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

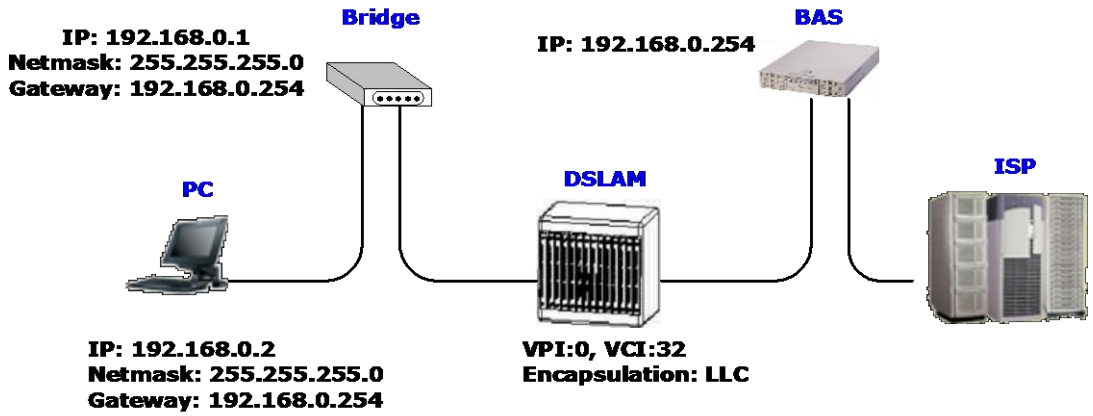
EoA (Ethernet-over-ATM) protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EoA protocol for data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

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



PPPoE or PPPoA

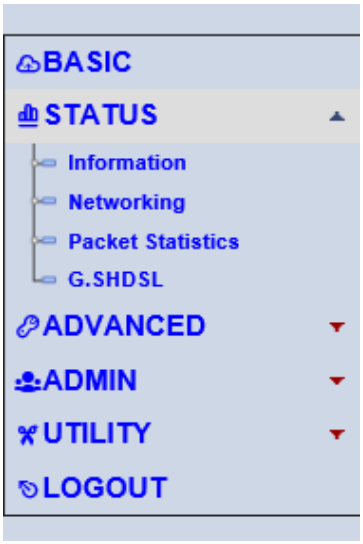
PPPoA (point-to-point protocol over ATM) and PPPoE (point-to-point protocol over Ethernet) are authentication and connection protocols used by many service providers for broadband Internet access. These are specifications for connecting multiple computer users on an Ethernet local area network to a remote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



4.2 STATUS

OVERVIEW

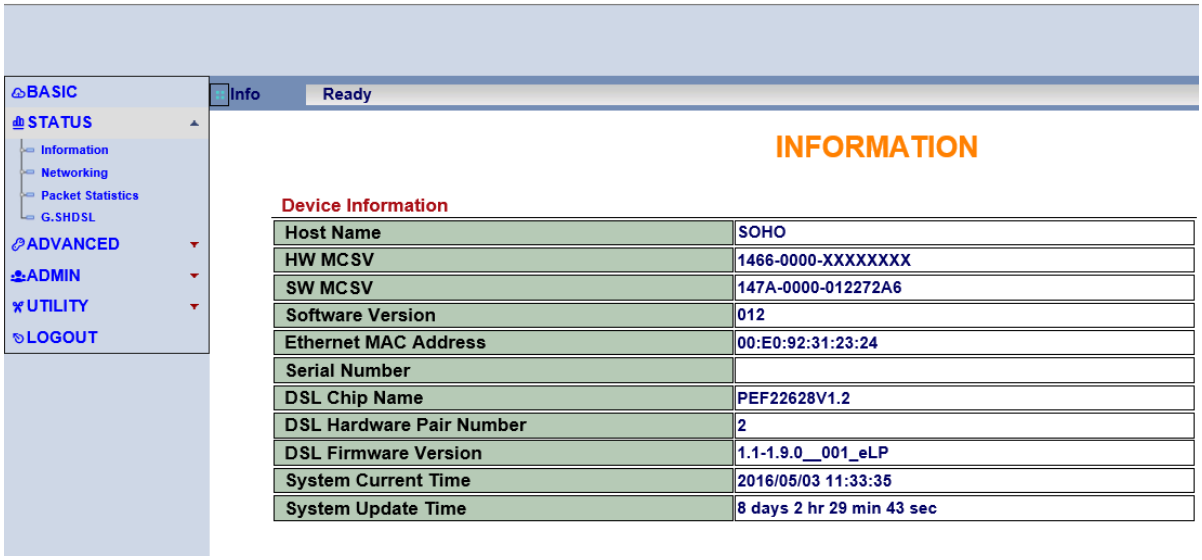
STATUS allows you to monitor the current status of the SHDSL.bis Router including basic software and hardware information, networking status, detailed packet statistics and G.SHDSL(WAN) status.



Information	Basic Device Information including Host Name, HW MCSV, SW MCSV, Software Version, MAC Address, Serial Number, DSL Chip information, System Time and System Update Time.
Networking	Current status of Network, DSL and Route Table.
Packet Statistics	System Status and Packet statistics for WAN port and LAN port.
G.SHDSL	Mode, Line rate and Performance information including SNR margin, atteunation and CRC error count.

4.2.1 Information

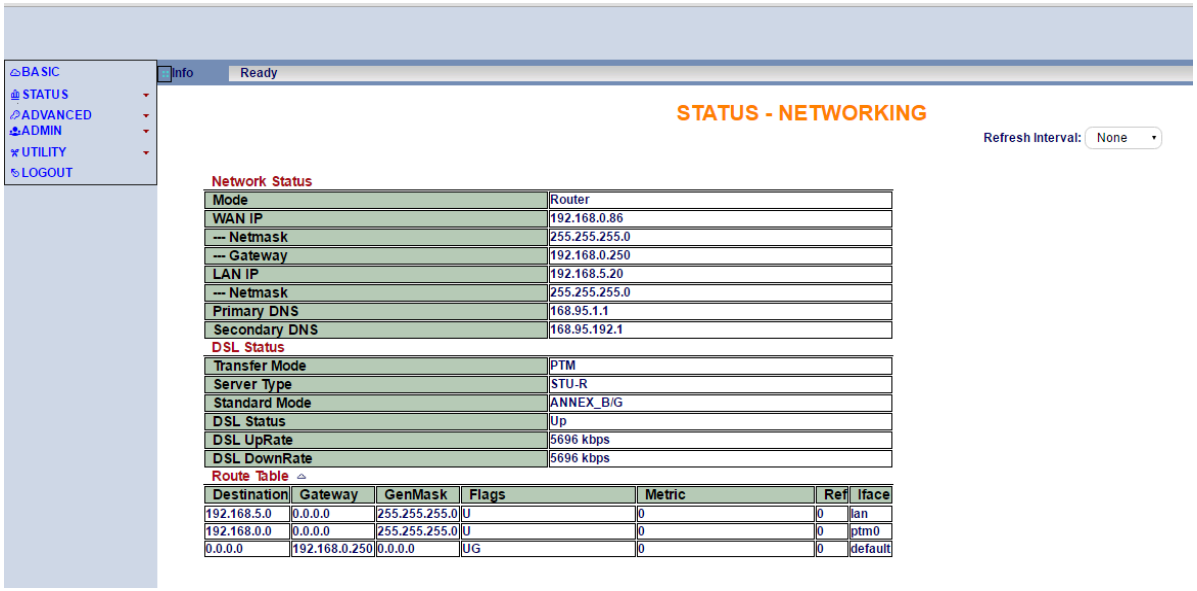
STATUS > Information



INFORMATION page displays basic device information including Host Name, HW MCSV, SW MCSV, Software Version, Ethernet MAC Address, Serial Number, DSL Chip Name, DSL Hardware Pair Number, DSL Firmware Version, System Current Time and System Update Time.

4.2.2 NETWORKING

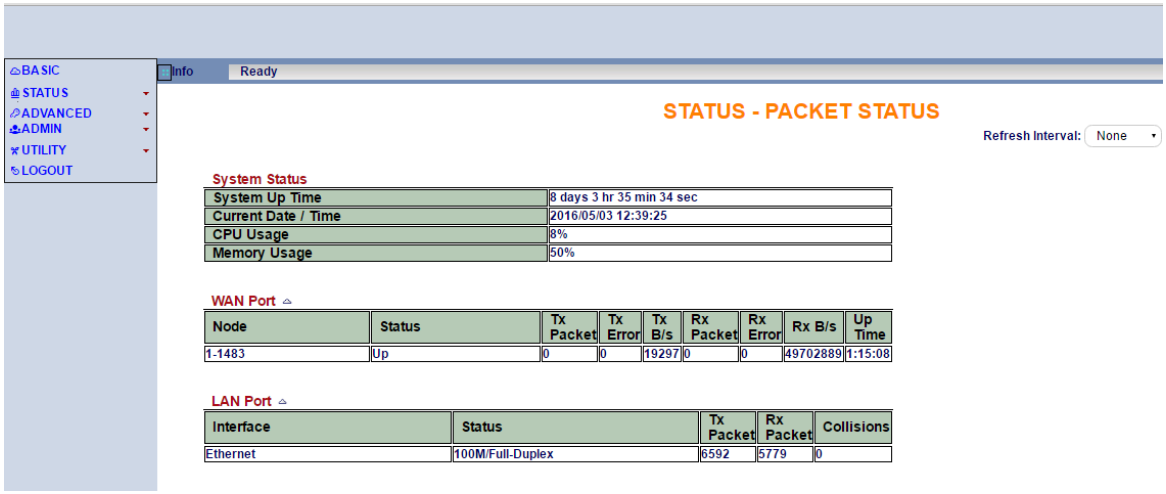
STATUS > Networking



NETWORKING STATUS page displays Network Status, DSL Status and Route Table information

4.2.3 PACKET STATISTICS

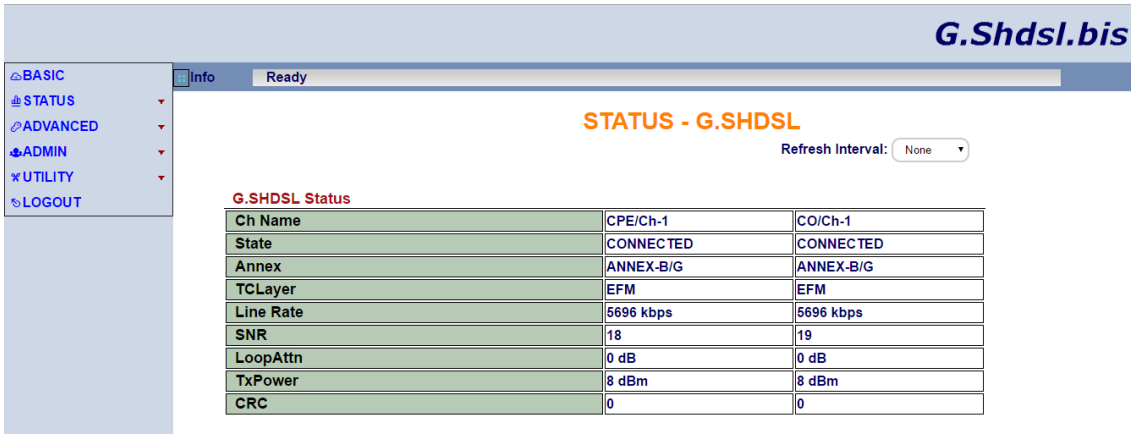
STATUS > Packet Statistics



PACKET STATUS page displays System Status and packet statistics for WAN port and LAN port.

4.2.4 G.SHDSL

STATUS > G.SHDSL



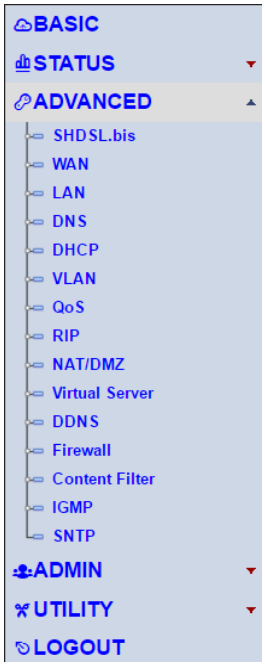
G.SHDSL STATUS page displays current status of DSL line including Channel Name, State, Annex, TCLayer, Line Rate, SNR, Loop Attenuation, TxPower and CRC.

