

ADSL Broadband Router



AR-6024

User's Manual

Table of Contents

Specification	2
Package Contents	5
Hardware Connecting	6
LED Indicators	7
General Setting	8
One Page Setup	12
Status	14
Router	14
ADSL	16
PPP	17
Advanced Setting	22
ADMINISTRATION	23
WAN	23
LAN	29
DNS	31
NAT	32
Port Forwarding	34
ADSL Configuration	35
RIP Configuration	36
Firewall	37
Service Filtering	41
Diagnostic Test	49
Router Table	51
MAC Filtering	52
Security	53
Admin Password	53
User Password	54
Misc Configuration	55
System Log	57
Code Update	58
Status	59
Router	59
ADSL	61
WAN Status	62
ATM Status	63
TCP connections	64
Learned MAC Table	65
PPP Status	66
Save Settings/Reboot	67
Appendix	68

Specification

4-Port Ethernet ADSL Router



DHCP server/client/relay agent PPP auto reconnect and configurable timeouts PPP auto reconnect on WAN access PPP Auto, PAP, and CHAP 128 character support for PPPx username/passwords DNS proxy NAT, NAPT & Dynamic NAPT ALG support (FTP, SMTP/POP3, ICMP, NNTP, RTSP, IRC, CuSeeMe, Telnet, Messenger, EPIC games, id games, Sierra studios games) Wild Card DMZ Virtual server (Port mapping) VPN pass through (IPSec - ESP Tunnel mode, L2TP, PPTP) Bridge filtering **ICMP** IGMP MAC Address Spoofing Auto VPI/VCI PPPoE/PPPoA detection Multiple PPP sessions per PVC Management HTTP client and server Password protection (2 levels) Configurable Web pages FTP server and client (for network upgrade) Local firmware upgrade via Web configuration pages Remote firmware upgrade via FTP client Restore to Factory defaults via Web or hardware reset 7 layer diagnostics with links to help pages System logging Inner pair / Outer pair / Auto-detection of RJ-11 Ethernet Features IEEE 802.3/802.3u auto-negotiation compliant Auto sense 10/100 Full or Half duplex mode Half duplex - back pressure flow control Full duplex - IEEE 802.3x flow control Crossover Detection and Auto Correction

Hardware
LAN: 4-Port 10/100Base-T (RJ-45)
ADSL: One Port (RJ-11)
Power: 9VAC 800mA
LED indicators: Power, Ready (Status), ADSL, LAN * 4
Reset button

Certification: FCC Part 15/Part 68, CE, LVD

Application Diagram



Package Contents

- ADSL Router
- CD-ROM containing Manual
- Ethernet Cable (CAT5 UTP Straight-Through)
- ADSL Cable (Standard telephone cable)
- USB Cable (Optional)
- Power Adapter
- Quick Installation Guide hardcopy

Hardware Connecting

4 Port Ethernet ADSL Router



ADSL cable here

LED Indicators

4 Port Ethernet ADSL Router

Label	Meaning	Status	Indicates
PWR	Power	On	Power is on
		Off	Power is off
RDY	WAN Link	Flashing	Link being attempted by router.
		On	Link established
		Off	No link
LAN 1/ LAN 2/	LAN Link	Flashing	Flashes when data is being sent or
LAN 3/ LAN 4			received on the LAN connection.
		On	Indicates a link to your LAN or Network card is active.
		Off	Indicates no link to LAN

General Setting

You can use the RJ 45 cable or the USB cable connect to the ADSL Router. Please see the connecting procedures as below:



Move your cursor as following sequence *Start* \ *Settings* \ *Control Panel* and click *Control Panel*. Then double-click on the *Network Connections*





In the *LAN or High-Speed Internet* window, right-click on icon corresponding to your network interface card (NIC) and select *Properties*.(This icon may be labeled Local Area Connection).





In the General Tab of the Local Area Connection Properties menu.

Highlight *Internet Protocol (TCP/IP)* under "This connection uses the following items." by click on it once. Click on the *Properties* button.

🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
B Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure
 ✓ Signature ✓ Client for Microsoft Networks ✓ File and Printer Sharing for Microsoft Networks ✓ QoS Packet Scheduler ✓ Internet Protocol (TCP/IP)
Install Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication
across diverse interconnected networks.
OK Cancel

Step 4

Select **Obtain an IP address automatically:** by clicking once in the circle. Click **OK** button to confirm and save your changes, and the close the Control Panel.

Internet Protocol (TCP/IP) Prope	rties 🔹 🛛 🛛 🛛
General Alternate Configuration	
You can get IP settings assigned autor this capability. Otherwise, you need to the appropriate IP settings.	natically if your network supports ask your network administrator for
 Obtain an IP address automatical 	ly l
Use the following IP address: —	
IP address:	
Subnet mask:	
Default gateway:	
 Obtain DNS server address autor 	natically
OUse the following DNS server add	dresses:
Preferred DNS server:	
Alternate DNS server:	· · · ·
	Advanced
	OK Cancel



Release IP & Renew IP, then Check Default Gateway: 10.0.0.2





Launch your PC web browser and enter the URL: 10.0.0.2

🗐 ht	http://10.0.0.2/ - Microsoft Internet Explorer							
File	Edit	View	Favorites	Tools	He	lp		
0	Back	- 6) - 🔀	2		🔎 Search	☆ Favorites	
Addre	ss 🧧	http://:	10.0.0.2					



In the User name/Password prompt, please type in admin/epicrouter

as default.





Now you can start browsing the web through the ADSL device.

Main Menu (Simple)	OnePage Configurat	ion
BASIC	LANI	
 <u>UnePage Setup</u> show advanced settings 	LAN	
Status	IP Address	
Deuter	Subnet Mask	255.255.255.0
ADSL	WAN	
• <u>PPP</u>	Service Name	
	Username	
Save Setting and Reboot	Password	
	Disconnect Timeout	0 seconds (Max:32767)
	WAN Type	PPPoe LLC
	VC Settings	
	VPI:	8
	VCI:	35
	Static IP Address :	192.168.241.101
	Subnet Mask :	255.255.255.0
	Default Gateway	0000
	BRIDGE	<u>-</u>

One Page Setup

When working with wide area connections, the first thing you must do is to have the handle of the connection. Once you have the handle for a Connection you must define the PVC and protocol settings for it.

Main Menu (Simple)	OnePage Configu	uration
BASIC		
OnePage Setup	LAN	
snow advanced settings	IP Address	10002
Status	Subnet Mask	255.255.255.0
Router ADSI	WAN	
• PPP	Service Name	
	Username	
Save Setting and Reboot	Password	
	Disconnect Timeout	econds (Max:32767)
		· · · · · · · · · · · · · · · · · · ·
	WAN Type	PPPoELLC V
	VC Settings	
	VPI:	8
	VCI:	35
	Static IP Address :	192.168.241.101
	Subnet Mask :	255.255.255.0
	Default Gateway	0000
	DDIDCE	
	BRIDGE	<u> </u>
Main Menu	Username	· · · · · · · · · · · · · · · · · · ·
	Password	
OnePage Setup	Disconnect Timeout	seconds (Max: 32767)
show advanced settings		
Status	WAN Type	PPPoe LLC V
<u>Router</u>		
ADSL PPP	VC Settings	
	VPI:	8
Save Setting and Reboot	VCI:	35
	Static IP Address :	192.168.241.101
	Subnet Mask :	255.255.255.0
	Default Gateway	0.0.0
	DDIDCE	
	BRILGE	Troubed -
	mode	
	Connection Status : N	lot Connected
	Connect Disconnect	
		Submit Reset
	You must click the 'Sub	mit' button and then 'Save setting and Reboot' button to commit changes.

LAN IP Address & Subnet Mask: The default is 10.0.0.2and 255.255.255.0 you can change it to another private IP address, such as 211.22.10.191 and 255.0.0.0. For most configurations it is recommended to leave it as default.

Service Name: Enter the name of your ISP. This information is for identification purposes only.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Disconnect Timeout: Disconnect Timeout means the router will disconnect after being idle for a preset amount of time.

