

NetComm[®]
Broadband Solutions

User Guide



NB712 and NB714
G.SHDSL 4-port Modem Router

Contents

1 Introduction	4
1.1 Features	4
1.2 Package Contents	4
1.3 Specification	5
1.4 Application	7
2 Firewall	8
2.1 Types of Firewall	9
2.2 Denial of Service Attack	10
3 VLAN (Virtual Local Area Network)	12
3.1 Specification	12
3.2 Frame Specification	12
3.3 Applications	13
4 Getting to know the router	14
4.1 Front Panel	14
4.2 Rear Panel	15
5 Connecting your G.SHDSL Modem Router	16
6 Configuration via Web Browser	19
7 Basic Setup	21
7.1 Bridge Mode	22
7.2 Routing Mode.....	24
8 Advanced Setup.....	34
8.1 SHDSL.....	35
8.2 WAN.....	37
8.3 Bridge	39
8.4 VLAN	41
8.5 Route	43
8.6 NAT/DMZ.....	45
8.7 Virtual Server	47
8.8 Firewall.....	48
8.9 IP QoS.....	56
9 Administration.....	58
9.1 Security	59
9.2 SNMP	61
9.3 Time Sync.....	64

10 Utility	66
10.1 System Info.....	67
10.2 Config Tool.....	68
10.3 Upgrade.....	69
10.4 Logout.....	70
10.5 Restart.....	71
11 Status	72
12 LAN-to-LAN connection with bridge Mode	73
12.1 CO side	73
12.2 CPE Side.....	75
13 LAN to LAN Connection with Routing Mode	76
13.1 CO side	76
13.2 CPE side.....	78
14 Configuration via Serial Console or Telnet with Menu Driven Interface.....	80
14.1 Serial Console.....	80
14.2 Telnet	80
14.3 Operation Interface.....	81
14.4 Window structure	82
14.5 Menu Driven Interface Commands.....	83
14.6 Menu Tree.....	84
14.7 Configuration	85
14.8 Status.....	87
14.9 Show.....	88
14.10 Write	89
14.11 Reboot.....	89
14.12 Ping	89
14.13 Administration	89
14.14 Utility.....	95
14.15 Exit.....	95
14.16 Setup	95
Appendix A: Cable Information	112
RJ-45 Network Ports	112
Straight and crossover cable configuration	113
Straight-Through Cabling.....	113
Cross-Over Cabling	113
SHDSL Line Connector.....	114
Console Cable.....	114
Appendix B: Registration and Warranty Information	115

1 Introduction

NetComm's NB712 (2-wire) and NB714 (2 or 4-wire selectable) G.SHDSL 4-port Security Modem Routers deliver symmetrical DSL services to small and medium size business making them an economical alternative to Leased Line or ISDN services.

Available in two modem router configurations, the NB712 (2-wire) and NB714 (2 or 4-wire selectable) are capable of providing data rates from 64kbps to 2.304Mbps (NB712) or 128kbps to 4.608Mbps (NB714) and fully comply with the ITU-T G.991.2 standards.

The NetComm NB712 and NB714 Modem Routers combine integrated high-end Bridging/Routing capabilities with advanced functions such as Multi-DMZ, virtual server mapping, and VPN pass-through. They also support port-based VLAN and IEEE802.1q VLAN over an ATM network. An advanced Firewall with Stateful Packet Inspection (SPI) and DoS protection, all combine to protect your network from outside intruders.

With 4 x 10/100 Base-T auto-sensing, auto-negotiation and auto-MDIX switching ports, the NetComm G.SHDSL Modem Routers enable you to leverage the latest broadband technology to meet the growing need for high performance data communication.

1.1 Features

- Easy configuration and management with password control for various applications and environments
- Efficient IP routing and transparent learning bridge to support broadband Internet services
- VPN pass-through for PPTP/L2TP/IPSec Tunneling
- Virtual LANs (VLANs) offering significant benefits in terms of efficient use of bandwidth, flexibility, performance and security
- Built-in advanced SPI firewall
- Four 10/100Mbps Auto-negotiation and Auto-MDIX switching port for flexible local area network connectivity
- DMZ host/Multi-DMZ/Multi-NAT enables multiple workstations on the LAN to access the Internet
- Full ATM protocol stack implementation over SHDSL
- PPPoA and PPPoE support user authentication with PAP/CHAP/MS-CHAP
- SNMP management with SNMPv1/SNMPv2 agent and MIB II
- Obtain enhancements and new features via Internet software upgrade

1.2 Package Contents

The following items are included in your G.SHDSL Modem Router pack:

- NB712 (2-wire)/NB714 (2 or 4-wire selectable) G.SHDSL Router
- 15V AC 1.0 Amp power supply
- RS232 Console Cable
- RJ11 ADSL line connection cable
- RJ45 10/100 Ethernet cable
- User Guide CD

If any of the above items are missing or damaged, please contact NetComm immediately.

1.3 Specification

Routing

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

Bridging

- IEEE 802.1D transparent learning bridge
- IEEE 802.1q VLAN
- Port-based VLAN
- Spanning tree protocol

Security

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

Management

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

ATM

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

ATM QoS

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

AAL5 Encapsulation

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

PPP

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

WAN Interface

- SHDSL: ITU-T G.991.2 (Annex A, Annex B)
- Encoding scheme: 16-TCPAM
- Data Rate (2-wire mode): N x 64Kbps (N=0~36, 0 for adaptive)
- Data Rate (4-wire mode): N x 128Kbps (N=0~36, 0 for adaptive)
- Impedance: 135 ohms

LAN Interface

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

Hardware Interface

- WAN: RJ-11
- LAN: RJ-45 x 4
- Console: RS232 female
- RST: Reset button for factory default

Indicators

- General: PWR
- WAN: LNK, ACT
- LAN: 1, 2, 3, 4
- SHDSL: ALM

Physical/Electrical

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

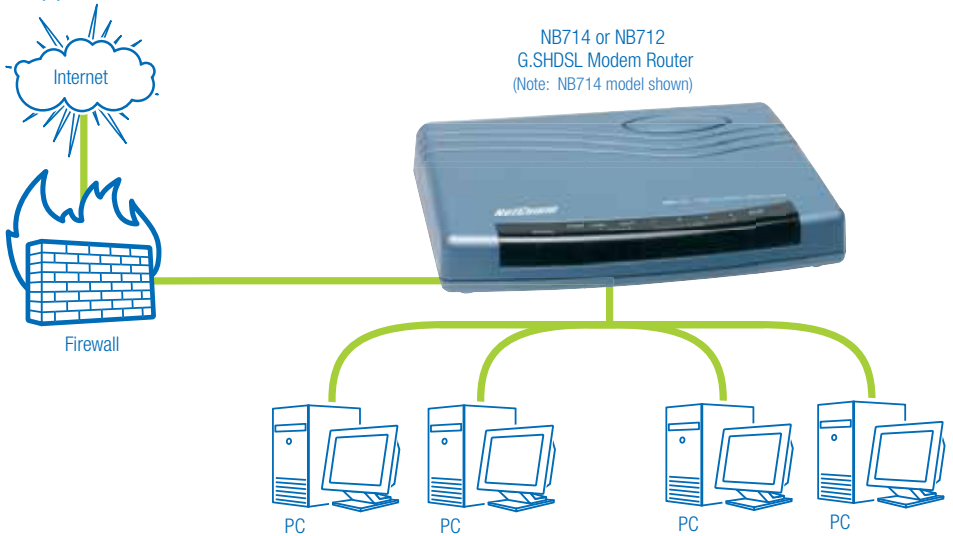
Memory

- 2MB Flash Memory, 8MB SDRAM

Product Information

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

1.4 Application

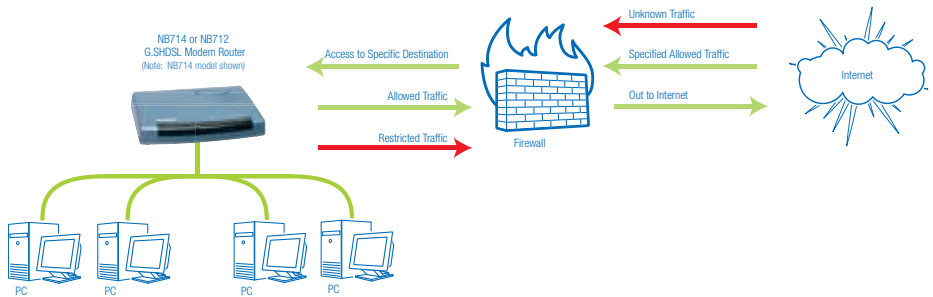


2 Firewall

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

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

It is important to note that an Internet firewall cannot prevent individual users with modems from dialling into or out of the network. By doing so they bypass the firewall altogether and open the network to attack. However, these are management issues that should be raised during the planning of any security policy and cannot be solved with Internet firewalls alone.

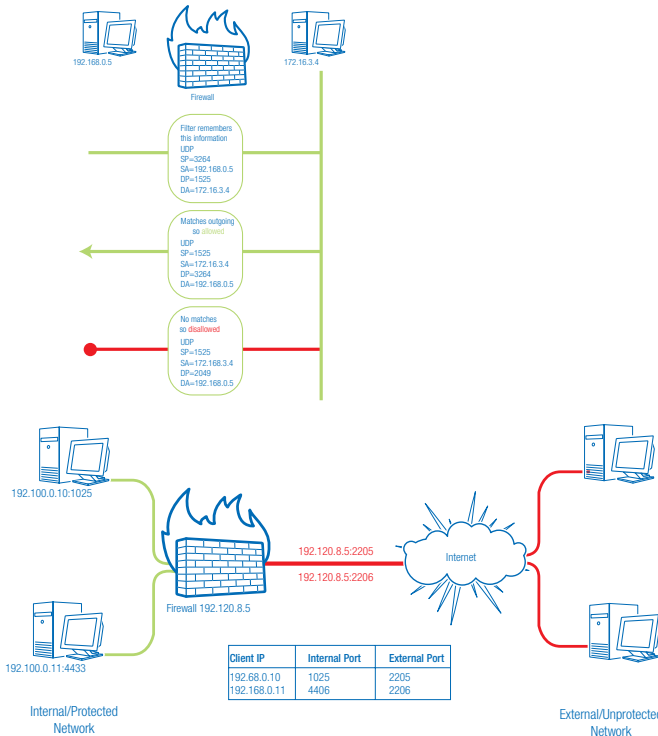
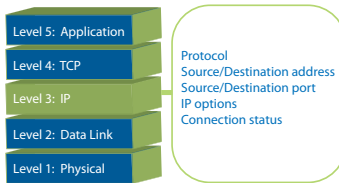


2.1 Types of Firewall

There are three types of firewall:

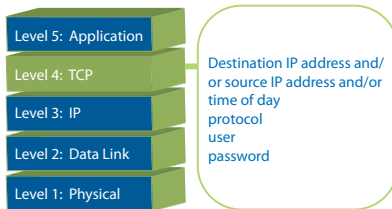
2.1.1 Packet Filtering

In packet filtering, only the protocol and the address information of each packet is examined. Its contents and context (its relation to other packets and to the intended application) are ignored. The firewall pays no attention to applications on the host or local network and it “knows” nothing about the source of the incoming data. Filtering consists of examining incoming or outgoing packets and allowing or disallowing their transmission on the basis of a set of configurable rules. Network Address Translation (NAT) routers offer the advantages of packet filtering firewalls but can also hide the IP addresses of computers behind the firewall, and offer a level of circuit-based filtering.