4.3 Advanced Setup

OVERVIEW

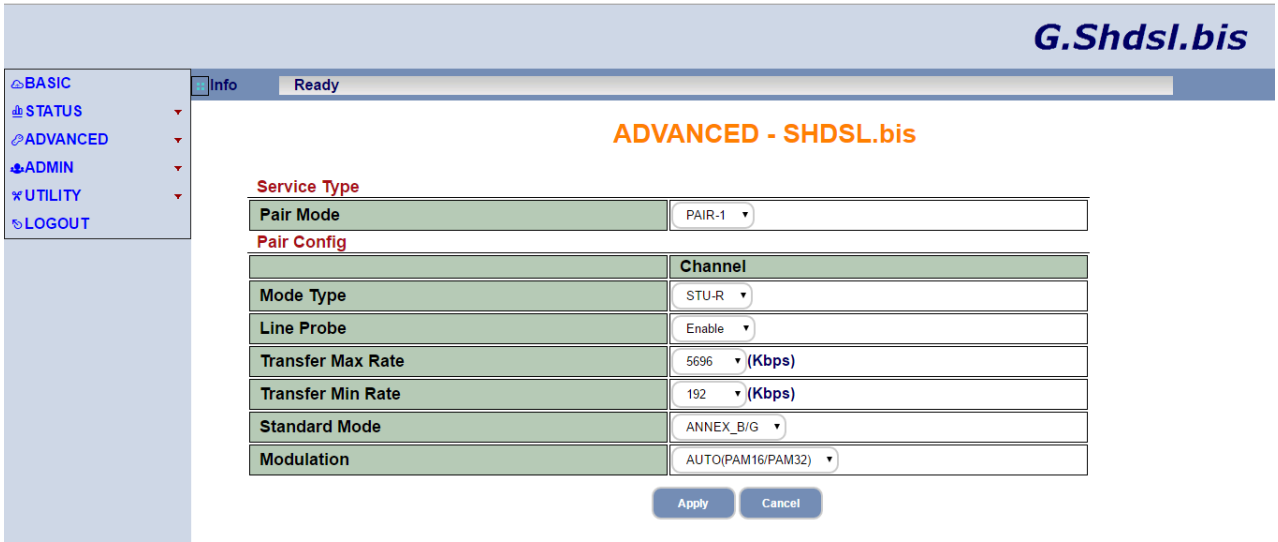
Advanced setup includes SHDSL.bis, WAN, LAN, DNS, DHCP, VLAN, QoS, RIP, NAT/DMZ, Virtural Server, DDNS, Firewall, Content Filter, IGMP and SNTP.

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



4.3.1 SHDSL.bis

ADVANCED>SHDSL.bis



Service Type

Item	Description
Pair Mode	Click on the drop-down list and select Pair Mode as Pair-1, Pair-2 or Pair-4. Pair-1 for 2-Wire SHDSL.bis Router Pair-2 for 4-Wire SHDSL.bis Router

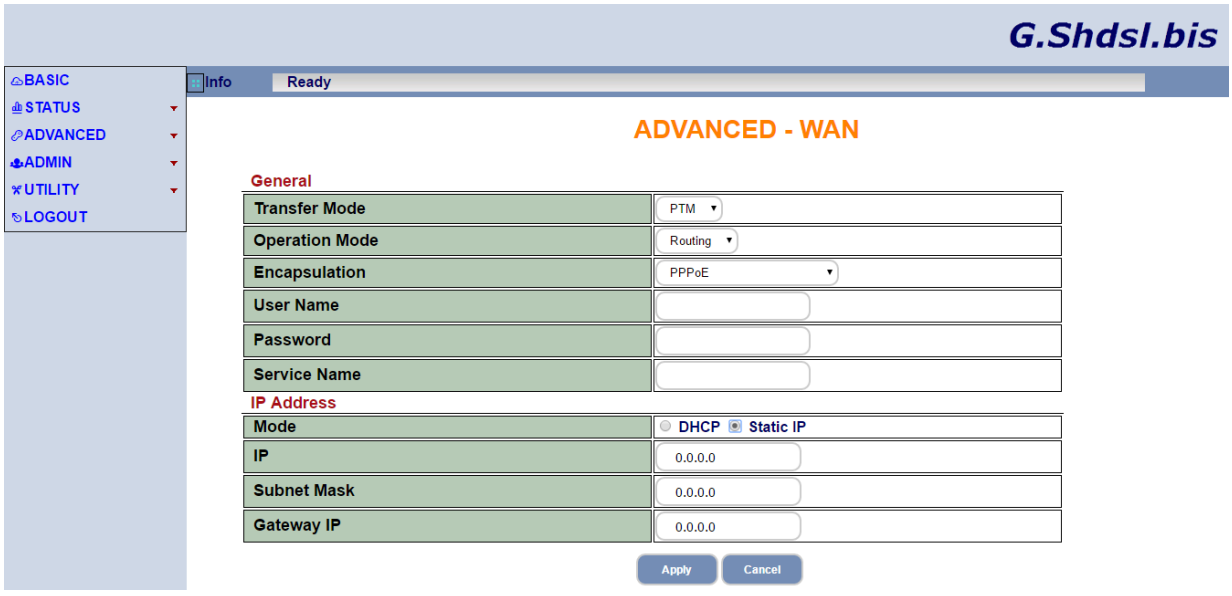
Pair Config

Item	Description
Mode Type	Click on the drop-down list and select STU Mode as STU-C or STU-R STU-C means the terminal of central office and STU-R means customer premise equipment. For point to point application, STU-C is the server/master unit while STU-R is the client/slave unit.
Line Probe	Click on the drop-down list and select Enable to enable Line Probe or Disable to diable Line Probe. For adaptive mode, you have to Enable Line Probe function. The router will adapt the data rate automatically according to the line status.
Transfer Max Rate	Select the maximum rate for sending and receiving data.
Transfer Min Rate	Select the minimum rate for sending and receiving data.
Standard Mode	There are four Annex types: Annex A (ANSI), Annex B (ETSI), Annex AF and Annex BG . Select the Standard Mode supported by your ISP. For point to point applications, you may choose one of the four types according to which line rate you need.
Modulation	Select the modulation supported by your ISP.

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.2 WAN

ADVANCED>WAN



General

Item	Description
Transfer Mode	Click on the drop-down list and select Transfer Mode as ATM(Asynchronous Transfer Mode) or PTM(Packet Transfer Mode). ATM uses asynchronous time-division multiplexing, and encodes data into small, fixed-sized packets called cells. SHDSL interfaces support Packet Transfer Mode (PTM). In PTM, packets (IP, PPP, Ethernet, MPLS, and so on) are transported over DSL links as an alternative to using Asynchronous Transfer Mode (ATM). PTM is based on the Ethernet in the First Mile (EFM) IEEE 802.3ah standard.
Operation Mode	Click on the drop-down list and select Operation Mode as Routing or Bridge Choose Routing if your ISP provides you with only one IP address and you need several computers to use the same Internet account. Choose Bridge when your ISP provides you with more than one IP address and you need several computers to get individual IP address from your ISP's DHCP server. When Bridge is selected, NAT, DHCP server and Firewall become unavailable.
Encapsulation	Click on the drop-down list and select Encapsulation used by your ISP as PPPoE or RFC1483 When select PPPoE as Encapsulation, you are required to enter the User Name and Password provided by your ISP.
User Name	Enter User Name provided by the ISP for PPPoE
Password	Enter Password provided by the ISP for PPPoE
Service Name	Enter Service name for PPPoE

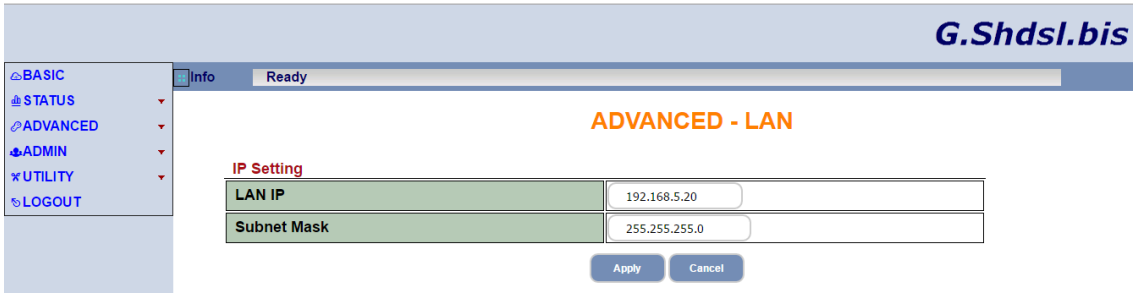
IP Address

Item	Description
IP Address Type	Click on the drop-down list and select WAN IP Address Type as Static or Dynamic A static IP address is a fixed IP provided by your ISP. A dynamic IP address is different every time when you connect to the Internet.
IP Address	Enter IP address for WAN when select Static IP address Type.
Submask	Enter a subnet mask in dotted decimal notation when select Static IP address Type.
Gateway IP Address	Enter a gateway IP address provided by your ISP when select Static IP address Type.

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.3 LAN

ADVANCED>LAN



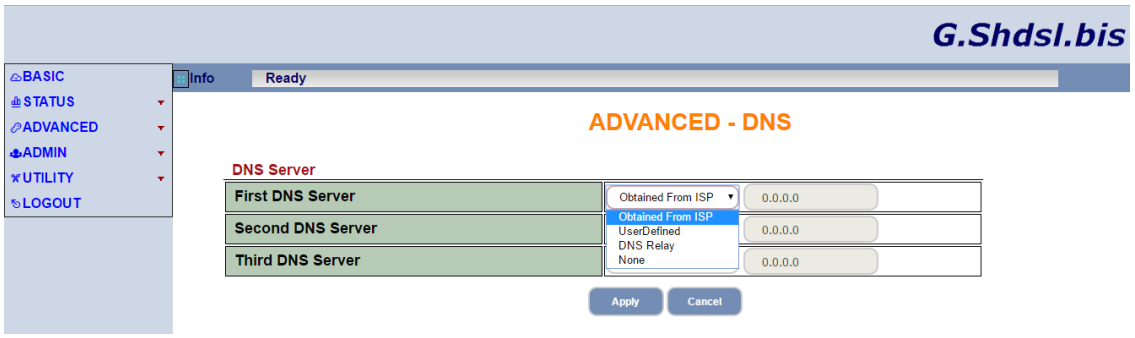
IP Setting

Item	Description
LAN IP	Enter IP address for LAN
Subnet Mask	Enter a subnet mask in dotted decimal notation when select Static IP address Type.