WAN Type: Select type from the list.

VC Settings

- *VPI:* If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = 8.
- *VCI:* If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = **35**.

Static IP Address: Enter the IP address provided by your ISP. such as

192.168.241.101.

Subnet Mask: Set your Subnet Mask such as 255.255.255.0

BRIDGE

Mode: Select **Enable** or **Disable** from the list.

Note: Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

Status

Router

The Home page shows the Firmware Version and WAN and LAN interface status.

 <u>hide advanced settings</u> 	^				-			
ADMINISTRATION			Home Page					
• VVAN • LAN								
• DNS			BootCode vers	sion:	BC_L	X82xxx_4.1.	0.21	
• NAT			Firmware vers	ion:	CX82:	xxx_4.1.0.21	_\$	
Port Forwarding			Customer Softw	ware Version:	4.1.0.	.21_\$		
ADSL Configuration								
RIP Configuration								
<u>Firewall</u> Disconstin Test				WA	N			
Route Table								
MAC Filtering								
SECURITY			IP Address	Subnet M	fask	MAC Addre	33	
Admin Password								
User Password Mins Configuration								
 Misc conliguration System Log 				TAL	-1			
Code Update				цьсц	N			
Status				- 1 - 14-				
Router			IP Address	Subnet Ma	isk	MAC Addie	88	
ADSL			10.0.0.2	255.255.255	5.0	00:09:F3:00:00	:8D	
WAN ATM		L						
AIM TCP connections			Tota	Mumber of I	on Inte	orfacep• 1		
Learned MAC Table			10	I NUMBER OF 2	an ma	ellaces. 1		
PPP Status		Nu	umber of ethern	et devices con	nected	to the DHCP s	erver: 1	
1	- 19 De							
Save Setting and Reboot			IP	Address	MAG	2 Address		
Save Setting and Reboot	•		IP	Address	MAC	C Address		
Save Setting and Reboot	•		IP	Address	MAC	C Address		
Save Setting and Reboot	•			Address	MAC	C Address		
Save Setting and Reboot Save Setting and Reboot hide advanced settings ADMINISTRATION VAN IAN	•			Address	MAC	C Address		
Save Setting and Reboot hide advanced settings ADMINISTRATION WAN LAN DNS	•			Address	MAC	C Address		
Save Setting and Reboot Save Setting and Reboot hide advanced settings ADMINISTRATION WAN LAN LAN DNS NAT	•			Address	MAC	C Address		
Save Setting and Reboot • hide advanced settings ADMINISTRATION • WAN • WAN • DNS • NAT • Port Forwarding	•		IP Address	Address WA Subnet M	MAC N	C Address	88	
Save Setting and Reboot Additional Settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration TO Set Configuration	×		IP Address	Address WA Subnet M	MAC N fask	MAC Addre	88	
Save Setting and Reboot Save Setting and Reboot MainisTration WAN LAN DNS NAT Post Forwarding ADSL Configuration RIP Configuration RIP Configuration Firewall	•		IP Address	Address WA Subnet M	MAC N fask	C Address	83	
Save Setting and Reboot • hide advanced settings ADMINISTRATION • VAN • UAN • DINS • NAT • Port Forwarding • ADSL Configuration • RIP Configuration • RIP Configuration • Firewall • Diaanostic Test	×		IP Address	Address WA Subnet M	MAC N fask	C Address	88	
Save Setting and Reboot Additional settings ADMINISTRATION WAN UAN DINS NAT Port Forwarding ADSL Configuration Firewall Diagnostic Test Route Table	•		IP Address	Address WA Subnet M	MAC N fask	MAC Addres	85	
Save Setting and Reboot hide advanced settings ADMINISTRATION VAN LAN DNS NAT Pont Forwarding ADSL Configuration RitP Configuration Firewal Diagnostic Test Route Table MAC Filtering	×		IP Address	Address WA Subnet M	MAC N fask	C Address	88 	
Save Setting and Reboot Automatic Settings ADMINISTRATION WAN LAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration Setting Security Add Setting Security Security Security Security Security Security Security Security Secur	*		IP Address	Address WA Subnet M LAI	MAC N fask	MAC Address	88	
Save Setting and Reboot bide advanced settings bide	×		IP Address	Address WA Subnet M LAI	MAC N Mask	MAC Addre	83	