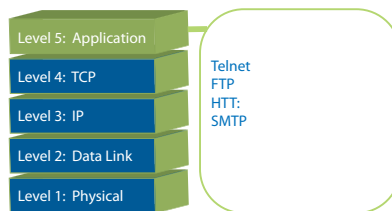
2.1.2 Circuit Gateway

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



2.1.3 Application Gateway

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



2.2 Denial of Service Attack

Denial of service (DoS) attacks typically come in two varieties: resource starvation and resource overload. DoS attacks can occur when there is a legitimate demand for a resource that is greater than the supply (i.e. too many web requests to an already overloaded web server). Software vulnerability or system misconfigurations can also cause DoS situations. The difference between a malicious denial of service and simple system overload is the requirement of an individual with malicious intent (attacker) using or attempting to use resources specifically to deny those resources to other users.

Ping of death

On the Internet, ping of death is a kind of denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments. Attackers began to take advantage of that feature when they found that a packet broken down into fragments could add up to more than the allowed 65,536 bytes. Many operating systems didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted. Other known variants of the ping of death include teardrop, bonk and nestea.

SYN Flood

The attacker sends TCP connections faster than the victim machine can process them, causing it to run out of resources and dropping legitimate connections. A new defence against this is to create "SYN cookies". Each side of a connection has its own sequence number. In response to a SYN, the attacked machine creates a special sequence number that is a "cookie" of the connection and forgets everything it knows about the connection. It can then recreate the forgotten information about the connection where the next packets come in from a legitimate connection.

ICMP Flood

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

UDP Flood

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

Land attack

The attacker attempts to slow your network down by sending a packet with identical source and destination addresses originating from your network.

Smurf attack

Where the source address of a broadcast ping is forged so that a huge number of machines respond back to the victim indicated by the address, thereby overloading it.

Fraggle Attack

A perpetrator sends a large amount of UDP echo packets at IP broadcast addresses, all of it having a spoofed source address of a victim.

IP Spoofing

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

3 VLAN (Virtual Local Area Network)

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

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

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

As DSL (over ATM) links are deployed more and more extensively, VLAN (VLAN-to-PVC) over DSL links is becoming a popular requirement of networks.

The following section will discuss the implementation of VLAN-to-PVC only for bridge mode operation, i.e., the VLAN spreads over both the COE and CPE sides, where there is no layer 3 routing involved.

3.1 Specification

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

3.2 Frame Specification

An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. Such frames are classified as belonging to a particular VLAN based on parameters associated with the receiving port. Also, priority tagged frames, which, by definition, carry no VLAN identification information, are treated the same as untagged frames.

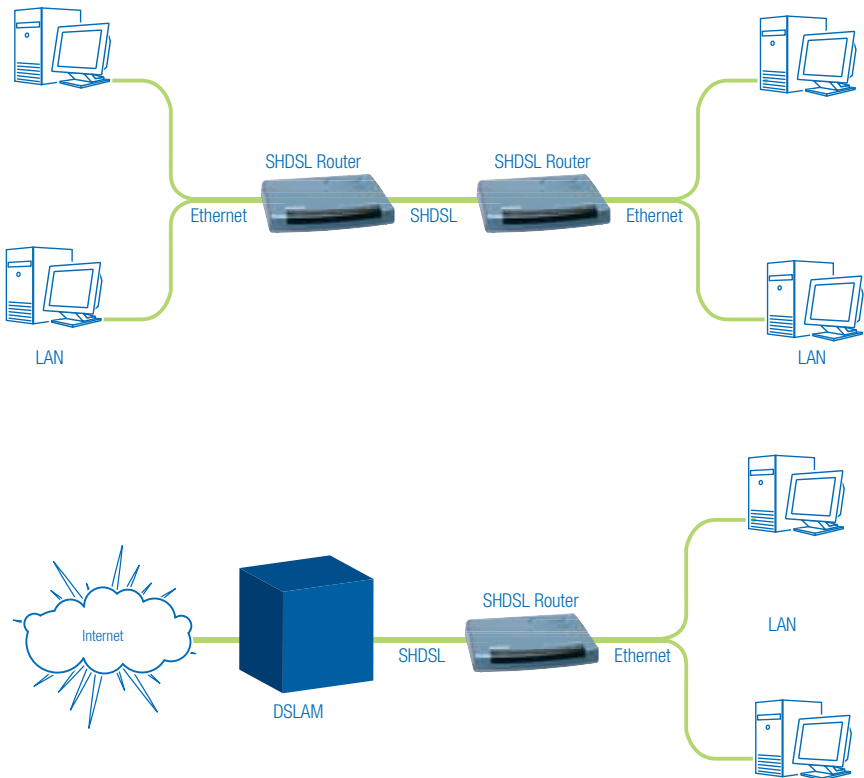
A VLAN-tagged frame carries an explicit identification of the VLAN to which it belongs; i.e., it carries a tag header that carries a non-null VID. This results in a minimum tagged frame length of 68 octets. Such a frame is classified

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

The following figure shows the difference between a untagged frame and VLAN tagged frame, where the Tag Protocol Identifier (TPID) is of 0x8100 and it identifies the frame as a tagged frame. The Tag Control Information (TCI) consists of the following elements:

- 1) User priority allows the tagged frame to carry user priority information across bridged LANs in which individual LAN segments may be unable to signal priority information (e.g., 802.3/Ethernet segments).
- 2) The Canonical Format Indicator (CFI) is used to signal the presence or absence of a Routing Information Field (RIF) field, and, in combination with the Non-canonical Format Indicator (NCFI) carried in the RIF, to signal the bit order of address information carried in the encapsulated frame.
- 3) The VID uniquely identifies the VLAN to which the frame belongs.

3.3 Applications



4 Getting to know the router

This section will introduce the hardware of the router.

4.1 Front Panel

The front panel contains LEDs which show the status of the SHDSL router. Note: The front panel LEDs of the NB712 (2-wire) and NB714 (2 or 4-wire selectable) are identical. The NB714 is shown below.



LED status

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

4.2 Rear Panel

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



Connectors	Description
DC-IN	Power adaptor inlet: Input voltage 9VDC
LAN (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
LINE	SHDSL interface for WAN port (RJ-11)
RST	Reset button to reboot or load factory default

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

- (1) Press the Reset Button for one second to reboot the system only.
- (2) Pressing the Reset Button for four seconds will cause the product to reload the factory default settings, thereby losing all of your settings. If you forget your user name or password, or if the router is having difficulties connecting to the Internet, you may want to reconfigure it to clear all previous settings. Press the Reset Button and hold for four (4) seconds with a paper clip or sharp pen/pencil.

5 Connecting your G.SHDSL Modem Router

This guide is designed to lead users through the Web Configuration of the G.SHDSL Modem 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 Modem Router at any given time. Select the method you wish to use and continue.

For Web configuration, you can skip step 3.

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

Step 1: Check the Ethernet Adapter in PC

Make sure that an Ethernet Adapter has been installed in the PC that is to be used for configuration of the router. TCP/IP protocol is necessary for web configuration, so please check that the PC has TCP/IP protocol installed.

Step 2: Check the Web Browser in PC

For Web Configuration, ensure that the PC has a Web Browser installed, such as IE or Netscape.

Note: Suggest IE5.0, Netscape 6.0 or above and 800x600 screen resolution or above.

Step 3: Check the Terminal Access Program

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

Step 4: Determine Connection Setting

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

Protocol	Selection
RFC1483	Ethernet over ATM
RFC1577	Classical Internet Protocol over ATM (CLIP)
RFC2364	Point-to-Point Protocol over ATM (PPPoA)
RFC2516	Point-to-Point Protocol over Ethernet (PPPoE)

Different Protocols are required to setup different WAN parameters. Your ISP will advise the correct protocol and the necessary WAN parameters to configure your Modem Router.

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)

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

Step 5: Install the SHDSL Router

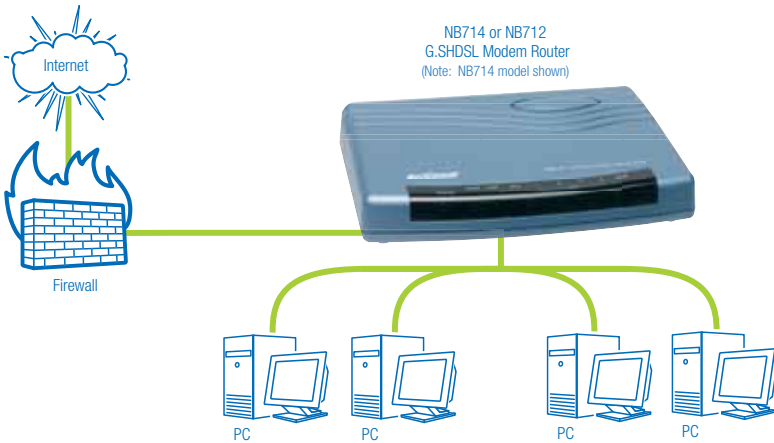
Do not turn on the Modem Router until you have completed the Hardware Installation.

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

Note: The 4-port modem router supports auto-MDIX switching, so both straight and cross-over Ethernet cables can be used.

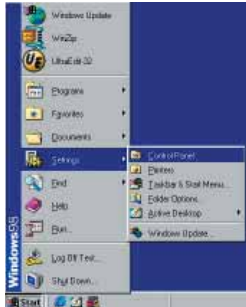
- Connect the phone cable to the product and the other side of the phone cable to the wall jack.
- Connect the power adapter to the power source.
- Turn on the PC which will be used to configure the Router.

4-port router with network topology



6 Configuration via Web Browser

For Win95, 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 associated with your network card and then click the **Properties** button.

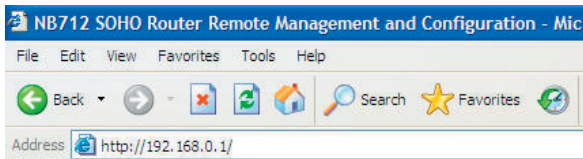


Choose IP Address tab. Select **Obtain IP address automatically**. Click the **OK** button.



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

After rebooting your PC, open your web browser and type <http://192.168.1.1> to connect to the Router.



The default IP address and sub net-mask of the Router is 192.168.1.1 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 in the network.

Type User Name **admin** and Password **admin** and then click OK.



The default user name and password are both **admin**. For the system security, we suggest you change them after configuration.

Note: After changing the User Name and Password, it is strongly recommended that you record them somewhere as a reminder for the next time you login. If you cannot remember the User Name and Password, you will need to reset the Modem Router, which will lose any previous configuration.

7 Basic Setup

The Basic Setup contains LAN, WAN, Bridge and Router operation modes. This section can be used to completely setup the router. After successfully completing it, you can access the Internet. This is the easiest and quickest way to setup the router.

Note: The advanced functions are only for advanced users. The incorrect settings of advanced functions can affect the performance of the network and cause a system error or disconnection.



Click Basic for basic installation.

7.1 Bridge Mode

Before configuring the router in bridge mode, check with your ISP to ensure you have the necessary information.

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

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

Two SHDSL modes are available: CO, Central Office, and CPE, Customer Premises Equipment. For a connection with a DSLAM, the correct SHDSL mode is CPE. For a LAN to LAN connection, one side must be CO and the other side must be CPE.