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.4 DNS

ADVANCED>DNS



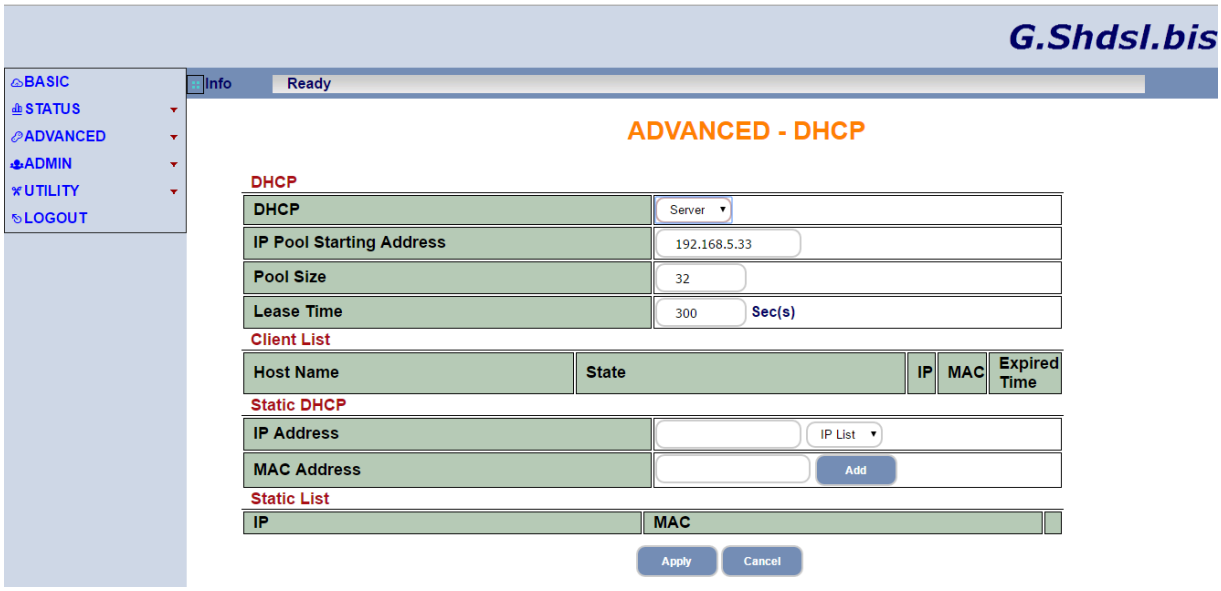
DNS Server

Item	Description
First DNS Server	Click on the drop-down list and select below options for DNS Servers; **Obtained From ISP**: Select this option when your ISP dynamically assigns the DNS server information. **User Defined**: Select this option when you have the IP address of a DNS server. **DNS Relay**: Select this option when your ISP uses IPCP DNS server extensions and the SHDSL.bis Router acts as DNS proxy. **None**: Select this option when you don't want to configure DNS servers.
Second DNS Server	
Third DNS Server	

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.5 DHCP

ADVANCED>DHCP



DHCP

Item	Description
DHCP	Click on the drop-down list and select below options for DHCP; **None**: Select this option to disable DHCP server. **Server**: Select this option when the router can assign IP addresses. Then enter the fields for IP Pool Starting Address, Pool Size and Lease Time. **Relay**: Select this option the router will relay DHCP requests and responses between the remote server and the clients. Then enter the field for Remote DHCP Server.
IP Pool Starting Address	Enter the 1st address in the IP address pool. *This field is required only when you enable DHCP server.
Pool Size	Enter the size of IP address pool. *This field is required only when you enable DHCP server.
Lease Time	Enter the lease time for IP addresses. *This field is required only when you enable DHCP server.

Client List

The table displays the list and status of clients with their Host Name, State, IP address, MAC and Expired Time.

Static DHCP

Item	Description
IP Address	Enter IP address to change the static DHCP setting
MAC Address	Enter the MAC address of the Ethernet device.

Static List

The table displays IP addresses and MAC added to the Static DHCP list.

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.6 VLAN

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

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

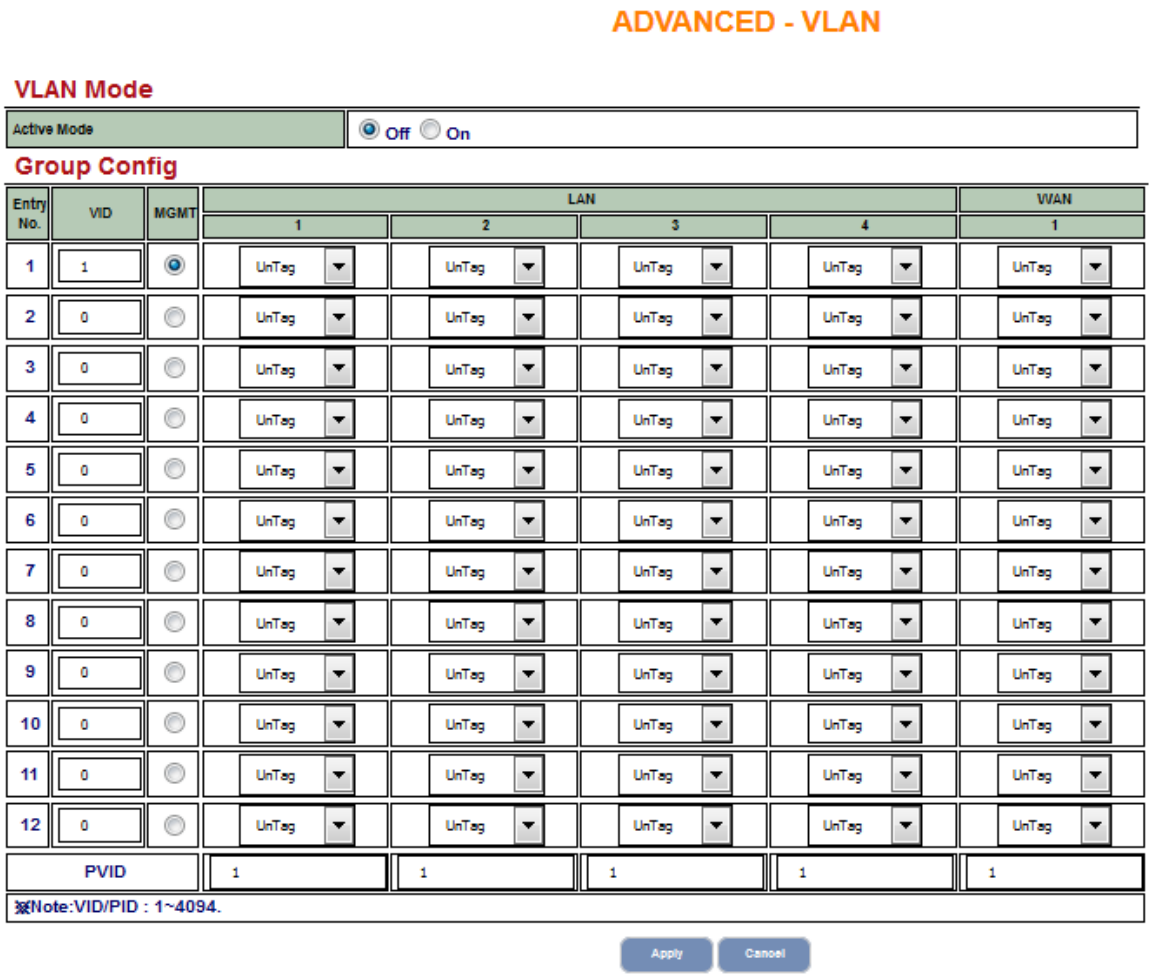
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

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

The router supports two types of VLAN: **802.1Q Tag-Based VLAN** and **Port-Based VLAN**.

VID: (Virtual LAN ID) It is an definite number of ID range from 1 to 4094.
PVID: (Port VID) It is an untagged member from 1 to 4094 of default VLAN.

ADVANCED>VLAN



VLAN Mode

Item	Description
Active Mode	Active 802.1Q VLAN function On: Enable VLAN Configure Off: Disable VLAN Configure

Group Config (Summary Table)

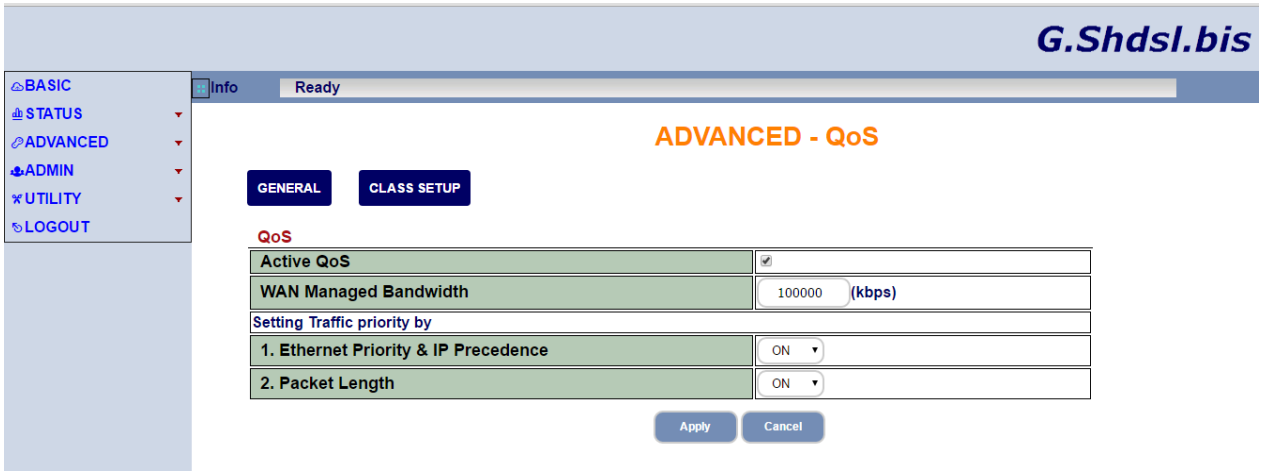
Item	Description
Name	This field displays the name of the VLAN group
VID	This field displays the ID number for a VLAN group.
MGMT	Specify the selected VLAN group as manageable.
Port Number	The columns display the VLAN settings on each port. "**Tag**" for a tagged port. "**UnTag**" for an untagged port. "Not Group" for ports without VLAN settings.
PVID	This field displays the ID number of the VLAN group

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.7 QoS

QoS is the function to decide the priorities of setting IPs to transfer packets under the situation of overloading bandwidth. Use QoS set up for traffic management of the SHDSL.bis router.

ADVANCED>QoS



General

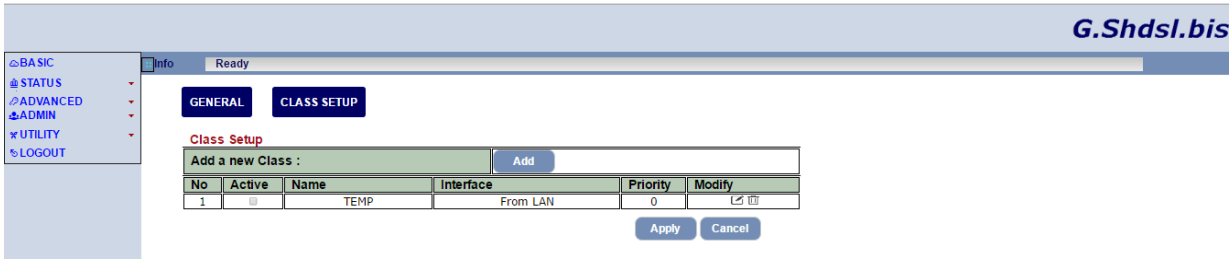
QoS

Item	Description
Active QoS	Active QoS for traffic management
WAN Management Bandwidth	Specify the bandwidth allocated to WAN using QoS. Matching the bandwidth to WAN's actual speed is recommended.
Ethernet Priority & IP Precedence	This field is not effective when traffic matches the class configured under **CLASS SETUP**. When select ON and traffic doesn't match the class configured under **CLASS SETUP**, the router assigns priority to unmatched traffic based on IEEE 802.1p priority level, IP precedence.