Save Setting and Reboot Administration WAN LAN DNS NAT Port Forwarding ADSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password	×		IP Address 10.0.0.2	Address WA WA Subnet M LAI 255255253	MAC N Mask N ssk	MAC Address MAC Addres MAC Addres	85 88 93 D	
Save Setting and Reboot hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration RitP Configuration Firewal Diagnostic Test Route Table MAC Filtering SECURITY Lassword User Password User Password Misc Configuration System Log	×		IP Address 10.0.0.2	Address WA Subnet M LAI 255255255	MAC N Isk	MAC Address MAC Addres MAC Addres	88 88 %D	
Save Setting and Reboot Automatic Settings RelP Configuration Firewall Diagnostic Test Route Table MAC Fittering SetURITY Admin Password Mise Configuration System Log Code Update	×		IP Address ID.0.0.2	Address WA Subnet M LA Subnet Ma 255.255.251	MAC N fask N ssk 5.0	MAC Address MAC Addres MAC Addres 00:09:F3:00:00 erfaces: 1	88 88 88 %D	
Save Setting and Reboot	•		IP Address IP Address 10.0.0.2 Tota	Address WA Subnet M Subnet Ma 255:255:251	MAC N fask N sk 5.0	MAC Address MAC Addre MAC Addre 00:09:F3:00:00 erfaces: 1	ss	
Save Setting and Reboot Automatic settings Automatic settings Automatic settings Automatic settings Automatic settings Automatic setting Security Automatic setting Automatic setting System Log Code Update Status Poutar Automatic Security Security Automatic Security Se	•		IP Address IO.0.0.2 Tota umber of ethern	Address WA WA Subnet M 255:255:251 I Number of I et devices con	MAC N Iask S.0 Lan Inte	MAC Address MAC Addres 00:09:F3:00:00 erfaces: 1 I to the DHCP s	ss ss 	
Save Setting and Reboot Automatic Settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration Settering SECURITY Admin Password User Password User Password User Password User Password User Configuration System Log Code Update Status Router ADSL	*		IP Address ID.0.0.2 Tota mber of ethern	Address WA Subnet M LAI 255.255.255 I Number of I et devices con	N task N usk .an Inte	MAC Address MAC Addres 00:09:F3:00:00 erfaces: 1 i to the DHCP s	ss :SD erver: 1	
Save Setting and Reboot Automatic Settings RelP Configuration Firewall Diagnostic Test Route Table Mac Fittering Securit Automatic Setting Code Update Status Router Automatic Setting Router Automatic Setting Rel Point S	•		IP Address 10.0.0.2 Tota unber of ethern	Address Addres	N fask N ssk an Inte anected	MAC Address MAC Addres 00:09:F3:00:00 erfaces: 1 I to the DHCP s C Address	88 88 89 89 erver: 1	
Save Setting and Reboot	×		IP Address IP Address 10.0.0.2 Tota mber of ethern IP	Address WA Subnet M Subnet M 255.255.251 I Number of L et devices con Address	N Isk 5.0 MAC	MAC Address MAC Addre MAC Addre 00:09:F3:00:00 erfaces: 1 I to the DHCP s C Address	ss ss x3D erver: 1	
Save Setting and Reboot Automatic settings Automatic settings Automatic settings Automatic settings Automatic settings Automatic setting A	×		IP Address ID.0.0.2 Tota unber of ethem I I I I I I I I I I I I I I I I I I I	Address WA Subnet M Subnet M 255.255.251 I Number of L et devices con Address 0.0.0,3	N Aask N ssk 5.0 .an Inte mected MAC	MAC Address MAC Addre MAC Addre 00:09:F3:00:00 erfaces: 1 It to the DHCP s C Address 49:E7:2B:23	ss ss v3D erver: 1	
Save Setting and Reboot Automatic settings ADMINISTRATION WAN LAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration Secture Code Update Status Router Table Router Table Code Update Status Router Configuration System Log Code Update Status Router Configuration Revent Configuration Revent Configuration System Log Code Update Status Router PEPP Status Revent Configuration Learned MAC Table PPP Status	*		IP Address 10.0.0.2 Tota unber of ethern 1 10	Address WA Subnet M Subnet Ma 255:255:255 1 Number of I et devices con Address 0 .0.0.3 7	MAC N fask S.0 Lan Inte mected MAC 72:08:	MAC Address MAC Addres 00:09:F3:00:00 erfaces: 1 d to the DHCP s C Address 49:E7:2B:23	ss SS SD erver: 1	