LAN Parameters

The screenshot shows the 'BASIC - STEP 2' configuration page. At the top, there are navigation tabs: Home, Basic, Advanced, Status, Admin, and Utility. Below the tabs, the title 'BASIC - STEP 2' is displayed in orange. Under the heading 'LAN:', there are four rows of input fields. The first row is 'IP Address:' with values 192, 168, 1, 1. The second row is 'Subnet Mask:' with values 255, 255, 255, 0. The third row is 'Gateway:' with values 192, 168, 1, 254. The fourth row is 'Host Name:' with the value SOHO. Under the heading 'WAN:', there are three rows of input fields. The first row is 'VPI:' with the value 0. The second row is 'VCI:' with the value 32. The third row is 'Encap:' with 'VC-mux' (unselected) and 'LLC' (selected). At the bottom of the form, there are four buttons: 'Back', 'Cancel', 'Reset', and 'Next'.

Enter IP: 192.168.1.1
Enter Subnet Mask: 255.255.255.0
Enter Gateway: 192.168.1.254
The Gateway IP is provided by ISP.
Enter Host Name: SOHO

Some ISPs will require the host name as identification. You may need to check with your ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

WAN1 Parameters

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

The screen will display the new parameters. Check the parameters and click **Restart**. The router will reboot with the new settings. Select **Continue** to configure other parameters.

Home

Basic

Advanced

Status

Admin

Utility

BASIC - REVIEW

REVIEW:

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

System Operation Mode:

System Mode	Bridge Mode
SHDSL Mode	GPE Side

LAN Interface:

IP Type	Fixed
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Hostname	SOHO

WAN1 interface:

VPI	0
VCI	32
AAL5 Encap.	LLC

Continue

Restart

7.2 Routing Mode

Routing mode includes DHCP server, DHCP client, DHCP relay, Point-to-Point Protocol over ATM and Ethernet and IP over ATM and Ethernet over ATM. The type of Internet protocol is provided by your ISP.

Click ROUTE and CPE Side then press Next.

The screenshot shows a configuration menu with tabs: Home, Basic, Advanced, Status, Admin, and Utility. Below the tabs, the text "BASIC - STEP1" is displayed in orange. Underneath, the "Operation Mode:" section contains two rows of radio button options: "System Mode:" with "ROUTE" selected and "BRIDGE" unselected; and "SHDSL Mode:" with "CO Side" unselected and "CPE Side" selected. At the bottom of the screen, there are three buttons: "Cancel", "Reset", and "Next".

Two SHDSL modes are available: CO, Central Office, and CPE, Customer Premises Equipment. For connection with a DSLAM, the SHDSL mode is CPE. For a LAN to LAN connection, one side must be CO and the other side must be CPE.

7.2.1 DHCP Client

Some ISPs provide a DHCP server service whereby the PC in the LAN can access IP information automatically. To setup the DHCP client mode, follow the procedure.

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

BASIC - STEP 2

LAN:

IP Type: Fixed Dynamic(DHCP Client)

IP Address: . . .

Subnet Mask: . . .

Host Name:

Trigger DHCP Service: Disable Server Relay

LAN IP Type:

Dynamic

Click Next to setup WAN1 parameters.

7.2.2 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a communication protocol that allows network administrators to centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Internet Protocol requires that each machine that can connect to the Internet has 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

Home	Basic	Advanced	Status	Admin	Utility									
BASIC - STEP 3														
DHCP SERVER:														
<ul style="list-style-type: none"> General DHCP Parameter: Start IP Address: 192.168.1. <input type="text" value="2"/> End IP Address: 192.168.1. <input type="text" value="51"/> DNS Server 1: <input type="text" value="192.168.1.1"/> DNS Server 2: <input type="text"/> DNS Server 3: <input type="text"/> Lease Time: <input type="text" value="72"/> hours Table of Fixed DHCP Host Entries: Hint: The format of the MAC Address is 12:34:56:78:9A:BC <table border="1"> <thead> <tr> <th>Index</th> <th>MAC Address</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table> 						Index	MAC Address	IP Address	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>
Index	MAC Address	IP Address												
1	<input type="text"/>	<input type="text"/>												
2	<input type="text"/>	<input type="text"/>												

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 entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically send a new IP address when a computer is plugged into a different place in the network. If the DHCP server is enabled, you have to setup the following parameters for processing DHCP requests from clients.

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

IP type:	Fixed
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Host Name:	SOHO Some ISPs require the host name as identification. Check with your ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

Trigger DHCP Service:

Server

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

For example: If the LAN IP address is 192.168.1.1, the IP range of LAN is 192.168.1.2 to 192.168.1.51. 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 legal IP address range is from 1 to 254. On the other hand, you cannot assign an IP greater than 254 or less than 1. Lease time 72 hours indicates that the DHCP server will reassign IP information every 72 hours.

DNS Server:

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

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

Click Next to setup WAN1 parameters.

7.2.3 DHCP relay

If you already have a DHCP server on your LAN and you want to use it for DHCP services, the router provides a DHCP relay function.

Home

Basic

Advanced

Status

Admin

Utility

BASIC - STEP 2

LAN:

IP Type: Fixed Dynamic(DHCP Client)

IP Address: . . .

Subnet Mask: . . .

Host Name:

Trigger DHCP Service: Disable Server Relay

Back

Cancel

Reset

Next

IP Type: Fixed

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Host Name: SOHO

Some ISPs require the host name as identification. Check with your ISP to see if your Internet service has been configured with a host name. In most cases, this field can be ignored.

Trigger DHCP Service: Relay

Home

Basic

Advanced

Status

Admin

Utility

BASIC - STEP 3

DHCP RELAY:

■ Remote DHCP Server Parameter:

IP address:

Back

Cancel

Reset

Next

Click Next to setup DHCP server parameters.

Enter the DHCP server IP address in IP address field.

Press Next

7.2.4 PPPoE or PPPoA

PPPoA (point-to-point protocol over ATM) and PPPoE (point-to-point protocol over Ethernet) are authentication and connection protocols used by many service providers for broadband Internet access. These are specifications for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. 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.

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

Before configuring the router, check with your ISP to ensure you have the correct information.



BASIC - STEP 4

WAN1:

VPI:

VCI:

AAL5 Encap: VC-mux LLC

Protocol:

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

Key in the WAN1 parameters:

VPI:	0
VCI:	33
AAL5 Encap:	LLC
Protocol:	PPPoA + NAT or PPPoE + NAT

Click Next to setup the User name and password.

For more information, refer to the section on NAT/DMZ.

Home	Basic	Advanced	Status	Admin	Utility
BASIC - STEP5					
ISP1:					
Username:	<input type="text" value="test"/>				
Password:	<input type="password" value="••••"/>				
Password Confirm:	<input type="password" value="••••"/>				
Idle Time:	<input type="text" value="10"/>	minutes			
IP Type:	<div style="border: 1px solid black; padding: 2px;"> Dynamic Fixed Unnumbered </div>				
IP Address:	<input type="text"/>				
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="Next"/>					

Type the ISP1 parameters.

Username: test
Password: test
Password Confirm: test

Your ISP will provide the user name and password.

Idle Time: 10

If you want your Internet connection to remain on at all times, enter 0 in the Idle Time field.

IP Type: There are three IP types, Dynamic, Fixed and IP Unnumbered, which you can setup. The default IP type is Dynamic. It means that ISP PPP server will provide IP information including a dynamic IP address when a SHDSL connection is established. I.e. you do not need to type the IP address of WAN1. Some ISPs will provide fixed IP address over PPP.

For fixed IP address:

IP Type: Fixed
IP Address: 192.168.1.1

Click Next.

For IP Unnumbered:

IP Type: IP Unnumbered
IP Address: 192.168.168.1

Click Next.

Don't forget to enable LAN: For IP Routing Usage and type IP address on STEP 2

Note: For security, the password will be displayed as asterisk characters.

The screen will display the parameters that will be written to EPROM. Check the parameters before writing to EPROM.

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

7.2.5 IPoA or EoA

Before configuring the router, check with your ISP to ensure you have the correct 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 information, refer to the section on NAT/DMZ.



WAN1:

IP Address:	<input type="text" value="10"/>	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="1"/>
Subnet Mask:	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Gateway:	<input type="text" value="10"/>	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="2"/>
DNS Server 1:	<input type="text" value="168.95.1.1"/>			
DNS Server 2:	<input type="text" value="168.95.192.1"/>			
DNS Server 3:	<input type="text"/>			



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

Click Next

The screen will display the parameters that will be written to EPROM. Check the parameters before writing to EPROM.

BASIC - REVIEW

REVIEW:

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

- System Operation Mode:

System Mode	Route Mode
SHDSL Mode	CPE Side

- LAN Interface:

IP Type	Fixed
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Hostname	SOHO
Trigger DHCP service	DHCP Server

- DHCP server:

Default gateway	192.168.1.1
Subnet mask	255.255.255.0
Start IP address	192.168.1.2
End IP address	192.168.1.51
DNS Server 1	192.168.1.1
DNS Server 2	
DNS Server 3	
Lease time	72 hours

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

8 Advanced Setup

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

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

8.1 SHDSL

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

Click SHDSL.

The following screen displays the Advanced SHDSL settings page for the NB712.

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

The NB714 supports an additional 4-wire mode with 4.0608Mbps data rate. The following screen displays the Advanced SHDSL settings page for the NB714 with the option to select the Link Type.

Annex Type:

There are three Annex types, Annex A (ANSI), Annex B (ETSI), or Annex AB in SHDSL. Check with your ISP.

Link Type:

The router supports two link types, 4-wire mode with 4.0608Mbps data rate and 2-wire mode with 2.304Mbps data rate.

Data Rate:

You can set the SHDSL data rate in multiples of 64kbps.

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

SHDSL SNR margin:

The margin range is from 0 to 10.

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 the SNR margin in the field to 2, the SHDSL connection will drop and reconnect when the SNR margin is lower than 2. I.e., the device will reduce the line rate and reconnect for better line connection.

The screen will display the parameters that will be written to EPROM. Check the parameters before writing to EPROM.

Home	Basic	Advanced	Status	Admin	Utility
ADVANCED - SHDSL					
SHDSL Parameters Review:					
To let the configuration that you have changed take effect immediately, please click Restart button to restart the setup procedure, please click Continue button.					
■ SHDSL Mode:					
Annex Type	Annex B				
Data Rate	0 (adaptive mode)				
SNR margin	0				
Continue Restart					

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

8.2 WAN

The SHDSL router supports up to 8 PVCs. WAN 1 was configured via BASIC except QoS. If you want to setup other PVCs, 2 to 8, the parameters are setup in WAN. I.e., you must apply two or more Internet Services with ISPs otherwise you do not need to setup WAN.

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



Enter the parameters.



WAN Interface Parameters:

Table of Current WAN Interface Parameter:

No	WAN	VC	ISP
1	Protocol: IP over ATM IP Address: 10.1.2.1 Subnet Mask: 255.255.255.0	VPI: 0 VCI: 32 AAL5 Encap: LLC QoS Class: UBR QoS PCR: 2400 QoS SCR: 2400 QoS MBS: 1	Username: test Password: **** Password Confirm: **** Idle Time: 10 IP Type: Dynamic
2	Protocol: Disable IP Address: 192.168.2.1 Subnet Mask: 255.255.255.0	VPI: 0 VCI: 33 AAL5 Encap: LLC QoS Class: UBR QoS PCR: 2400 QoS SCR: 2400 QoS MBS: 1	Username: test Password: **** Password Confirm: **** Idle Time: 10 IP Type: Dynamic

If the WAN protocol is PPPoA or PPPoE with dynamic IP, leave the default WAN IP address and Subnet Mask as default settings. The system will ignore the IP address and Subnet mask information but deleting or leaving blank the items will cause system error.