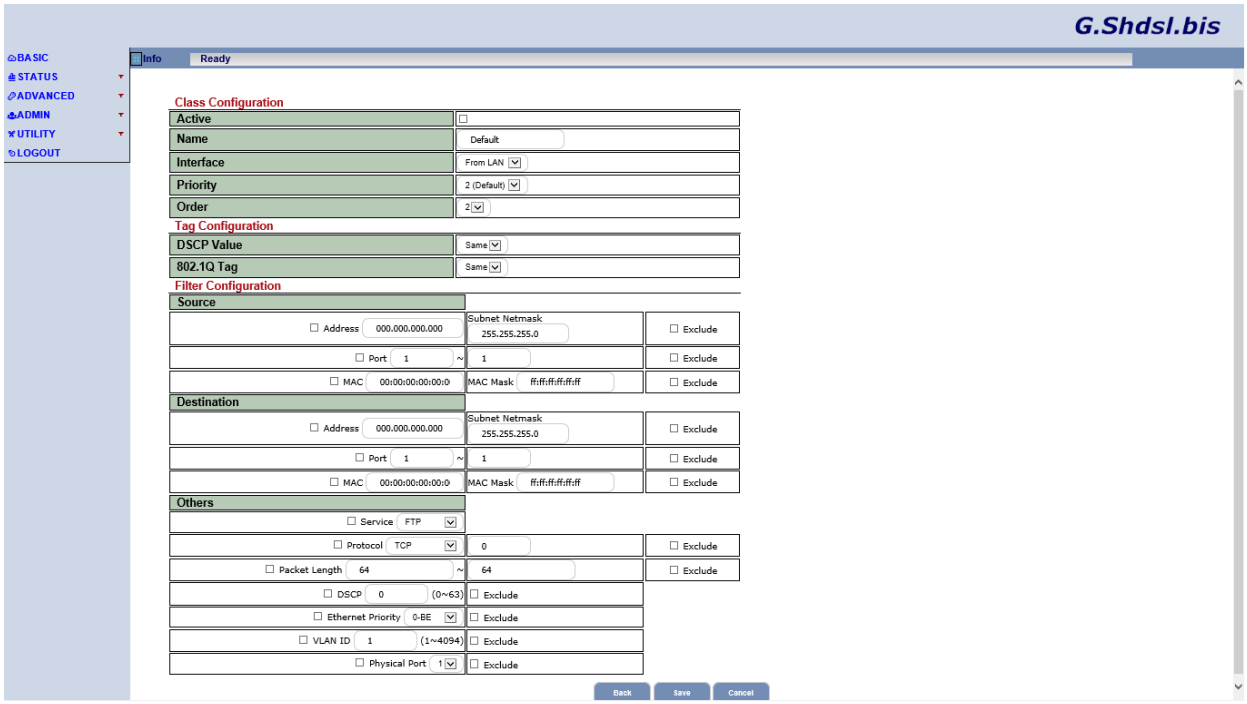
	When select OFF, unmatched traffic is mapped to Queue Two.
Packet Length	This field is not effective when traffic matches the class configured under **CLASS SETUP**. When select ON and traffic doesn't match the class configured under **CLASS SETUP**, the router assigns priority to unmatched traffic based on IEEE 802.1p priority level, Packet Length. When select OFF, unmatched traffic is mapped to Queue Two.

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

CLASS SETUP



Click on Add to create a new class



Class Configuration

Item	Description
Active	Activate the classifier
Name	Enter the name of the classifier
Interface	Select from WAN or from LAN for the traffic of the classifier
Priority	Assign priority to the traffic of the classifier
Order	Ordering number of the classifier

Tag Configuration

Item	Description
DSCP Value	Select Same to keep the DSCP field in the packets. Select Auto to map the DSCP value to 802.1 priority level automatically
802.1Q Tag	Select Same to keep the priority setting and VLAN ID of the frames. Select Auto to map 802.1 priority level to the DSCP value automatically

Filter Configuration

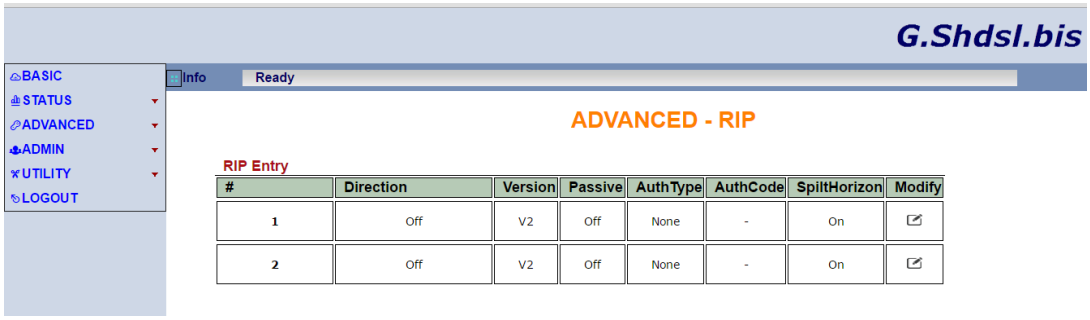
Item	Description
Active	Activate the classifier
Name	Enter the name of the classifier
Interface	Select from WAN or from LAN for the traffic of the classifier
Priority	Assign priority to the traffic of the classifier
Order	Ordering number of the classifier

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.8 RIP

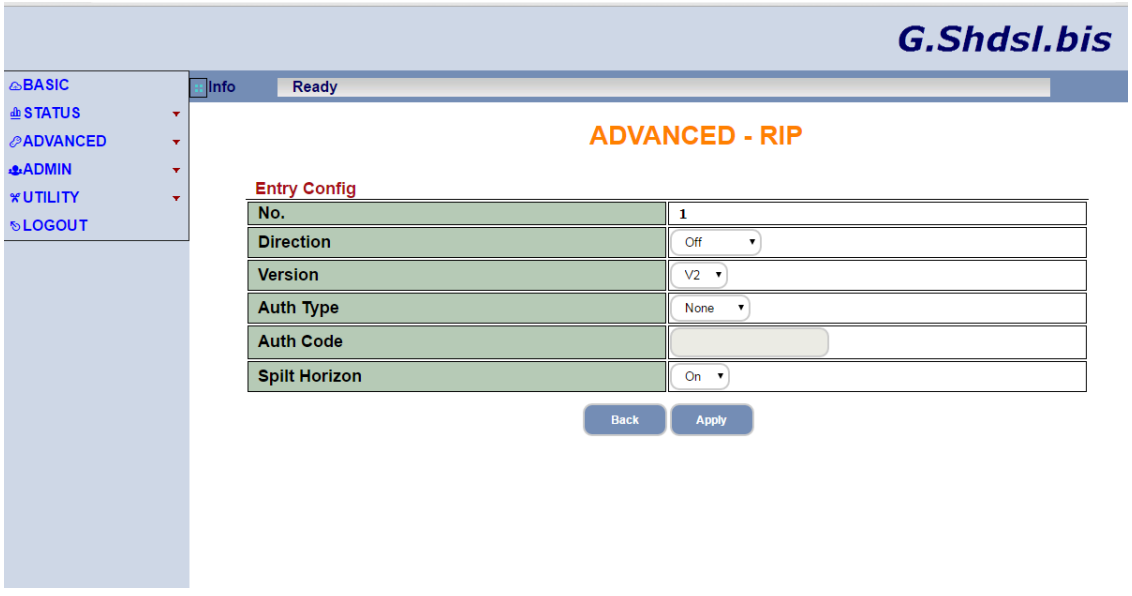
RIP (Routing Information Protocol) allows one router to exchange routing information with another.

ADVANCED>RIP



Click Modify to edit each entry information

RIP>Entry Config



Entry Config

Item	Description
Direction	Select Directions from: **Off**: No RIP packets will be sent, and incoming RIP packets will be ignored **Both**: Routing table will be broadcasted periodically and incorporated received information from both direction **In Only**: Only RIP information received will be incorporated **Out Only**: Only broadcast device's routing table periodically
Version	Select from:

	RIP-V1: Only sends RIP v1 messages only **RIP-V2**: Sends RIP v2 messages in multicast and broadcast format
Auth Type	Select from (1)Simple (2)MD5
Auth Code	Enter the Corresponded Authentication Code for the Type picked above
Split Horizon	Enable or Disable Split Horizon feature

Click Apply to save the parameters changed or Back to return to previous page

4.3.9 NAT/DMZ

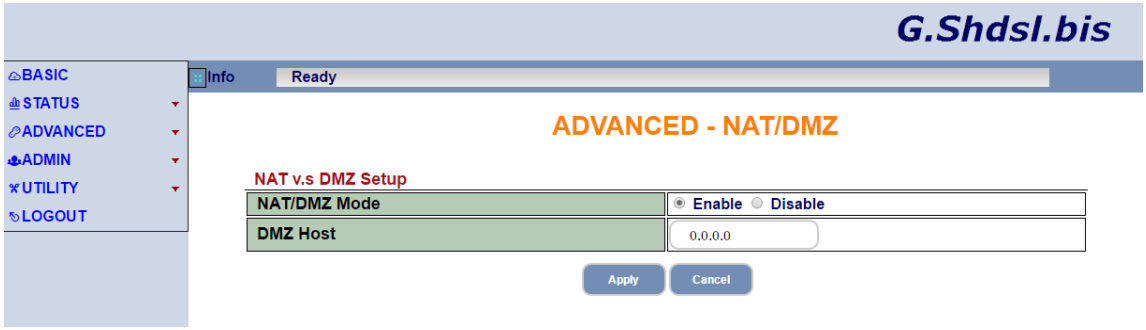
NAT *(Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network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

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

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

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

ADVANCED>NAT/DMZ



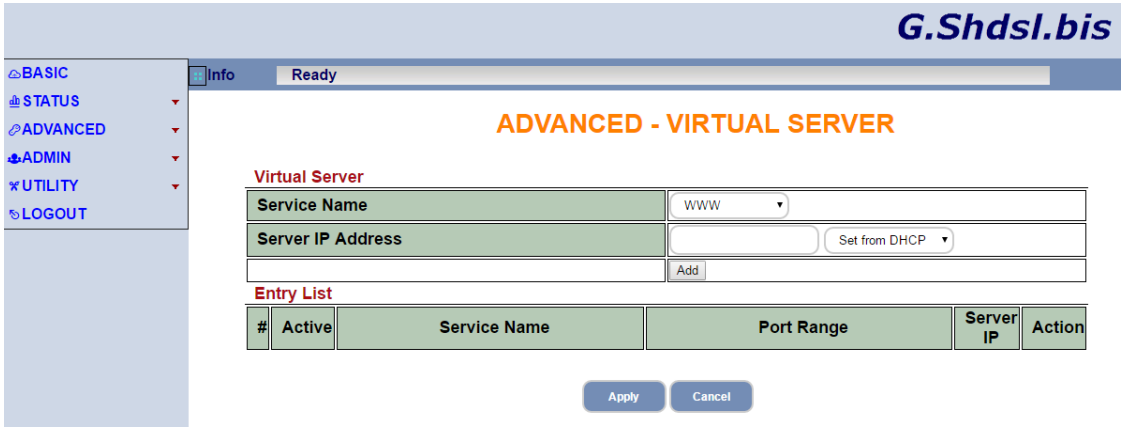
NAT v.s DMZ Setup

Item	Description
NAT/DMZ Mode	Select to Enable or Disable NAT/DMZ mode
DMZ Host	Assign IP address for the DMZ Host

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.10 Virtual Server

ADVANCED>Virtual Server



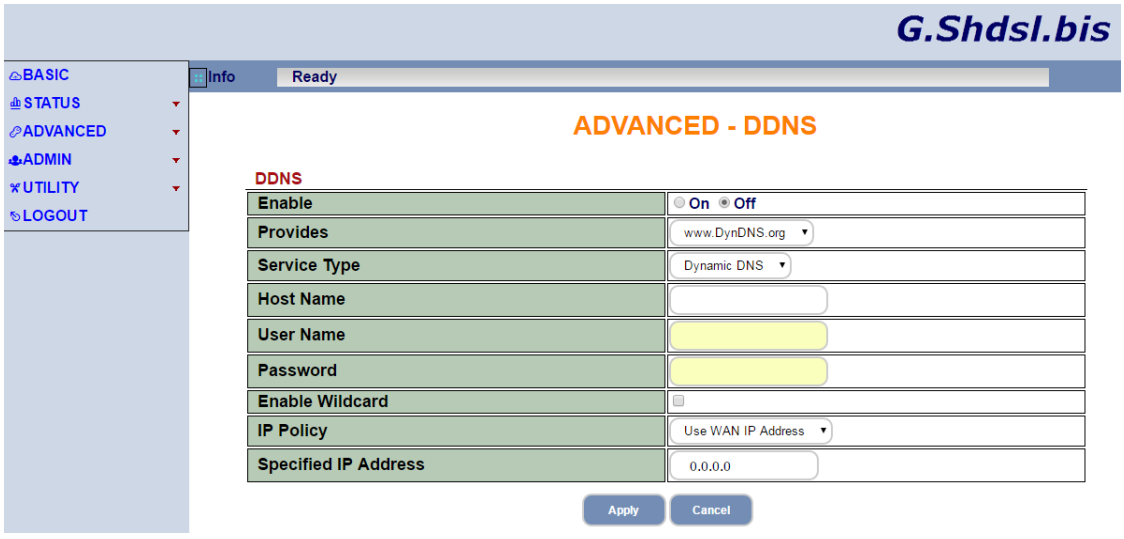
Virtual Server

Item	Description
Service Name	Select the desired Service name from the drop down list with predefined parameters or manually define the Service with corresponded IP address and Port range.
Server IP Address	Specify the IP address of the Service's Hosting Server