Firmware Version: This field displays the Firmware Version number.

Save Setting and Reboot

WAN: These fields display the IP Address, Subnet Mask, MAC Address for WAN interface.

Ethernet Link Status: UP

USB Link Status: DOWN

- *LAN:* These fields display the IP Address, Subnet Mask, MAC Address for LAN interface.
- *Number of Ethernet devices connected to the DHCP server:* This field displays the number of DHCP clients connected to the ADSL Router. It also shows the IP address and MAC address of the attached DHCP clients.

ADSL

The ADSL Status page shows the ADSL physical layer status.

Main Menu (Simple) BASIC • OnePage Setup • show advanced settings Status • Router • AOSI • PPP	Showtir Line Xt Modula Anney	ne Firmware Versio ate: tion: Mode:	ADSL STATI Restart v Exec on: 3.46 ACTIVAT N/A ANNEY	US ute ION		
Save Setting and Reboot	Startup Max Tx CO Ver Elaspee	Attempts: : Power: idor: d Time:	INNE 0 I			seconds
		SNR Margin	NA	NA	dB	
		Line Attenuation	NA	NA	dB	
		Errored Seconds	0	0		
		Loss of Signal	0	0		
		Loss of Frame	0	0		
		CRC Errors	0	0		
		Data Rate	0	0	kbps	

Showtime Firmware Version: This field displays the ADSL data pump firmware version number.

Line State: This field displays the ADSL connection process and status.
 Modulation: This field displays the ADSL modulation status for G.dmt or T1.413.
 Annex Mode: This field displays the ADSL Annex modes for Annex A or Annex B.
 Startup Attempts: This field displays the ADSL connection attempts after loss of showtime.

Max Tx Power: This field displays the transmit output power level of the CPE.Co Vendor: This field displays the Central Office DSLAM vendor name. If available.Elaspsed Time: This field displays the time of the modem has been in operation.

PPP

The PPP Status page shows the status of PPP for each PPP interface. See PPP.



These fields display the following information on each PPP interface:

- Connection Name (user defined)
- Interface (PVC)
- Mode (PPPoE or PPPoA)
- Status (Connected or Not Connected)
- Packets Sent
- Packets Received
- Bytes Sent
- Byte Received
- **Connect and Disconnect:** Each PPP session can be individually controlled, simply enter the desired connection number into the "Connection #" field and select either connect or disconnect from the drop down menu and click on the "Execute" button.

WAN Configuration: The WAN configuration page allows the user to set the configuration WAN/ADSL ports.