If the WAN protocol is IPoA or EoA, leave the ISP parameters as default setting. The system will ignore the information but deleting or leaving blank fields will cause a system error.

QoS (Quality of Service):	The Traffic Management Specification V4.0 defines ATM service catalogues that describe both the traffic transmitted by users onto a network as well as the Quality of Service that the network needs to provide for that traffic.
UBR (Unspecified Bit Rate):	UBR is the simplest service provided by ATM networks. There is no guarantee of any rate. It is a primary service used for transferring Internet traffic over the ATM network.
CBR (Constant Bit Rate):	CBR is used by connections that require a static amount of bandwidth that is available during the connection life time. This bandwidth is characterized by Peak Cell Rate. Based on the PCR of the CBR traffic, specific cell slots are assigned for the VC in the schedule table. The ATM always sends a single cell during the CBR connection's assigned cell slot.
VBR-rt (Variable Bit Rate real-time):	VBR-rt is intended for real-time applications, such as compressed voice over IP and video conferencing, that require tightly constrained delays and delay variation. VBR-rt is characterized by a peak cell rate (PCR), sustained cell rate (SCR), and maximum burst rate (MBR).
PCR (Peak Cell Rate) in kbps:	The maximum rate at which you expect to transmit data, voice and video. Consider PCR and MBS as a means of reducing latency, not increasing bandwidth. The range of PCR is 64kbps to 2400kbps
SCR (Sustained Cell Rate):	The sustained rate at which you expect to transmit data, voice and video. Consider SCR to be the true bandwidth of a VC and not the long-term average traffic rate. The range of SCR is 64kbps to 2400kbps.
MBS (Maximum Burst Size):	The amount of time or the duration at which the router sends at PCR. The range of MBS is 1 cell to 255 cells.

Click Finish to finish setting.

The screen will display the parameters that will be written to EPROM. Check the parameters before writing to EPROM.

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

8.3 Bridge

If your router is setup in bridge mode and you want to setup advanced filter functions, you can use the BRIDGE menu to setup the filter and blocking functions.

Click Bridge to setup.



Press Add to add the static bridge information.

Home Basic Advanced Status Admin Utility

ADVANCED - BRIDGE

Generic Bridge Parameters:

- General Parameter:
 - Default Gateway:

Static Bridge Parameters:

- Table of Current MAC Entries:

No	MAC Address	LAN	WAN1 - 4	WAN5 - 8
1	<input type="text" value="00:00:00:00:00:00"/>	Filter	1 Filter	5 Filter
			2 Filter	6 Filter
			3 Filter	7 Filter
			4 Filter	8 Filter
		<input type="button" value="Reset"/>	<input type="button" value="Add"/>	

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

If you want to filter the MAC address of WAN PC to access the LAN, press Add to establish the filtering table. Enter the MAC address in the MAC address field and select Filter in the WAN field. For example: if your VC is setup at WAN 1, select WAN 1 Filter.

The screen will display the parameters that will be written to EPROM. Check the parameters before writing to EPROM.

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

ADVANCED - BRIDGE

Bridge Parameters Review:
To let the configuration that you have changed take effect immediately, please click **Restart** button to reboot the system. If you want to continue the setup procedure, please click **Continue** button.

- **Generic Bridge Parameter:**

Default Gateway	192.168.1.254
-----------------	---------------
- **Static Bridge Parameter:**

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

[Continue](#) [Restart](#)

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

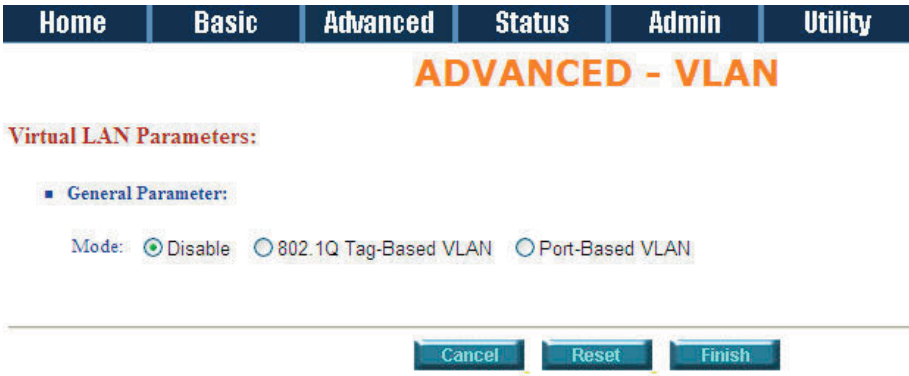
8.4 VLAN

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

Click VLAN to configure VLAN.



Two types of VLAN are supported: either 802.1Q or Port-Based. Note that only one type of VLAN can be configured at a time.



For setting 802.1Q VLAN click the 802.1Q Tag-Based VLAN and click Reset. The screen will display as follows:

Home Basic Advanced Status Admin Utility

ADVANCED - VLAN

Virtual LAN Parameters:

• **General Parameter:**

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

• **802.1Q Tag-Based VLAN Table:**

No	VID	LAN1	LAN2	LAN3	LAN4	VLAN1	VLAN2	VLAN3	VLAN4	VLAN5
1	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PVID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Link Type	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access

Cancel Reset Apply

- VID:** Virtual LAN ID is a defined ID number from 1 to 4094.
- PVID:** Port VID is an untagged member of a default VLAN.
- Link Type:** **Access** means the port can receive or send **untagged** packets.
- Link Type:** **Trunk** means that the port can receive or send **tagged** packets.

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

Click Port-Based VLAN to configure the router and press Reset.

Home Basic Advanced Status Admin Utility

ADVANCED - VLAN

Virtual LAN Parameters:

• **General Parameter:**

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

• **802.1Q Tag-Based VLAN Table:**

No	VID	LAN1	LAN2	LAN3	LAN4	VLAN1	VLAN2	VLAN3	VLAN4	VLAN5
1	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PVID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Link Type	Access	Access	Access	Access	Access	Access	Access	Access	Access	Access

Cancel Reset Apply

8.5 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 physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the least 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



Home
Basic
Advanced
Status
Admin
Utility

■ General RIP Parameters:

RIP Mode: Disable Enable

Auto RIP Summary: Disable Enable

■ Table of Current Interface RIP Parameter:

Interface	RIP Mode	Version	Authentication Required	Poison Reverse	Authentication Code
<input checked="" type="radio"/> LAN	Disable	2	None	Enable	None
<input type="radio"/> WAN1	Disable	2	None	Enable	None
<input type="radio"/> WAN2	Disable	--	None	Disable	None
<input type="radio"/> WAN3	Disable	--	None	Disable	None
<input type="radio"/> WAN4	Disable	--	None	Disable	None
<input type="radio"/> WAN5	Disable	--	None	Disable	None
<input type="radio"/> WAN6	Disable	--	None	Disable	None
<input type="radio"/> WAN7	Disable	--	None	Disable	None
<input type="radio"/> WAN8	Disable	--	None	Disable	None

Press Modify

RIP Mode:

This parameter determines how RIP (Routing Information Protocol) is handled. 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 incorporates RIP broadcasts by other routers into its routing table. If set to silent, the router does not broadcast the routing table, but it accepts RIP broadcast packets that it receives.

RIP Version:

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

RIP v1: it only sends RIP v1 messages only.

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

Authentication required:

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

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

MD5: The RIP will be decoded by MD5 rather than be protected by password, authentication code.

Poison Reverse:

Poison Reverse promptly broadcasts or multicasts the RIP while the route is changed. (e.g. shutting down one of the routers in routing table)

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

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

After modifying the RIP parameters, press finish.

The screen will display the modified parameters. Check the parameters and press Restart to restart the router or press Continue to setup other parameters.

8.6 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 and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP address and changes 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 the number of global IP addresses that a company needs and lets the company 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 private network and the outside public network. It prevents outside users from getting direct access to a server that has company private data.

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

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - NAT/DMZ

Network Address Translation and DMZ Hosts Parameters:

- **NAT DMZ Feature:**
 NAT DMZ Feature: Enable Disable
- **DMZ Host:**
 DMZ Host Feature: Enable Disable
 Virtual IP Address:
 Access Protocol: WAN1
- **Multi DMZ:**

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

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

Cancel
OK
Help

In a typical DMZ configuration for an enterprise, a separate computer or host receives requests from users within the private network to access 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 uses the IP address assigned to the WAN for enabling DMZ functions for the virtual IP address.

Multi-DMZ:	Some users who have two or more global IP addresses assigned by their ISP can be used as a multi DMZ. The table is for the mapping of global IP address and virtual IP address.
Multi-NAT:	Some of the virtual IP addresses (e.g.: 192.168.1.10 ~ 192.168.1.50) collectively use two of the global IP addresses (e.g.: 69.210.1.9 and 69.210.1.10). The Multi-NAT table will be setup as;
Virtual Start IP Address:	192.168.1.10
Count:	40
Global Start IP Address:	69.210.1.9
Count:	2

Press Finish to continue.

The screen will display the parameters that will be written to EPROM. Check the parameters before writing to EPROM. Press Restart to restart the router with new parameters or Continue to configure other parameters.

8.7 Virtual Server

Virtual Server allows specific ports on the WAN interface to be re-mapped to services inside the LAN. For example, 69.210.1.8 is assigned to WAN by the ISP and is visible to the Internet but does not actually have any services (other than NAT) running on the gateway. TCP requests made to 69.210.1.8:80 are remapped to the server 1 on 192.168.1.2:80 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 192.168.1.3:25 which is always on.

You can setup the router as Index 1, protocol TCP, interface WAN1, service name test1, private IP 192.168.1.2, 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 192.168.1.3, private port 25, public port 25, schedule always.

Click Modify to configure the parameters.

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

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

ADVANCED - VIRTUAL SERVER

Virtual Server Mapping Parameters:

■ **Virtual Server 1:**

Protocol:

Interface:

Service Name:

Private IP:

Private Port:

Public Port:

Schedule: Always

From Day to

Time : to :

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

8.8 Firewall

A firewall is a set of related programs that protect the resources of a private network from other networks. It prevents unauthorised users from accessing private data and resources accidentally.

Basic Firewall Security



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

Press Finish to finish setting up the firewall. The screen will display the parameters, which will be written to EPROM. Check the parameters.

Press restart to restart the router or press continue to setup another function.



Automatic Firewall Security



Select Automatic Firewall Security. This level enables basic firewall security as well as all DoS protection and the SPI filter function. Press Finish to finish setting up the firewall.

The screen will display the parameters, which will be written to EPROM. Check the parameters.



DoS Protection Parameters Review:

Detect SYN Attack	Enable	SYN Attack Threshold 200 packets per second
Detect ICMP Flood	Enable	ICMP Flood Threshold 200 packets per second
Detect UDP Flood	Enable	UDP Flood Threshold 200 packets per second
Detect PING of Death Attack	Enable	-----
Detect Land Attack	Enable	-----
Detect IP Spoofing Attack	Enable	-----
Detect Smurf Attack	Enable	-----

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

Advanced Firewall Security

You can determine the security level for special purpose, environment, and applications by configuring DoS protection and defining an extra packet filter with higher priority than the default SPI filter. Note that an improper filter policy may degrade the capability of the firewall and/or even block the normal network traffic.