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.11 DDNS

ADVANCED>DDNS



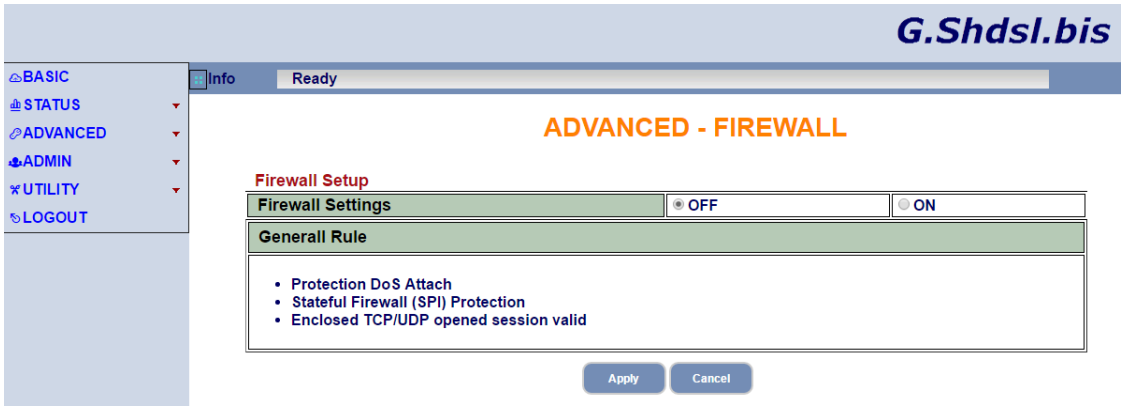
DDNS

Item	Description
Enable	Select On to enable or Off to disable DDNS function
Providers	Drop down menu to select desired DNS service provider
Service Type	Select the type of service you have registered with your DDNS service provider. It can be one of the following: **Dynamic DNS:** **Static DNS:** **Custom DNS:**
Host Name	Domain name assigned to the device by the DDNS provider
User Name	Username for the registered DDNS service provider
Password	Password for the registered DDNS service provider
Enable Wildcard	Check the box to enable Wildcard feature
IP Policy	**Use WAN IP Address**: Update the IP address of the Host Name with the WAN IP address **Server Auto Detect**: This allows DDNS server to automatically detect and use the IP address of the NAT router that has a public IP address. **Note**: *therefore, select this option only when there is at least one NAT router available in-between device and DDNS server* **Specified IP Address**: Specify a static IP address for the Host Name.
Specified IP Address	Input the static IP address for the Host Name if IP Policy is selected with Specified IP Address option.

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.12 FIREWALL

ADVANCED>FIREWALL



Firewall Setup

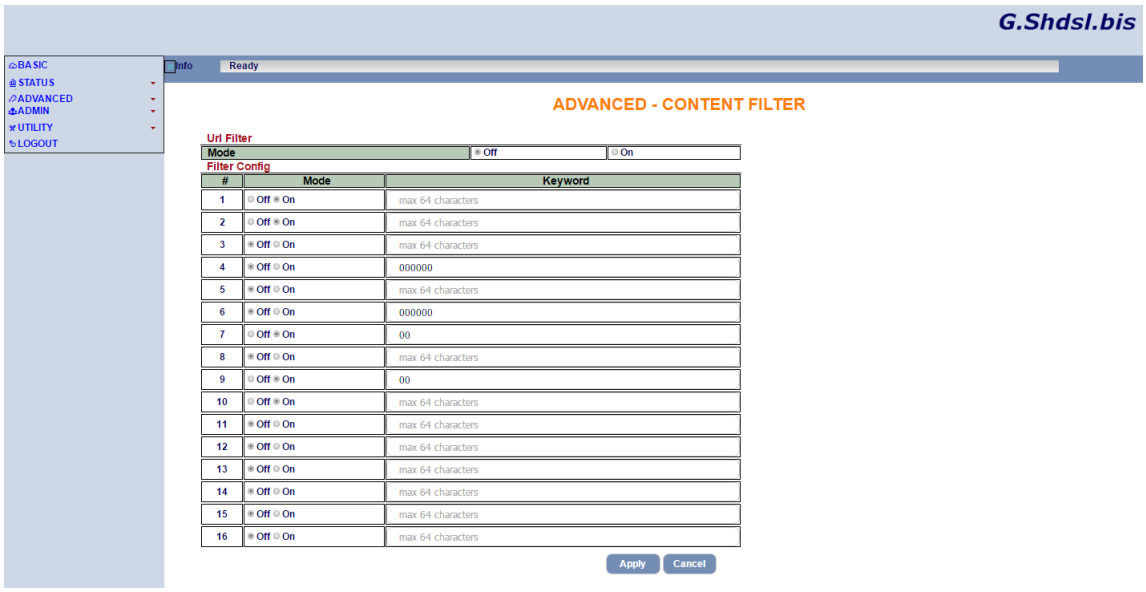
Item	Description
Firewall Settings	Select OFF to disable Firewall, or ON to enable Firewall

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.3.13 Content Filter

Content Filter allows you to limit access to specific websites based on keywords in the URL

ADVANCED>Content Filter



Url Filter

Item	Description
Mode	Select OFF to disable Content Filter, or ON to enable Content Filter feature

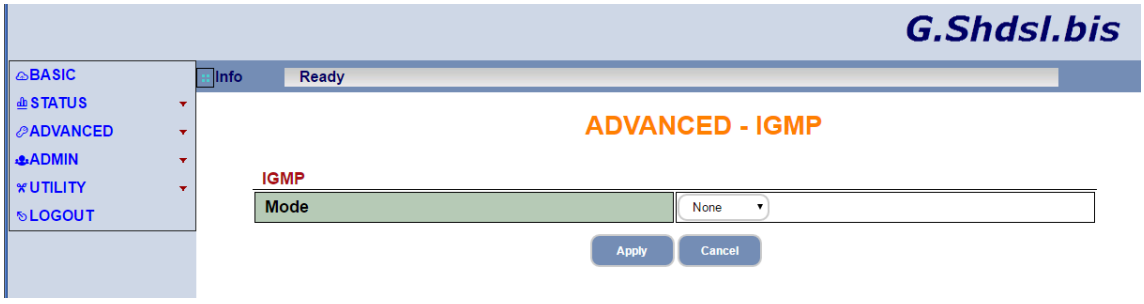
Filter Config

Item	Description
Mode	Turning Off or On of the selected Filter condition
Keyword	Specify the desired keywords to be filtered with

4.3.14 IGMP

IGMP (Internet Group Multicast Protocol) is a network layer protocol which is used to establish membership in a Multicast group.

ADVANCED>IGMP

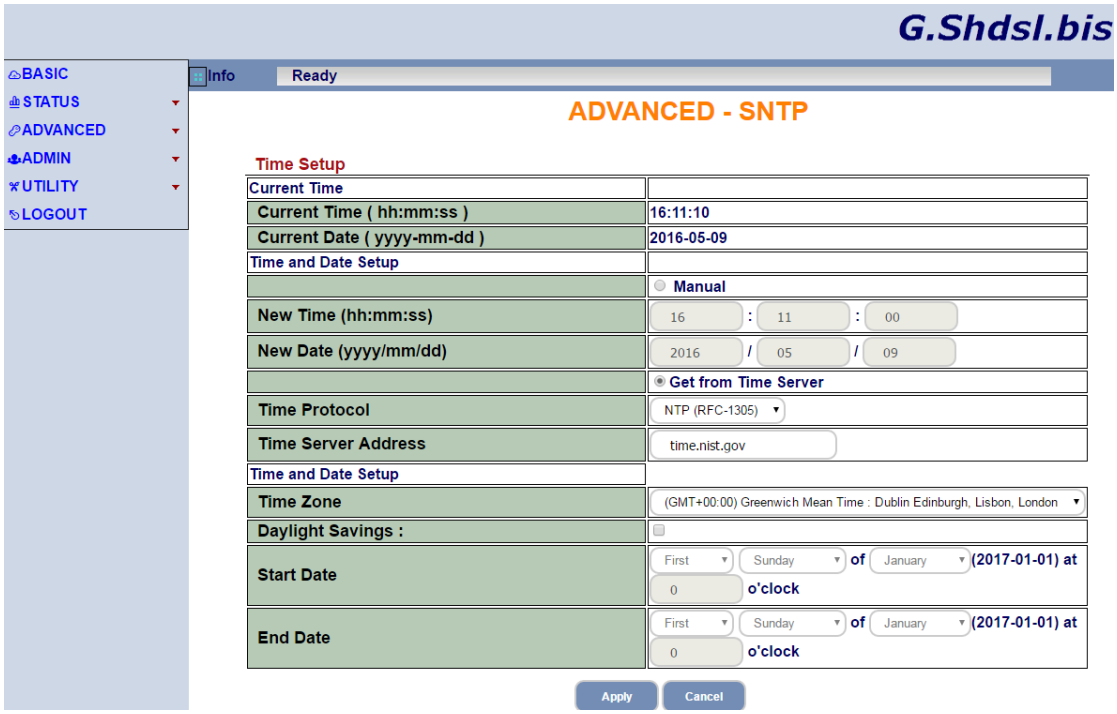


IGMP

Item	Description
Mode	Select from the drop down menu for desired IGMP modes: **None**: Don't support any of the IGMP **IGMP-v1**: Support only version1 **IGMP-v2**: Support only version2 **IGMP-v3**: Support only version3 **IGMP-all**: Support all the available versions

4.3.15 SNTP

ADVANCED>SNTP



Time Setup

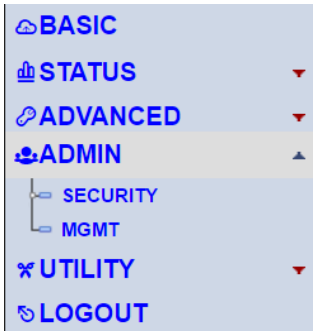
Item	Description
Current Time (hh:mm:ss)	Display current system time
Current Date (yyyy-mm-dd)	Display current system date
	*Manual
New Time (hh:mm:ss)	Manually define the new time
New Date (yyyy/mm/dd)	Manually define the new date
	*Get from Time Server
Time Protocol	Time protocol used to communicate with Time server
Time Server Address	Specify the IP address or URL of the Time server
Time Zone	Specify the Time zone
Daylight Savings	Check box to enable Daylight Savings function
Start Date	Specify the date when daylight saving starts
End Date	Specify the date when daylight saving ends

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.1 ADMIN

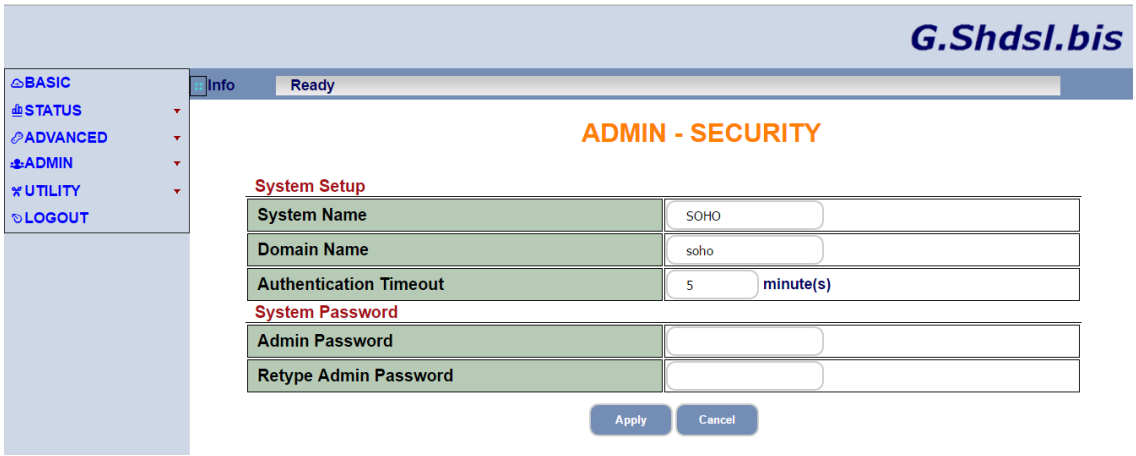
Overview

Administration session introduces security and management features (SNMP, WWW, TELNET, SSH) of the SHDSL.bis router.