Click Advanced Firewall Security and then press Finish.



SYN Attack:

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

ICMP Flood:

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

UDP Flood:

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

Ping of Death:

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

Land Attack:

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

IP Spoofing:

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

Smurf Attack:

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

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



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

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

PKT FILTER - RULE 1

Packet Filter Rule Parameters:

- Filter Rule:
 - Protocol: ANY
 - Direction: INBOUND OUTBOUND
 - Action: DENY PERMIT
 - Description:
 - Src. IP Address: e.g., Any:0.0.0.0, Single:10.0.0.1
 - Dest. IP Address: Range:192.168.0.1-192.168.0.76
 - Schedule: Always
 - From Day: Sunday to Saturday
 - Time: 00:00 to 23:59

Buttons: Back, Cancel, OK

Select the protocol and configure the parameters.

If you want to ban all of the protocol from the IP (e.g.: 200.1.1.1) to access the all PCs (e.g.: 192.168.1.2 ~ 192.168.1.50) in the LAN, key in the parameter as;

- Protocol:** ANY
- Direction:** INBOUND (INBOUND is from WAN to LAN, and OUTBOUND is LAN to WAN.)
- Description:** Hacker
- Src. IP Address:** 200.1.1.1
- Dest. IP Address:** 192.168.1.2-192.168.1.50

Press OK to finish.

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

FIREWALL - PKT FILTER

Packet Filtering Parameters:

- General Packet Filtering Parameters:
 - Trigger Packet Filtering Service: Disable Enable
 - Deep Inspected Packets: Disable Enable
- Access Policies:

Index	Enable	Protocol	Direction	Action	Source	Destination	TCP Flag	ICMP Type	Schedule	Description
1	ON	ANY	Inbound	Permit	200.1.1.1	192.168.1.2-192.168.1.50	--	--	Always	Hacker

Buttons: Back, Exchange, Modify, Delete, Add, Total

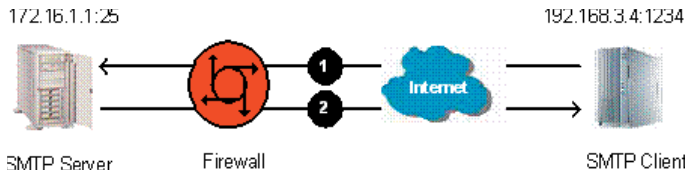
Click Restart to restart the gateway or Continue to configure another parameters.

Filtering Rule for SMTP connection

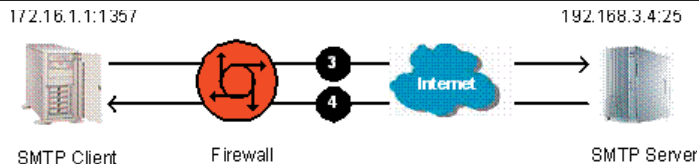
Filtering rule will be configured as follow

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

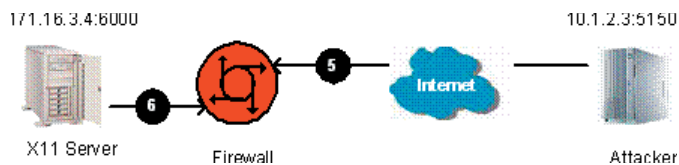
Packet	Direction	Source	Destination	Protocol	Dest. Port	Action (Rule)
1	Inbound	192.168.3.4	172.16.1.1	TCP	25	Permit (A)
2	Outbound	172.16.1.1	192.168.3.4	TCP	1234	Permit (B)



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



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



Update Filtering Rule

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

Filtering Result

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

Rule Order

The order of the rules affects the filtering result. The filtering process will proceed from top to bottom, changing the order will give a different result. For example:

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

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

When the rule is ordered as ABC.

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

The rule order will permit 10.1.99.1 to access 172.16.6.1.

When the rule is ordered as BAC.

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

The rule order will deny 10.1.99.1 to access 172.6.6.1.

8.9 IP QoS

IP QoS allows you to prioritise different types of traffic, thereby ensuring Quality of Service. This is particularly useful for Voice over IP (VoIP) where the amount of bandwidth can affect the line quality in a phone call.

Select Enable to enable IP QoS and then click on the Add button to set the IP QoS Policy parameters.

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

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - IP QoS

IP QoS Parameters:

▪ General IP QoS Parameters:

Trigger IP QoS Service: Disable Enable

▪ IP QoS Policies:

Index	Enable	Protocol	Local	Remote	Precedence	Description
Pool is Empty !						

Cancel
Add
Finish

Enter the information to define the Policy Rule and click on the OK button.

Home
Basic
Advanced
Status
Admin
Utility

IP QoS - POLICY 1

IP QoS Policy Parameters:

▪ Policy Rule:

Description:

Local IP: e.g., Any:0.0.0.0, Single:10.0.0.1

Remote IP: Range:192.168.0.1-192.168.0.76

Local Port: e.g., Any:0-65535, Single:80

Remote Port: Range:1024-5050

Protocol: ANY ▼

Precedence: 0 ▼

Back
Ok

The screen will display the configured parameters. Check the parameters. In this example 192.168.1.60 is the highest priority; 192.168.1.50 is the second high priority; 192.168.1.40 is the third highest priority and so on.

Home
Basic
Advanced
Status
Admin
Utility

ADVANCED - IP QoS

IP QoS Parameters:

- General IP QoS Parameters:**
 Trigger: IPQoSService: Disable Enable
- IP QoS Policies:**

Index	Enable	Protocol	Local	Remote	Precedence	Description
1	ON	ANY	192.168.1.10 0-255.35	0.0.0.0 0-255.35	0	priority 6
2	ON	ANY	192.168.1.20 0-255.35	0.0.0.0 0-255.35	1	priority 5
3	ON	ANY	192.168.1.30 0-255.35	0.0.0.0 0-255.35	2	priority 4
4	ON	ANY	192.168.1.40 0-255.35	0.0.0.0 0-255.35	3	priority 3
5	ON	ANY	192.168.1.50 0-255.35	0.0.0.0 0-255.35	4	priority 2
6	ON	ANY	192.168.1.60 0-255.35	0.0.0.0 0-255.35	5	priority 1

Cancel Modify Delete Add Finish

9 Administration

This section details security, simple network management protocol (SNMP) and time synchronous.

- ▶ **BASIC**
- ▶ **ADVANCED**
- ▶ **STATUS**
- ▼ **ADMIN**
 - SECURITY
 - SNMP
 - TIME SYNC
- ▶ **UTILITY**

9.1 Security

For system security, it is suggested that the default user name and password is changed from the default.

There are three ways to configure the route: Web browser, telnet and serial console.

Press Security to setup the parameters.

For greater security, define the Supervisor ID and password for the gateway. If you don't set them, all users on your network will be able to access the gateway.

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



ADMIN - SECURITY

Supervisor Profile and Security Parameters:

■ Supervisor ID and Password:

Supervisor ID:

Supervisor Password:

Password Confirm:

■ User Profile:

ID	User Name	User Password	Password Confirm	UI Mode
1	<input type="text" value="admin"/>	<input type="password" value="••••"/>	<input type="password" value="••••"/>	Menu <input type="button" value="v"/>
2	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command <input type="button" value="v"/>
3	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command <input type="button" value="v"/>
4	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command <input type="button" value="v"/>
5	<input type="text"/>	<input type="password"/>	<input type="password"/>	Command <input type="button" value="v"/>

■ General Parameters:

Telnet Port:

Trusted Host address pool will setup the IP addresses from which authorized users can configure the gateway. This is the most secure way to setup and control authorised access to the router.

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

Leaving blank the Trust Host List will block all PCs from WAN to access the router. I.e. only PCs on the LAN would be able to access the router.

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

Home Basic **Advanced** Status Admin Utility

- Remote Management Host:
Modify legal management IP address. Note, an empty pool defaults to a security level that would allow any host in LAN but deny all connections from WAN side. A 0.0.0.0 entry in the pool will allow all management including the Internet.

ID	IP Address
1	0.0.0.0
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Cancel Reset Finish

Click Finish to finish the setting.

The browser will display the configured parameters and check it before writing them to EPROM.

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

9.2 SNMP

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

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

Click SNMP to configure the parameters.

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

- ▶ BASIC
- ▶ ADVANCED
- ▶ STATUS
- ▼ ADMIN
 - SECURITY
 - **SNMP**
 - TIME SYNC
- ▶ UTILITY

Home
Basic
Advanced
Status
Admin
Utility

ADMIN - SNMP

SNMP Community and Trap Parameters:

■ **Table of current community pool:**

Index	Status	Access Right	Community
<input checked="" type="radio"/> 1	Disable	---	---
<input type="radio"/> 2	Disable	---	---
<input type="radio"/> 3	Disable	---	---
<input type="radio"/> 4	Disable	---	---
<input type="radio"/> 5	Disable	---	---

■ **Table of current trap host pool:**

Index	Version	IP Address	Community
<input checked="" type="radio"/> 1	Disable	---	---
<input type="radio"/> 2	Disable	---	---
<input type="radio"/> 3	Disable	---	---
<input type="radio"/> 4	Disable	---	---
<input type="radio"/> 5	Disable	---	---

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

Click on the Modify button to modify the community pool.

SNMP Community and Trap Parameters:

Table of current community pool:

Index	Status	Access Right	Community
1	Disable	Deny	private
2	Disable	---	---
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

SNMP status: Enable

SNMP Community and Trap Parameters:

Table of current community pool:

Index	Status	Access Right	Community
1	Disable	Deny	private
2	Disable	---	---
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

Access Right: Deny for deny all access

Access Right: Read for access read only

Access Right: Write for access read and write.

Community: Serves as password for access right.

Click on the OK button to submit the changes.

Table of current trap host pool:

Index	Version	IP Address	Community
1	Disable	192.168.1.254	private
2	Disable	---	---
3	Version 1 Version 2	---	---
4	Disable	---	---
5	Disable	---	---

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

- | | |
|-------------------|------------------------------------------------------------------------|
| Version: | Select version for trap host (SNMP v1 or SNMP v2). |
| IP: | Type the trap host IP |
| Community: | Type the community password. The community is setup in community pool. |

Click on OK to finish the setup.

The browser will display the configured parameters.

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

9.3 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 can vary and cause firewall packet filtering schedule processes to fail, security to be compromised, and virtual servers to work in wrong schedule.

Click on TIME SYNC.

There are two synchronization modes: Simple 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.

- ▶ BASIC
- ▶ ADVANCED
- ▶ STATUS
- ▼ ADMIN
 - SECURITY
 - SNMP
 - TIME SYNC
- ▶ UTILITY

Home	Basic	Advanced	Status	Admin	Utility
ADMIN - TIME SYNC					
Time Synchronization:					
<ul style="list-style-type: none"> ■ SYNC method: <ul style="list-style-type: none"> Sync with PC ▼ SNTP v4.0 Sync with PC ■ Synchronization with client: <input type="text" value="System Time: 2002/01/01 00:24:33 (GMT+8:00)"/> <input type="button" value="Sync Now"/> 					

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 to ensure the ultimate performance of full NTP implementation.

Home	Basic	Advanced	Status	Admin	Utility
ADMIN - TIME SYNC					
Time Synchronization:					
<ul style="list-style-type: none"> ■ SYNC method: <ul style="list-style-type: none"> SNTP v4.0 ▼ ■ Simple network time protocol: <p>Service: <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Time Server 1: <input type="text" value="ntp-2.vt.edu"/></p> <p>Time Server 2: <input type="text" value="ntp.drydog.com"/></p> <p>Time Server 3: <input type="text" value="ntp1.cs.wisc.edu"/></p> <p>Time Zone: <input style="background-color: #0070C0; color: white;" type="text" value="GMT(+10:00) CANBERRA, MELBOURNE, SYDNEY"/></p> <p>Update Period (secs): <input type="text" value="3600"/></p> 					
<input type="button" value="Cancel"/> <input type="button" value="Reset"/> <input type="button" value="Finish"/>					

For SNTP, select SNTP v4.0.

SNTP service: Enable

Time Server: Any time server in the world can be used but it is suggested that you use the nearest timeserver.

Time Zone: You have to choose the right time zone.

Click on Finish to finish the setup. The browser will display the configured parameters.

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

10 Utility

This section describes the utility of the router including system information, loading the factory default configuration, upgrading the firmware, logout and restarting the gateway.

- ▶ **BASIC**
- ▶ **ADVANCED**
- ▶ **STATUS**
- ▶ **ADMIN**
- ▼ **UTILITY**
 - SYSTEM INFO
 - CONFIG TOOL
 - UPGRADE
 - LOGOUT
 - RESTART

10.1 System Info

Click on System Info to review the information.

The browser will display your system information on the screen.

- ▶ BASIC
- ▶ ADVANCED
- ▶ STATUS
- ▶ ADMIN
- ▼ UTILITY
 - SYSTEM INFO
 - CONFIG TOOL
 - UPGRADE
 - LOGOUT
 - RESTART

Home
Basic
Advanced
Status
Admin
Utility

UTILITY - SYSTEM INFO

General System Information:

Product Model	NB712
MCSV	145B-0000-15309D71
Software Version	145B-0000-2040EB3E
Chipset	G2237-108-041GT
Firmware Version	R3.0.5
Host Name	SOHO
System Time	2002/01/01 00:29:09 (GMT+8:00)
System Up Time	0DAY/0HR/29MIN

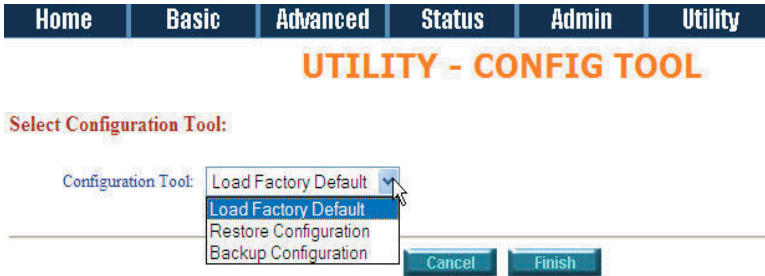
Finish
Refresh
Help

10.2 Config Tool

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

Press Config Tool.

Choose the function and then click on Finish.



Load Factory Default function:

Will reload the factory default parameters to the gateway.

Note: All of the settings will be changed to factory default. On the other hand you will lose all the configured parameters.

Restore Configuration:

Will help you to recover your backup configuration:

- * Click Finish after selecting Restore Configuration.
- * Browse the router for the backup file and then click Finish. The router will automatically restore the saved configuration.

Backup Configuration:

Any changes to the default configuration should be backed up. Use this function to backup your router parameters on a PC.

- * Select Backup Configuration and then press Finish.
- * Browse the place of backup file named backup. Press Finish. The router will automatically backup the configuration.

10.3 Upgrade

You can upgrade the gateway using the upgrade function.

Press Upgrade.

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

- ▶ BASIC
- ▶ ADVANCED
- ▶ STATUS
- ▶ ADMIN
- ▼ UTILITY
 - SYSTEM INFO
 - CONFIG TOOL
 - **UPGRADE**
 - LOGOUT
 - RESTART

Home Basic Advanced Status Admin Utility

UTILITY - FIRMWARE UPGRADE

Firmware Upgrade:
Please select the firmware file that you want, and press Ok button to upgrade the system, then the system will restart automatically.

Browse

Cancel OK

10.4 Logout

To logout the router, press logout.

- ▶ BASIC
- ▶ ADVANCED
- ▶ STATUS
- ▶ ADMIN
- ▼ UTILITY
 - SYSTEM INFO
 - CONFIG TOOL
 - UPGRADE
 - **LOGOUT**
 - RESTART

10.5 Restart

To restart the router, select Restart in UTILITY.

Click on the Restart button to reboot the router.

- ▶ BASIC
- ▶ ADVANCED
- ▶ STATUS
- ▶ ADMIN
- ▼ UTILITY
 - SYSTEM INFO
 - CONFIG TOOL
 - UPGRADE
 - LOGOUT
 - **RESTART**



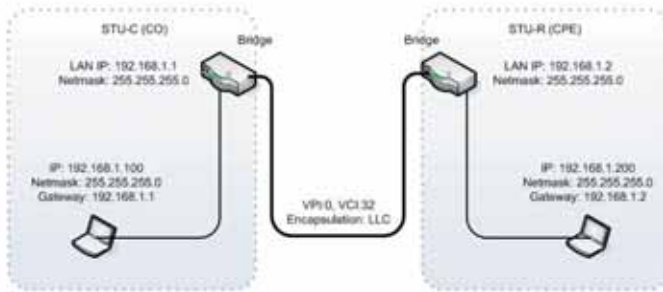
11 Status

You can monitor the following:

- SHDSL status including mode, Tx power, 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.
- Route status will display the routing table of router.
- Interface status includes LAN and WAN statistics information.
- Firewall status display DoS protection status and dropped packets statistics.

- ▶ **BASIC**
- ▶ **ADVANCED**
- ▼ **STATUS**
 - SHDSL
 - LAN
 - WAN
 - ROUTE
 - INTERFACE
 - FIREWALL
 - IP QoS
- ▶ **ADMIN**
- ▶ **UTILITY**

12 LAN-to-LAN connection with bridge Mode



12.1 CO side

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

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

LAN Parameters

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

Enter IP:	192.168.1.1
Enter Subnet Mask:	255.255.255.0
Enter Gateway:	192.168.1.1
Enter Host Name:	SOHO

WAN1 Parameters

Enter VPI:	0
Enter VCI:	32
Encap:	Click LLC

Click Next

The screen will display the configured parameters. Check the parameters and click Restart . The router will reboot with the new settings.

12.2 CPE Side

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

Home Basic Advanced Status Admin Utility

BASIC - STEP 1

Operation Mode:

System Mode: ROUTE BRIDGE

SHDSL Mode: CO Side CPE Side

Cancel Reset Next

LAN Parameters

Home Basic Advanced Status Admin Utility

BASIC - STEP 2

LAN:

IP Address: 192 168 1 2

Subnet Mask: 255 255 255 0

Gateway: 192 168 1 2

Host Name: SOHO

WAN1:

VPI: 0

VCI: 32

Encap: VC-mux LLC

Back Cancel Reset Next

IP Address: Enter 192.168.1.2

Subnet Mask: Enter 255.255.255.0

Gateway: Enter 192.168.1.2

Host Name: Enter SOHO

WAN1 Parameters

VPI: 0

VCI: 32

Encap: LLC

Click Next

The screen will display the configured parameters. Check the parameters and click Restart . The router will reboot with the new settings.

13 LAN to LAN Connection with Routing Mode

13.1 CO side

Click ROUTE and CO Side then press Next.

Home | **Basic**

BASIC - STEP 1

Operation Mode:

System Mode: ROUTE BRIDGE

SHDSL Mode: CO Side CPE Side

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.

Home | **Basic**

BASIC - STEP 2

LAN:

IP Type: Fixed Dynamic(DHCP Client)

IP Address: 192 | 168 | 20 | 1

Subnet Mask: 255 | 255 | 255 | 0

Host Name: SOHO

Trigger DHCP Service: Disable Server Relay

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.

Refer to the section NAT/DMZ for more information.

IP Address: 192.168.30.1

Subnet mask: 255.255.255.0

Gateway: 192.169.30.2

Click Next

The screen will display the parameters that will be written to EPROM. Check the parameters before writing to EPROM.

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

13.2 CPE side

Click ROUTE and CPE Side then press Next.

Home | **Basic**

BASIC - STEP 1

Operation Mode:

System Mode: ROUTE BRIDGE
SHDSL Mode: CO Side CPE Side

Cancel Reset Next

LAN parameters:

Home | **Basic**

BASIC - STEP 2

LAN:

IP Type: Fixed Dynamic(DHCP Client)
IP Address: 192 . 168 . 10 . 1
Subnet Mask: 255 . 255 . 255 . 0
Host Name: SOHO
Trigger DHCP Service: Disable Server Relay

Back Cancel Reset Next

- IP Address:** 192.168.10.1
- Subnet Mask:** 255.255.255.0
- Host Name:** SOHO
- DHCP Service:** For more DHCP service, review DHCP Service.

WAN Parameters

Home | **Basic**

BASIC - STEP 4

WAN1:

VPI: 0
VCI: 32
AAL5 Encap: VC-mux LLC
Protocol: IPoA

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

Back Cancel Reset Next

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.

Refer to the section NAT/DMZ for more information.

IP Address:	192.168.30.2
Subnet mask:	255.255.255.0
Gateway:	192.168.30.1

Click Next

The screen will display the parameters that will be written to EPROM. Check the parameters and click the Restart button to restart the router with the new parameters or press continue to setup other parameters.

14 Configuration via Serial Console or Telnet with Menu Driven Interface

14.1 Serial Console

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

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

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

Note: You have to use the SPACE key. Pressing other keys will not work.

User: admin
Password: *****

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

14.2 Telnet

Make sure the correct Ethernet cable is used to connect the LAN port of your computer to the Router. The LAN LNK indicator on the front panel will glow if the correct cable is used. Start your Telnet client with a VT100 terminal emulation and connect to the management IP of Router. When the login screen appears enter your User name and Password.

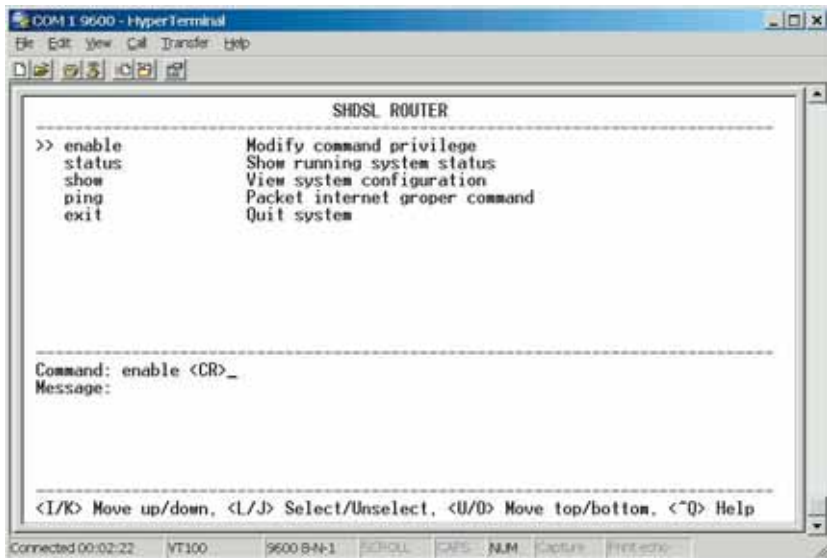
User: admin
Password: *****

Note: The default IP address is 192.168.1.1.