4.1.1 Security

ADMIN>SECURITY



System Setup

Item	Description
System Name	Enter desirable System/Host Name
Domain Name	Enter desirable Domain Name
Authentication Timeout	Enter desirable Authentication Timeout period in minutes

System Password

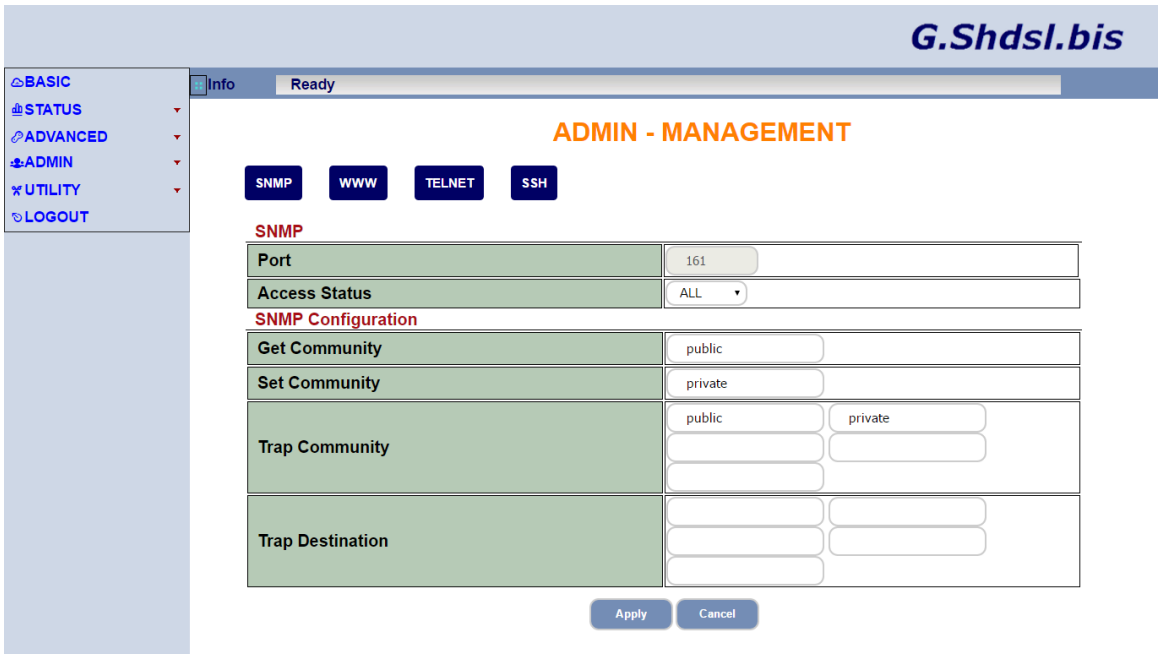
Item	Description
Admin Password	Enter Password
Retype Admin Password	Enter Password again for confirmation

For system security, please change the default password in the first setup otherwise unauthorized persons can access the router and change the parameters. If you don't change it, all users on your network can access the router using the default password: "***root***".

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.1.2 Management

ADMIN>MGMT



4.1.2.1 SNMP

Simple Network Management Protocol (SNMP) defines the exchange of messages between a network management client and a network management agent for remote management of network nodes. These messages contain requests to get and set variables that exist in network nodes in order to obtain statistics, set configuration parameters, and monitor network events. SNMP communications can occur over LAN or WAN connection.

The router can generate SNMP traps to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security. The SHDSL.bis routers support SNMPv1/SNMPv2 (RFC 1157/1901/1905) and MIB-II (RFC 1213/1493)

Click SNMP to configure the parameters for remote management via SNMP.

SNMP

Item	Description
Port	Enter port number for the SNMP service
Access Status	Click on the drop-down list and select **ALL** to allow the service or **Disable** to disable the remote management service

SNMP Configuration

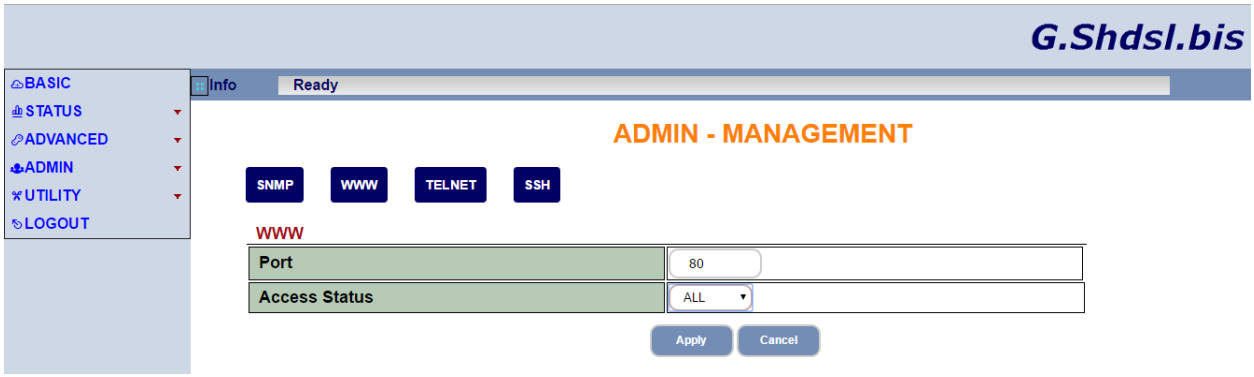
Item	Description
Get Community	Enter the password for the incoming Get and Get Next requests from the management station. The default is public which allows all requests.

Set Community	Enter the password for the incoming Set requests from the management station. The default is public which allows all requests.
Trap Community	Enter the password sent with each trap to the SNMP manager. The default is public which allows all requests.
Trap Destination	Enter the IP address of the station to send SNMP traps

Click on Apply to save the parameters or Cancel to start configuring this page from beginning.

4.1.2.2 WWW

Click WWW to configure the parameters for remote management via WWW

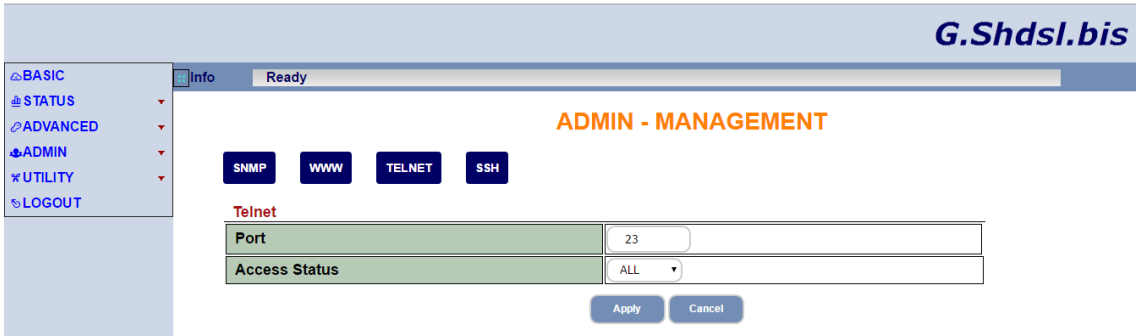


WWW

Item	Description
Port	Enter port number for remote management via WWW
Access Status	Click on the drop-down list and select **ALL** to allow the service or **Disable** to disable the remote management service

4.1.2.3 TELNET

Click TELNET to configure the parameters for remote management via TELNET

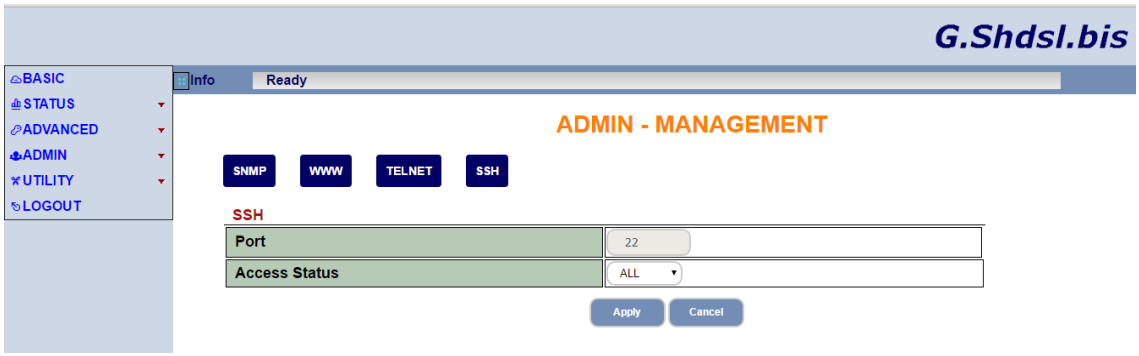


TELNET

Item	Description
Port	Enter port number for remote management via TELNET
Access Status	Click on the drop-down list and select **ALL** to allow the service or **Disable** to disable the remote management service

4.1.2.4 SSH

Click SSH to configure the parameters for remote management via SSH



SSH

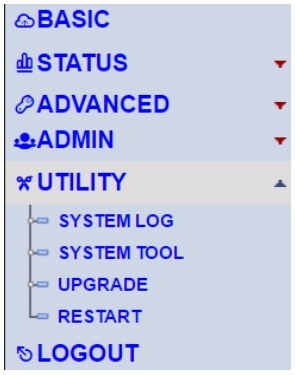
Item	Description
Port	Enter port number for remote management via SSH
Access Status	Click on the drop-down list and select **ALL** to allow the service or **Disable** to disable the remote management service

4.2 Utility

Overview

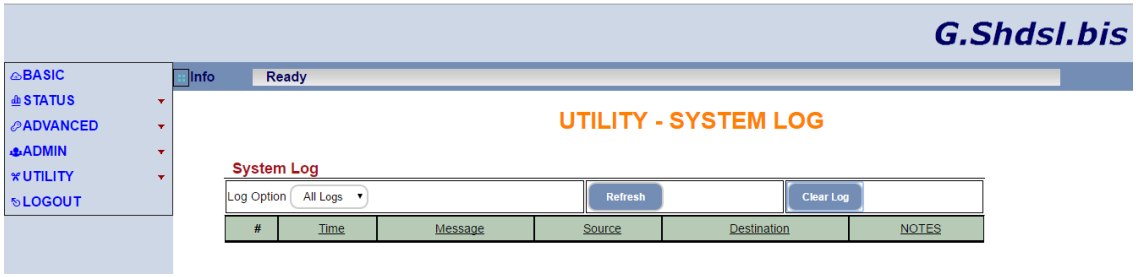
This section describes the utility of the SHDSL.bis router including:

SYSTEM LOG	Capturing log information
SYSTEM TOOL	Backup and restore configuration, and load the factory default configuration
UPGRADE	Upgrade the firmware
RESTART	Restart the router.



4.2.1 SYSTEM LOG

UTILITY>SYSTEM LOG

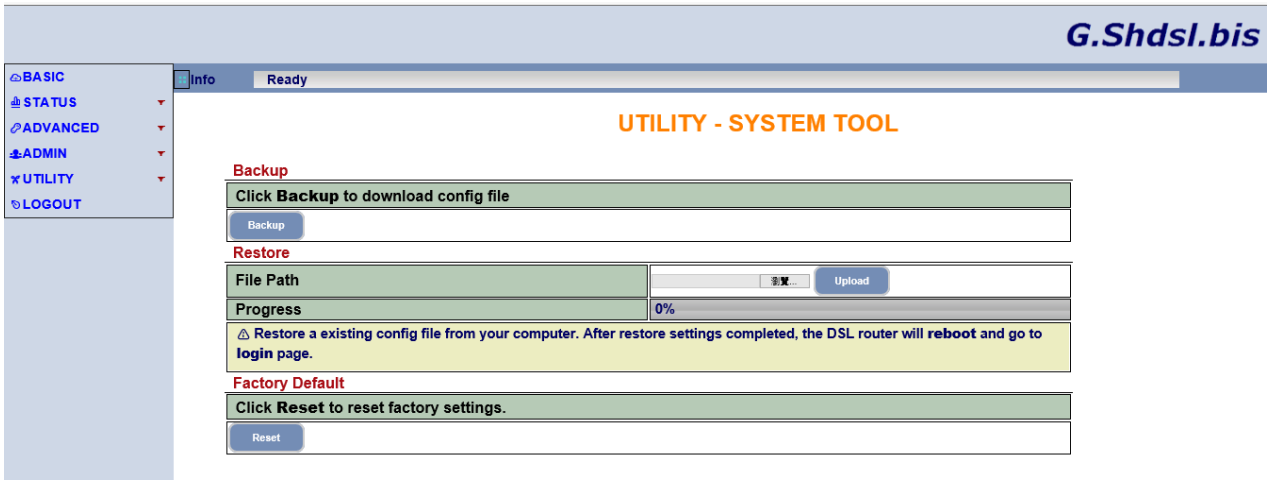


SHDSL.bis routers support detailed logging information via System Log function. The system log protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event message. The router can generate a syslog message and send it to a syslog server.

You may click Refresh to renew the Sytem Log page or Clear Log to delete all log information.

4.2.2 System Tool

UTILITY>SYSTEM TOOL



System Tool provides three main functions: Backup Configuration, Restore Configuration and Load Factory Default settings.

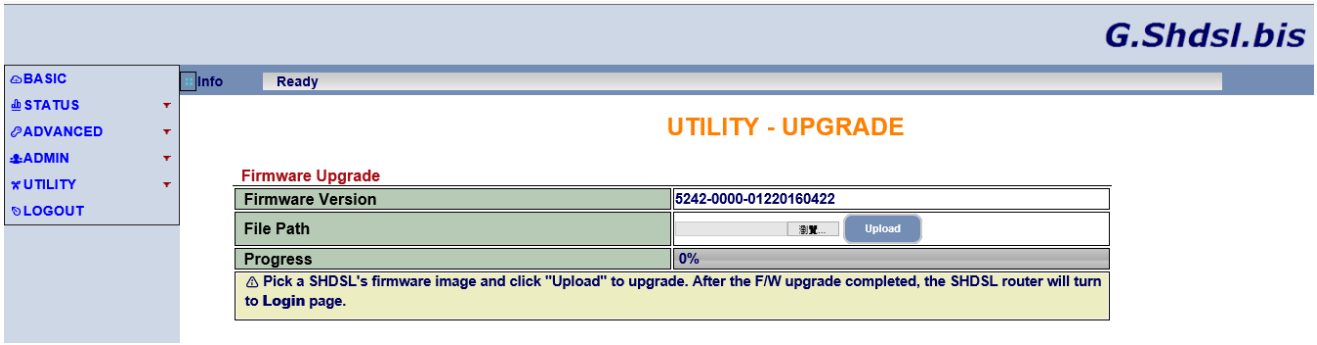
Click Backup to save config.cfg in your computer.

To restore a previously saved config file from your computer. Click Browse to select the file and then click Upload.

Click Reset to load factory default settings to the router. A warning message will appear. Confirm by clicking on OK.

4.2.3 Upgrade

UTILITY>UPGRADE

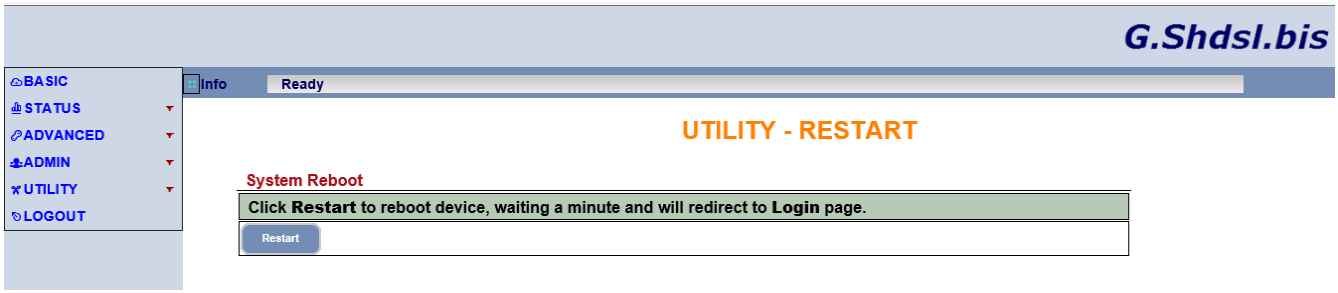


You can upgrade the SHDSL.bis router using the upgrade function.

Click Browse to select the firmware file and then click Upload. The system will reboot automatically after finish the firmware upgrade operation.

4.2.4 Restart

UTILITY>RESTART



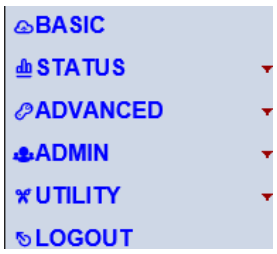
Use RESTART to reboot the SHDSL.bis router.

Click on Restart to reboot the system.

4.3 LOGOUT

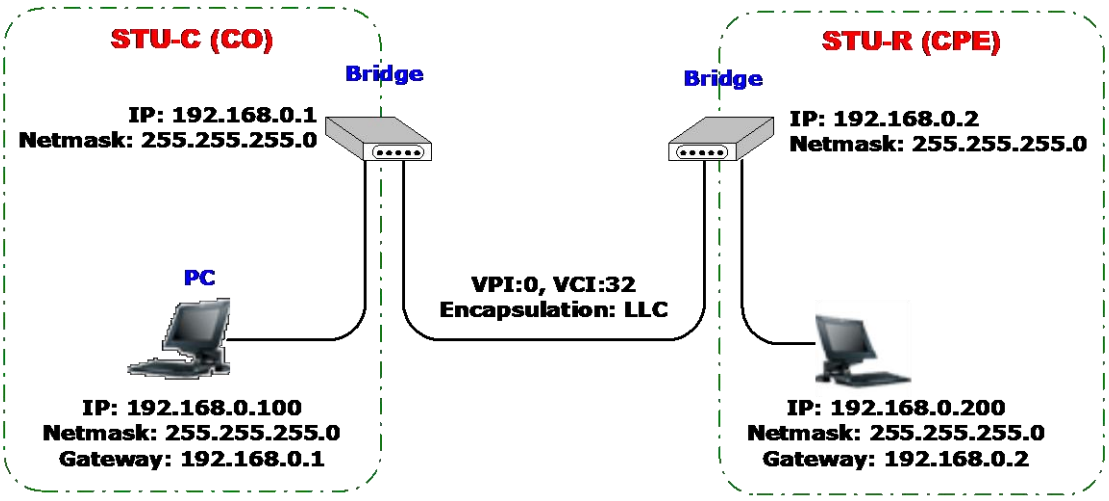
Overview

To logout the router, click on LOGOUT. A warning message will appear. Confirm by clicking on OK.



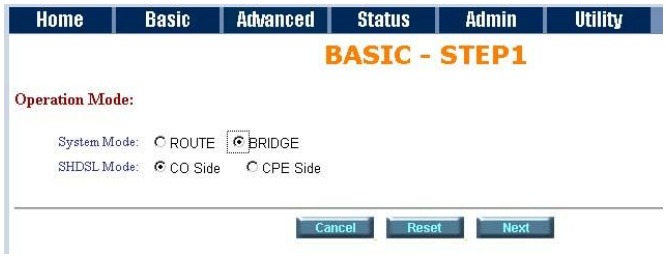
Example

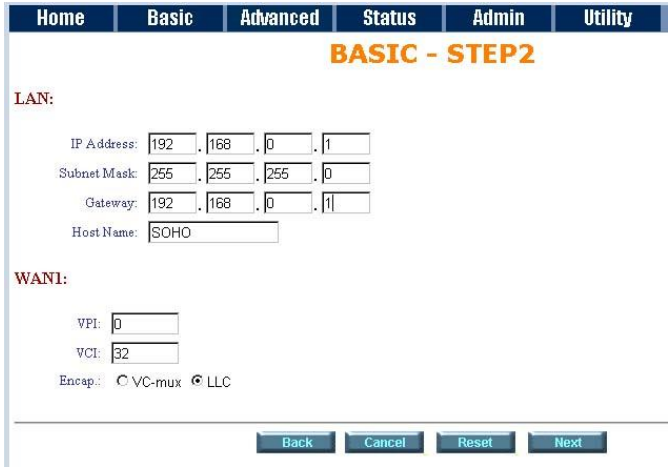
4.3.1 LAN-to-LAN connection with bridge Mode



4.3.1.1 CO side

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





Enter **LAN** Parameters
IP: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
Host Name: SOHO

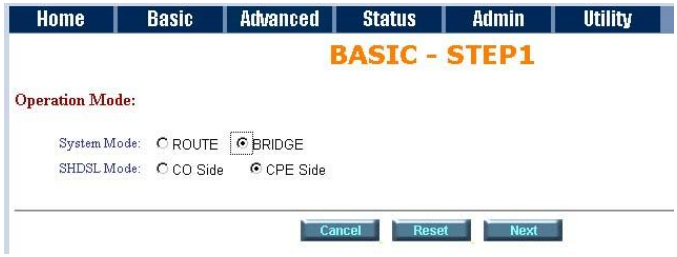
Enter **WAN1** Parameters

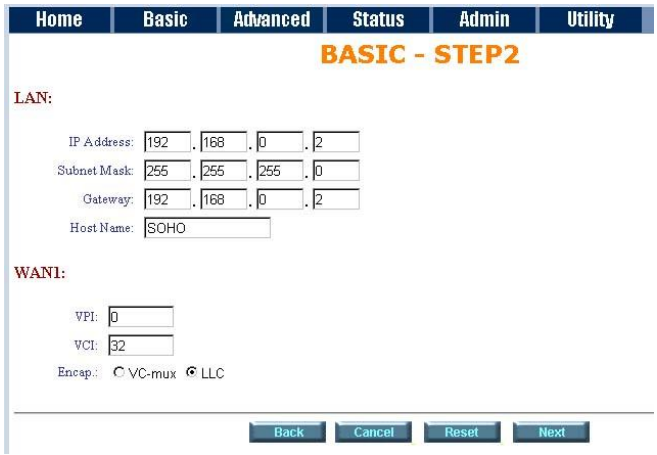
VPI: 0
VCI: 32
Click LLC
Click Next

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

4.3.1.2 CPE Side

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



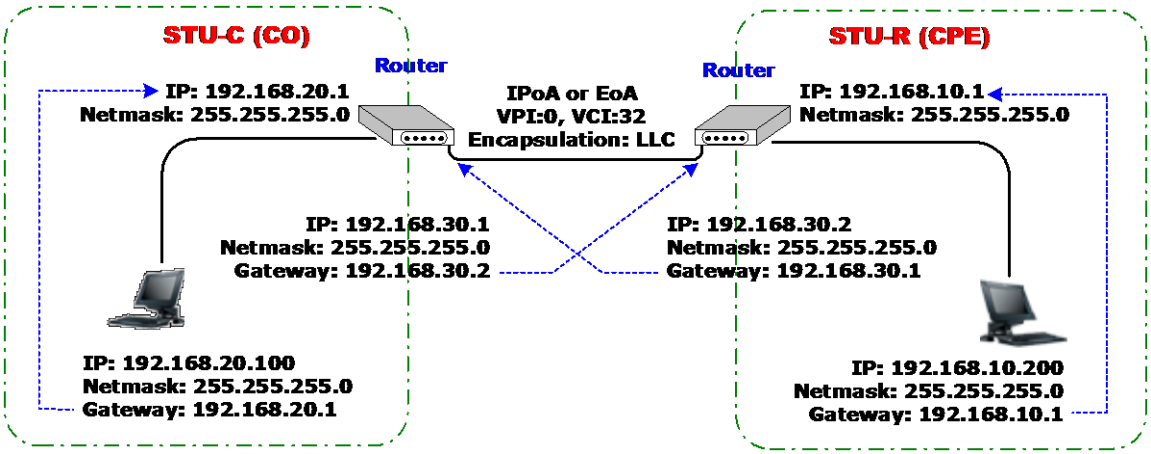


Enter **LAN** Parameters
IP: 192.168.1.2
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.2
Host Name: SOHO

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

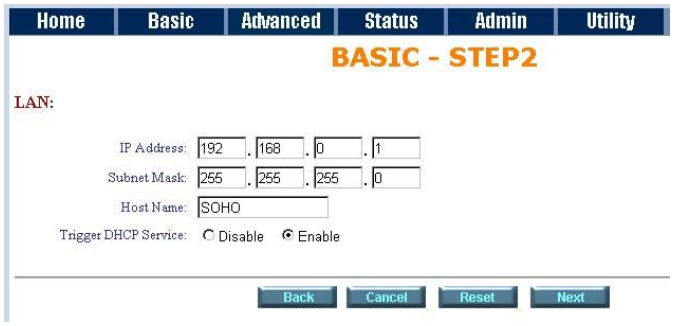
The screen will prompt the new configured parameters. Check the parameters and Click Restart
The router will reboot with the new setting.