14.3 Operation Interface

For serial console and Telnet management, the Router implements two operational interfaces: command line interface (CLI) and menu driven interface. The CLI mode provides users with a simple command line interface. The menu driven interface is a more user-friendly interface for general operations. The command syntax for CLI is the same as that of the menu driven interface. The only difference is that the menu driven interface displays all available commands for you to select. This means that you don't need to remember the command syntax and can save you time by not requiring you to type the whole command line.

The following figure gives you an example of the menu driven interface. In the menu, you scroll up/down by pressing key I / K, select one command by key L, and go back to a higher level of menu by key J. For example, to show the system information, just logon to the Router, move down the cursor by pressing key K twice and select "show" command by pressing key L, you shall see a submenu and select "system" command in this submenu, then the system will display the general information.



14.4 Window structure

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

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

The following table shows the parameters in the brackets.

Command	Description
<ip>	An item enclosed in brackets is required. If the item is shown in lower case bold, it represents an object with special format. For example, <ip> may be 192.168.1.3.
<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.

14.5 Menu Driven Interface Commands

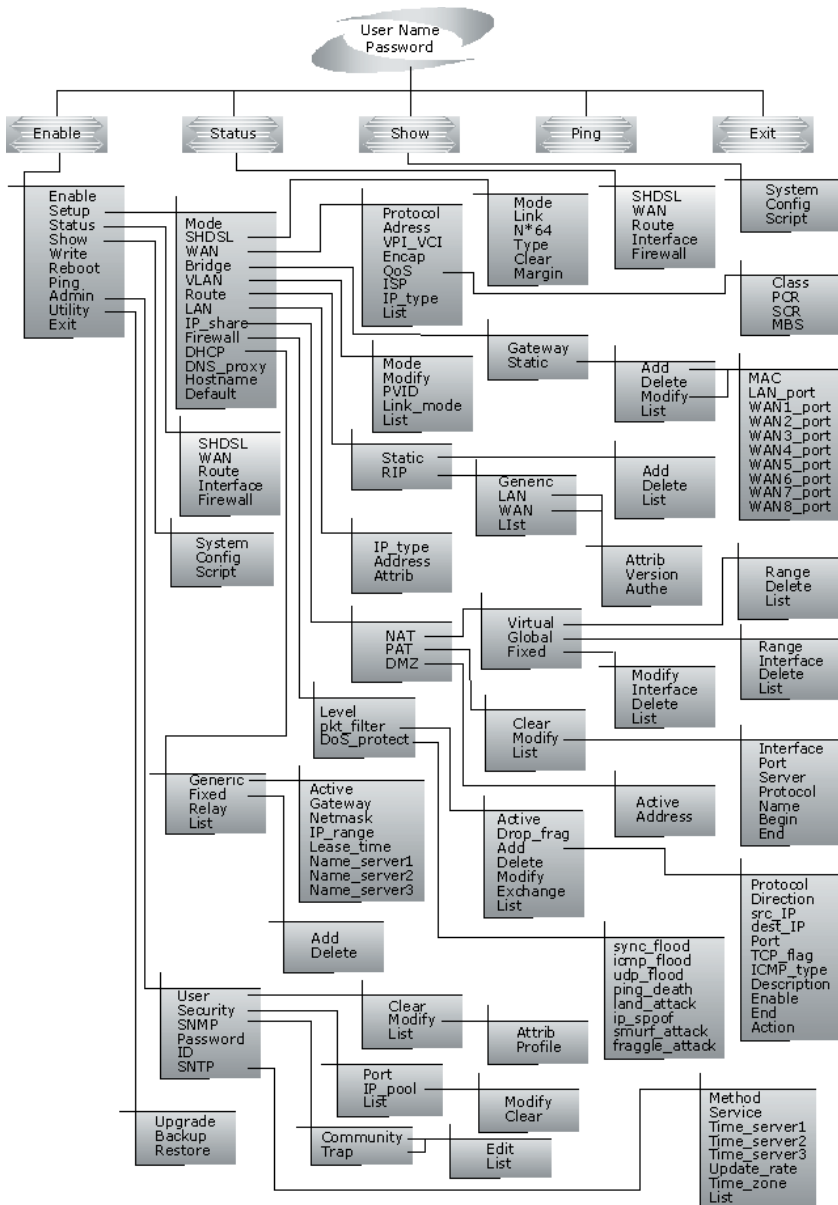
Before changing the configuration, familiarize yourself with the operations list in the following table. The Keystroke list are also displayed on the window.

Menu Driven Interface Commands

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

14.6 Menu Tree

The menu tree is shown below. All configuration commands are included in the Enable directory and are protected by a supervisor password. Unauthorized users can view the status and configuration of the router, but cannot change any configuration information.



14.7 Configuration

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 admin. The password will be prompted as a “ * ” 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.

Any changes will need to be written to EPROM and the router will need to be rebooted to work with 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 proper command
   admin       Setup management features
   utility     TFTP upgrade utility
   exit        Quit system
```

The description of the commands are:

Command	Description
enable	Modify command privilege. When you login via serial console or Telnet, the router defaults to a program execution (read-only) privileges. To change the configuration and write changes to nonvolatile RAM (NVRAM), you must work in enable mode.
setup	To configure the product, you have to use the setup command.
status	View the status of product.
show	Show the system and configuration of product.
write	Update flash configuration. After you have completed all necessary settings, write the new configuration to NVRAM by the “write” command and reboot the system, or all of your changes will not take effect.
reboot	Reset and boot system. After you have completed all necessary changes, write the new configuration to NVRAM and reboot the system by “reboot” command, or all of your changes will not take effect.

Command	Description
ping	Packet internet groper command.
admin	You can set management features with this command.
utility	Upgrade software and backup and restore configuration are done via “utility” command.
exit	Quit system

14.8 Status

You can view the 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
firewall    Show firewall status
```

Command	Description
shdsl	The SHDSL status includes line rate, SNR margin, TX power, attenuation and CRC error of the product, and SNR margin, attenuation and CRC error of remote side. The product access remote side information via EOC (embedded operation channel).
wan	WAN status shows the 8 PVC information which are configured.
route	You can see the routing table via the route command.
interface	The statistic status of WAN and LAN interface can be monitor by interface command.
firewall	The current and history status of firewall are shown in this command.

14.9 Show

You can view the system information, configuration and configuration via 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
```

Command	Description
system	The general information of the system is displayed.
config	Config command displays detailed configuration information.
script	Configuration information will display in the command script.

14.10 Write

Any changes to the router configuration must be written to EPROM using the write command and the router needs to be rebooted for the changes to take affect.

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

```
-----  
Command: write <CR>  
Message: Please input the following information.  
Are you sure? (y/n): y  
-----
```

14.11 Reboot

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

```
-----  
Command: reboot <CR>  
Message: Please input the following information.  
Do you want to reboot? (y/n): y  
-----
```

14.12 Ping

Ping command will be used to test the connection of the router. Move cursor " >> " to ping and press enter.

```
-----  
Command: ping <ip> [1~65534|-t] [1~1999]  
Message: Please input the following information.  
IP address <IP> : 10.0.0.1  
Number of ping request packets to send (TAB select): -t  
Data size [1~1999]: 32  
-----
```

There are 3 types of number of ping request packet to send, default, 1~65534 and -t. Default will send 4 packet and -t continuous packet until you key in Ctrl+c to stop.

14.13 Administration

You can modify the user profile, telnet access, SNMP (Sample Network Management Protocol), supervisor information and SNTP (Simple Network Time Protocol) in admin. The route is enable ==> admin.

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

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

14.13.1 User Profile

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

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

You can delete the user by number using the clear command. Make sure the number of the user is correct. You can use list command to check it. Modify command is to modify any user information or add a new user to user profile.

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

```
-----
Command: admin user modify <1~5> <more...>
Message: Please input the following information.
Legal access user profile number <1~5> : 2
-----
```

The screen will prompt as follow.

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

There are two UI mode, command and menu mode, to setup the product. We will not discuss command mode in this manual.

14.13.2 Security

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

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

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

14.13.3 SNMP

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

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

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

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

Up to 5 SNMP community entries can be configured in this system. Move the cursor to community and press enter.

```
-----
Command: admin snmp community <1~5> <more...>
Message: Please input the following information.
Community entry number <1~5> : 2
-----
```

The screen will prompt as follow:

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

Up to 5 SNMP trap entries can be configured in this system. Move the cursor to trap and press enter.

```
-----
Command: admin snmp trap <1~5> <more...>
Message: Please input the following information.
Trap host entry number <1~5> : 2
-----
```

The screen will prompt as follow:

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

14.13.4 Supervisor Password and ID

The supervisor password and ID are the last door for security but the most important. Users who access the router via web browser have to use the ID and password to configure the router and users who access the router via telnet or console mode have to use the password to configure the router. Change the ID and password after configuration and save it. When you access to the router again, you have to use the new password.

```
-----  
Command: admin passwd <pass_conf>  
Message: Please input the following information.  
Input old Supervisor password: ****  
Input new Supervisor password: ****  
Re-type Supervisor password: ****  
-----  
Command: admin id <pass_conf>  
Message: Please input the following information.  
Legal user name (Enter for default) <root> : test  
-----
```

14.13.5 SNTP

Time synchronization is an essential element for any business that relies on an IT system. The reason for this is that these systems all have clocks that are the source of time for files or operations they handle. Without time synchronization, time on these systems can vary 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 a PC or SNTPv4. If you choose synchronize with PC, the router will synchronize with a PC. If you choose SNTPv4, the router will use the protocol to synchronize with the time server. Synchronization with time server, SNTP v4, needs to configure service, time_server and time_zone. Synchronization with PC does not require the above parameters.

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

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

To configure SNTP v4 time synchronization, follow the procedures detailed 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 <Disable|Enable>
Message: Please input the following information.
Active SNTP v4.0 service (Tab Select) <Enable> : Enable
-----
```

Move the cursor to time_server1 and press enter.

```
-----
Command: admin sntp time_server1 <string>
Message: Please input the following information.
Time server address(Enter for default) <ntp-2.vt.edu> : ntp-2.vt.edu
-----
```

You can configure up to three time servers in this system.

Move the cursor to update_rate and press enter.

```
-----
Command: admin sntp update_rate <10~268435455>
Message: Please input the following information.
Update period (secs) (Enter for default) : 86400
-----
```

Move the cursor to `time_zone` and configure where your router is placed. The easiest way to know the time zone offset hour is from your PC clock. Double click the clock at the right corner of monitor and check the time zone.

```
-----  
Command: admin sntp time_zone <-12~12>  
Message: Please input the following information.  
GTM time zone offset (hours) (Enter for default) : -8  
-----
```

Move the cursor to list and review the setting.