4.3.2 LAN to LAN connection with routing mode

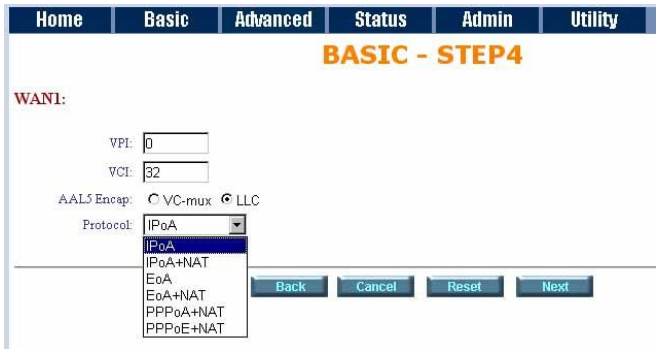


4.3.2.1 CO Side

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



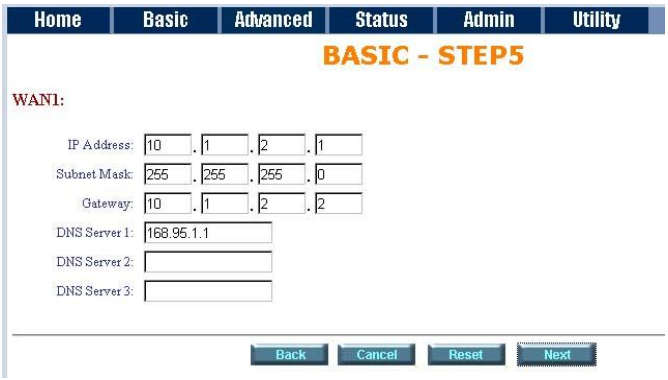
Type **LAN** parameters:
IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0
Host Name: SOHO
DHCP Service: Disable or Enable
For more **DHCP** service, review the chapter on DHCP Service



Type the **WAN1** Parameters;
VPI: 0

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

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



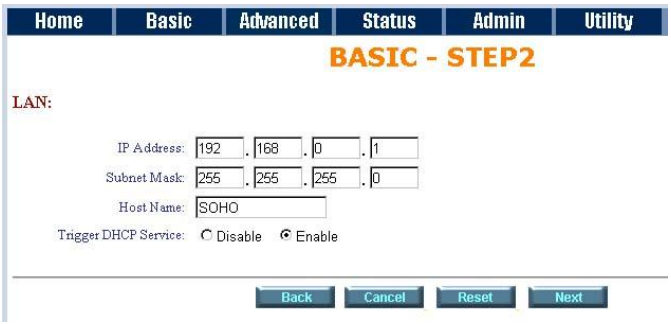
IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0
Gateway: 192.169.30.2
Click Next

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

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

4.3.2.2 CPE side

Click ROUTE and CPE Side then press Next.



Type LAN parameters:

IP Address: 192.168.10.1

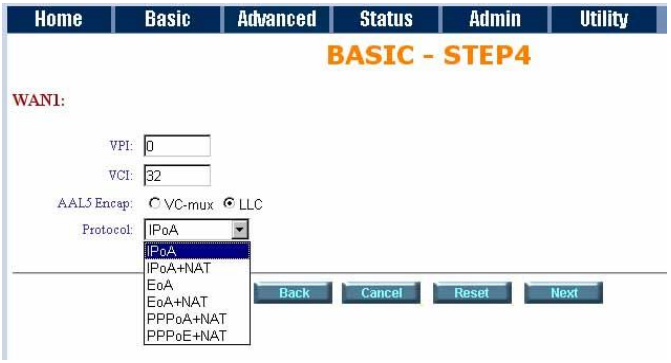
Subnet Mask: 255.255.255.0

Host Name: SOHO

DHCP Service: Disable or Enable

For more **DHCP** service, review the chapter of DHCP Service.

Type the WAN1 Parameters:



VPI: 0

VCI: 32

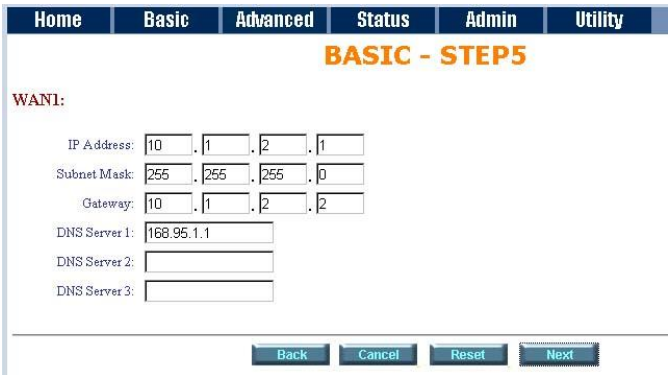
AAL5 Encap: LLC

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

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

Click Next to setup the IP parameters.

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



IP Address: 192.168.30.2

Subnet mask: 255.255.255.0

Gateway: 192.169.30.1

Click Next

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

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

5 Configuration via Serial Console or Telnet

In this section, the basic of console line configuration will be described on below.

5.1 Introduction

5.1.1 Serial Console

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

Parameter	Value
Baud Rate	115200bps
Data Bits	8
Parity Check	No
Stop Bits	1
Flow-control	No

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

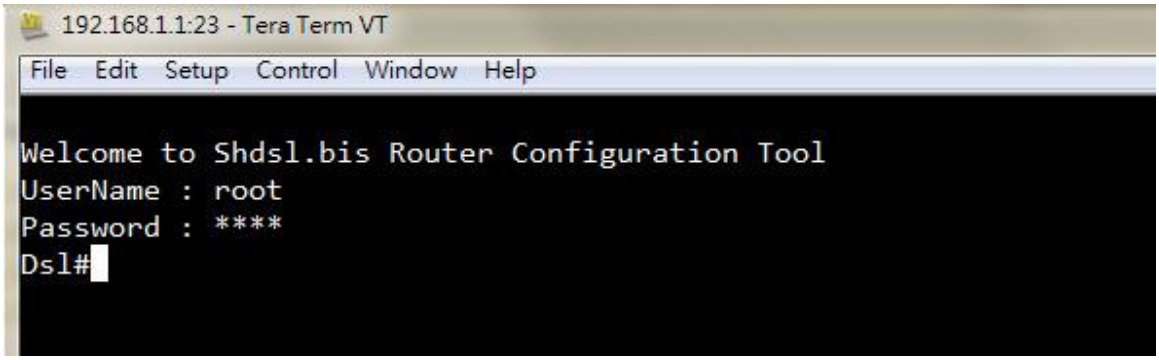
```
5242-0000-1220160511
Beta r400
Wed May 11 05:34:57 UTC 2016
======================================================
Welcome to Shdsl.bis Router Configuration Tool
UserName : root
Password : ****
```

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

Note: The factory default **User** and **Password** are “root” for both.

5.1.2 Telnet

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




```
User: root
Password: ****
```

Note: The default IP address is 192.168.1.1.

5.2 Main menu

When enter to prompt screen, you can input command **?** to view the available top level menus of each command set:

For example: type **?** after the #, will display the current level of available command sets as below:

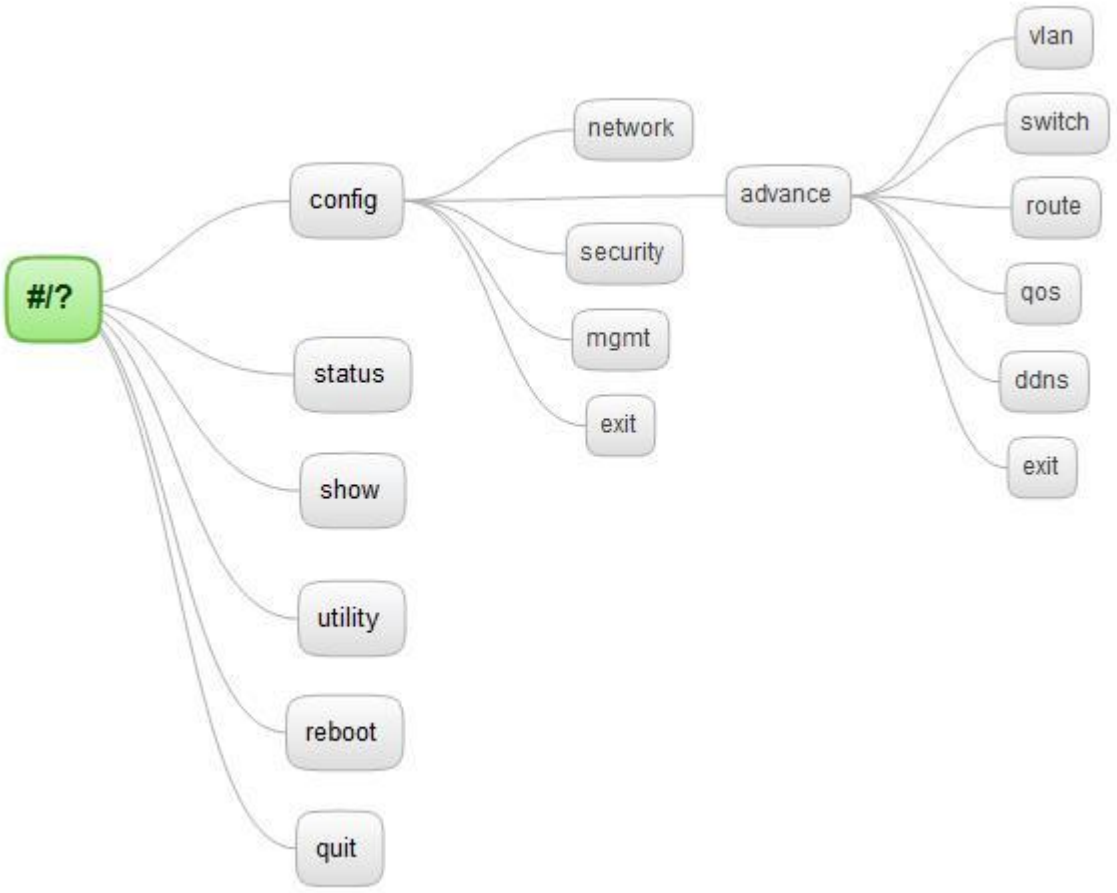
```
Dsl#?
   config              enter submenu system
   status              enter submenu status
   show                enter submenu information
   utility             enter submenu utility
   test                test tool(DebugVersion)
   ps                  show  ps
   reboot              reboot system
   shell               enter linux shell
   mib                 enter submenu mib
   quit                logout
Dsl#
```

Top level Command set Description:

Command	Description
config	Config parameters of router by entering submenu: **network** **advance** **security** **mgmt.** **exit**
status	View the status of router.
show	Show the system and configuration of router.
utility	Upgrade software and backup and restore configuration.
test	Test tool (DebugVersion)
ps	
reboot	Reset and boot system. After you have completed all necessary setting, make sure to apply the new configuration to NVRAM and reboot the system,

	otherwise, all of your changes will not take effect.
Shell	Enter linux shell
Mib	Enter submenu mib
quit	Quit system.

5.3 Key CLI Command tree overview



CTC union®

www.ctcu.com

T +886-2 2659-1021 F +886-2 2659-0237 E sales@ctcu.com