14.14 Utility

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

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

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

14.15 Exit

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

14.16 Setup

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

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

14.16.1 Mode

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

```
-----
Command: setup mode <Route|Bridge>
Message: Please input the following information.
System operation mode (TAB select) <Route>: Route
-----
```

14.16.2 SHDSL

You can setup the SHDSL parameters by the command shdsl. Move the cursor “ >> ” to shdsl and press enter.

```
>> mode          Configure SHDSL mode
Link            Configure SHDSL link
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 mode, STU-R and STU-C. STU-R means the terminal of central office and STU-C customer premises equipment.

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

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

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

Clear command can clear CRC error count.

Generally, you do not need to change the SNR margin, which ranges 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. I.e., the device will reduce the line rate and reconnect for better line connection.

14.16.3 WAN

The router supports up to 8 PVCs, private virtual circuits, and so you can setup up to 8 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 idle time  
   ip_type       Configure IP type in PPPoA and PPPoE  
   list          WAN interface configuration
```

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

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

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

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

You can setup virtual circuit quality of service, VC QoS, using qos command. The product supports UBR, CBR, VBR-rt and VBR-nrt. The peak cell rate can be configured from 64kbps to 2400kbps. Move the cursor to qos and press enter.

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

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

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

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

14.16.4 Bridge

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

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

You can setup default gateway IP via gateway command.

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

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

After enter add menu, the screen will prompt as follow

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

14.16.5 VLAN

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

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

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

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

To active the VLAN function, move the cursor “>>” to `mode` and press enter. The router supports two types of VLAN, 802.11q and Port-Based. The IEEE 802.1Q defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure. Port-Based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

14.16.6 802.11Q VLAN

Follow the following steps to configure 802.11q VLAN.

```
-----  
Command: setup vlan active <Disable|8021Q|Port>  
Message: Please input the following information.  
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 among 1~4095.

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

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

```
-----  
Command: setup vlan pvid <1~12> <1~4094>  
Message: Please input the following information.  
Port index <1~12>: 1  
VID Value (Enter for default) <10>: 10  
-----
```

To modify the link type of the port, move the cursor to link mode and press enter. There are two types of link: access and trunk. Trunk link will send the tagged packet form the port and access link will send un-tagged packet form the port. Port index 1 to 4 represents LAN1 to LAN4 respectively. According to the operation mode of the device, link type of WAN port is automatically configured. If the product operates in bridge mode, the WAN link type will be trunk, and in routing mode, access.

```
-----  
Command: setup vlan link_mode <1~12> <Access|Trunk>  
Message: Please input the following information.  
Port index <1~12>: 1  
Port link type (Tab select) <Trunk>: Access  
-----
```

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

14.16.7 Route

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

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

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

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

You can setup 20 sets of static route in static command. After entering static menu, the screen will show as follow:

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

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

You can delete the static route information via delete command.

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

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

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

Generic command can setup RIP mode and auto summery mode.

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

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

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

The screen will display the following:

```
>> attrib      Operation, authentication and Poison reverse mode
   version     RIP protocol version
   authe       Authentication code
   Attrib      command can configure RIP mode, authentication type and
               Poison reverse mode.
   Version     command can configure RIP protocol version.
   Authe       command can configure authentication code.
```

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

14.16.8 LAN

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

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

14.16.9 IP share

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

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

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

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

14.16.10 NAT

You can configure NAT parameters in nat menu.

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

The virtual menu contains range of virtual IP address, delete virtual IP address and show virtual IP address.

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

You can create up to five virtual IP address pool ranges in range command.

```
-----
Command: setup ip_share nat virtual range <1~5> <ip> <1~253>
Message: Please input the following information.
NAT local address range entry number <1~5>: 1
Base address: 192.168.1.2
Number of address: 49
-----
```

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

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

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

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

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

```
-----
Command: setup ip_share nat global range <1~5> <ip> <1~253>
Message: Please input the following information.
NAT global IP address range entry number <1~5>: 1
Base address: 122.22.22.2
Number of address: 3
-----
```

After configuring the global IP address range, you can bind the address pool to a specific interface via bind command.

```
-----
Command: setup ip_share nat global interface <1~5> <1~8>
Message: Please input the following information.
NAT global address range entry number <1~5>: 1
Active interface number <1~8>: 1
-----
```

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

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

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

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

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

```
-----
Command: setup ip_share nat fixed modify <1~10> <ip> <ip>
Message: Please input the following information.
Fixed NAT mapping entry number <1~10>: 1
Local address: 192.168.1.250
Global address: 122.22.22.2
-----
```

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

```
-----
Command: setup ip_share nat fixed interface <1~5> <1~8>
Message: Please input the following information.
Fixed NAT mapping entry number <1~5>: 1
Active interface number (Enter for default) <1~8>: 1
-----
```

You can delete fixed NAT mapping entries - from 1 to 5 - by using the delete command.

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

14.16.11 PAT

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

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

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

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

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

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

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

Set the active interface number via interface command.

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

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

The authorized access protocol is setup via protocol command.

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

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

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

14.16.12 DMZ

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

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

You can enable the demilitarized zone via active command.

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

```
-----
Command: setup ip_share dmz address <ip> <1~10>
Message: Please input the following information.
Virtual IP address: 192.168.1.251
Active interface number (Enter for default) <1>: 1
-----
```

14.16.13 Firewall

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

```
>> Level           Configure firewall security level
   pkt_filter      Configure packet filter
   dos_protection  Configure DoS protection
```

There are three levels of firewall:

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

Level two, automatic, enables basic firewall security, all DoS protection, and the SPI filter function.

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

The firewall security level can configure via level command.

14.16.14 Packet Filtering

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

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

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

Add the packet filtering rule via `add` command.

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

14.16.15 DoS Protection

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

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

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

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

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

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

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

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

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

14.16.16 IPQoS

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

To configure IP QoS function, move the cursor to IPQoS and press enter.

```
>> Active      Trigger IP QoS function
Add           Add IP QoS policy
Delete       Delete IP QoS policy
Modify       Modify IP QoS policy
list         Show IP QoS policy table
```

You can enable the IPQoS function via active command.

The add parameters of IPQoS can be configured via add command

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

The port type is configured by protocol command.

The local ip range is configured by local_ip command.

The remote ip range is configured by remote_ip command.

The port range is configured by port command.

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

To enable the policy is configured by enable command.

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

To delete the policy is configured by delete command.

To modify the policy is configured by modify command.

You can view the IPQoS configuration via list command.

14.16.17 DHCP

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

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

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

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

The generic DHCP parameters can be configured via generic command.

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

Active the DHCP function with active command.

Set the default gateway via gateway command.

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

Ip_range command is to configure dynamic assigned IP address range.

The dynamic IP maximum lease time is configured by lease_time command.

You can setup 3 domain name servers via name_server commands.

Fixed Host IP Address list are setup via fixed command.

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

You can view the DHCP configuration via list command.

14.16.18 DNS proxy

You can setup three DNS servers in the router. The number 2 and 3 DNS servers are optional. Move cursor ">>" to dns_proxy and press enter.

```
-----  
Command: setup dns_proxy <IP> [IP] [IP]  
Message: Please input the following information.  
DNS server 1 (ENTER for default) <168.95.1.1>: 10.0.10.1  
DNS server 2: 10.10.10.1  
DNS server 3:  
-----
```

14.16.19 Host name

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

```
-----  
Command: setup hostname <name>  
Message: Please input the following information.  
Local hostname (ENTER for default) <SOHO>: test  
-----
```

14.16.20 Default

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

```
-----  
Command: setup default <name>  
Message: Please input the following information.  
Are you sure? (Y/N): y  
-----
```

Appendix A: Cable Information

This cable information is provided for your reference only. Please ensure you only connect the appropriate cable into the correct socket on either this product or your computer.

If you are unsure about which cable to use or which socket to connect it to, please refer to the hardware installation section in this manual. If you are still not sure about cable connections, please contact a professional computer technician or NetComm for further advice.


RJ-45 Network Ports

RJ-45 Network Ports can connect any networking devices that use a standard LAN interface, such as a Hub/Switch Hub or Router. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable to connect the networking device to the RJ-45 Ethernet port. Depending on the type of connection, 10Mbps or 100Mbps, use the following Ethernet cable, as prescribed.

10Mbps: Use EIA/TIA-568-100-Category 3, 4 or 5 cable.

100Mbps: Use EIA/TIA-568-100-Category 5 cable.

Note: To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 metres.



RJ-45 Connector Pin Assignment	Normal Assignment
1	Input Receive Data +
2	Input Receive Data -
3	Output Transmit Data +
6	Output Transmit Data -
4,5,7,8	Not used

Figure 1



Figure 2

Straight and crossover cable configuration

There are two types of the wiring: Straight-Through Cables and Crossover Cables. Category 5 UTP/STP cable has eight wires inside the sheath. The wires form four pairs. Straight-Through Cables has same pinouts at both ends while Crossover Cables has a different pin arrangement at each end.

In a straight-through cable, wires 1,2,3,4,5,6,7 and 8 at one end of the cable are still wires 1~8 at the other end. In a crossover cable, the wires of 1,2,3,6 are reversed so that wire 1 become 3 at the other end of the cable, 2 becomes 6, and so forth.

To determine which wire is wire 1, hold the RJ-45 cable tip with the spring clip facing towards the ground and the end pointing away from you. The copper wires exposed upwards to your view. The first wire on the far left is wire 1. You can also refer to the illustrations and charts of the internal wiring on the following page.

Straight-Through Cabling

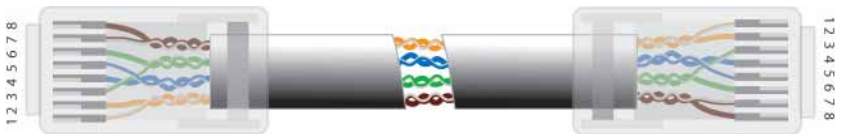


Figure 3

Wire	Becomes
1	1
2	2
3	3
6	6

Cross-Over Cabling

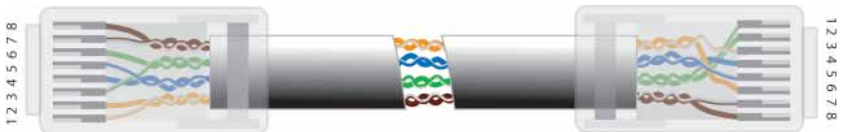
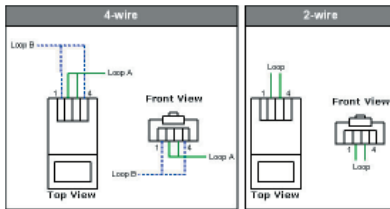


Figure 4

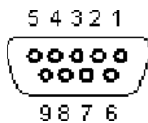
Wire	Becomes
1	3
2	6
3	1
6	2

Note: To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 metres.

SHDSL Line Connector



Console Cable



Pin Number	Description
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

Appendix B: Registration and Warranty Information

All NetComm Limited ("NetComm") products have a standard 12 month warranty from date of purchase against defects in manufacturing and that the products will operate in accordance with the specifications outlined in the User Guide. However some products have an extended warranty option (please refer to your packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at:

www.netcomm.com.au

Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department.

Email: support@netcomm.com.au

Fax: (+612) 9424-2010

Web: www.netcomm.com.au

Copyright Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product. Please note that the images used in this document may vary slightly from those of the actual product. Specifications are accurate at the time of the preparation of this document but are subject to change without notice.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice. NetComm is a registered trademark of NetComm Limited. All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

- (1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.
- (2) This equipment has been tested and found to comply with the Standards for C-Tick and/or A-Tick as set by the ACA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
 - Change the direction or relocate the receiving antenna.
 - Increase the separation between this equipment and the receiver.
 - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - Consult an experienced radio/TV technician for help.
- (3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.



NetComm[®]
Broadband Solutions

NETCOMM LIMITED ABN 85 002 490 486
PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 F: 02 9424 2010
E: sales@netcomm.com.au W: www.netcomm.com.au