Main Menu (Advanced)	WAN Configuration (Pvc 0)					
BASIC OnePage Setup	Change Adapter					
hide advanced settings ADMINISTRATION	Winters] Cinemia	Fedded -	Static IP Settings			
• WAN	Virtual Circuit	Disabled	IP Address	192.168.241.101		
LAN DNS	Bridge	Disabled	Subnet Mark	255 255 255 0		
NAT Port Forwarding	IGMP Enconculation		Gateway	0000		
ADSL Configuration	Encapsulation		Galeway			
Firewall	АТМ		PPP	Advanced PPP configuration		
Diagnostic Test Route Table	VPI	8	Service Name			
MAC Filtering SECURITY	VCI	35	Username			
Admin Password	Service	UBR	Password			
<u>Misc Configuration</u>	Peak Cell Rate	0 khna	Disconnect Timcout	0 minutes (Max:32767)		
<u>System Log</u> <u>Code Update</u>	Sustainable	r Kops	Timeout	PPP Disconnect Timer Config		
Status	Cell Rate	kbps	MRU	1492		
Router ADSI	Max Burst Size	0	MTU	1492		
• WAN	DHCP Client	Disabled -	MSS	1432		
<u>AIM</u> <u>TCP connections</u>	Host Name		Lcp Echo Interval	10 seconds		
Learned MAC Table	Tiost Maine		Len Echo			
Main Menu (Simple)	VPI	8	Service Name			
BASIC	VCI	35	Username			
 <u>OnePage Setup</u> show advanced settings 	Service Category	UBR	Password			
Status	Peak Cell Rate	0 kbps	Timeout	0 minutes (Max:32767)		
<u>Router</u>	Sustainable	0 kbps		PPP Disconnect Timer Config		
ADSL PPP	Cell Rate	0	MRU	1492		
	Max Buist Size	P	MTU	1492		
Save Setting and Reboot	DHCP Client	Disabled -	MSS	1432		
	Host Name		Lcp Echo Interval	10 seconds		
			Lcp Echo Maximum	6		
	MAC Spoofing	Disabled -	Consecutive Failure			
	Mac Address	000000000	Authentication	Auto		
			Automatic Reconnect			
		Subr	mit Reset			
	Settin	gs need to be saved to Flash and the syst	tem needs to be reboo	ted for changes to take effect.		
		<u>Save C</u>	onfiguration			
				_		

Per VC Settings

Virtual Circuit: Selection Enable or Disable.

- *VPI:* If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = **0**.
- VCI: If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = 0
- *MAC Spoofing:* MAC Spoofing is developed to solve the scenario when the ISP only recognizes one MAC address. Copy the ISP-recognized MAC address here.

ATM

Service Category: UBR and CBR are supported from the ATM.

Bandwidth: Bandwidth setting takes effect only when the CBR is selected. The maximum available bandwidth is from the upstream data rate of ADSL status page.

ENCAPSULATION: Selection follow as Table-1 Configuration

BRIDGE: Enabling bridge mode will place the unit into Transparent bridge mode (like a Ethernet ADSL modem) to use this mode you should also set your WAN type to a Bridging option (e.g RFC1482 Bridge using LLC).

IGMP: IGMP relay/proxy specification and environment:

Support IGMP proxy/relay function for ADSL modem, based on the following requirement and case:

On CO side, there must be at least one IGMP querier (router) present. IGMP querier will send IGMP query packet. The ADSL modem is responsible to relay these IGMP query to Ethernet.

End-user multicast application device send IGMP report while receiving IGMP query or being activated by user, the ADSL modem should be responsible to proxy (that is, change source IP to ADSL modem's WAN IP) the IGMP report to ADSL WAN side, include all PVCs. The same case is for IGMP leave packet. Not necessary to relay multicast routing between two ADSL PVCs or two interfaces in LAN side.

Special purpose multicast packet (such as RIP 2 packet) should run without interference.

Table-1 Configuration

WAN	Bridge Mode	Router Mode	Router Mode	Router Mode
Configuration		(PPPoA/PPPoE)	(Dynamic IP)	(Static IP)
IP address	N/A	Automatically	Automatically	Provided by ISP
		assigned by ISP	assigned by ISP	
Subnet Mask	N/A	Automatically	Automatically	Provided by ISP
		assigned by ISP	assigned by ISP	
WAN Type	1483 Bridged	PPPoA	1483	1483
	IP LLC,	LLC/VC-Mux,	Bridged/Routed	Bridged/Routed
	1483 Bridged	PPPoE	IP LLC,	IP LLC,
	IP VC-Mux	LLC/VC-Mux	1483	1483
			Bridged/Routed	Bridged/Routed
			VC-Mux,	VC-Mux,
			Classical IP over	Classical IP over
			ATM	ATM
Bridge	Enabled	Disabled	Disabled	Disabled
PPP Service	N/A	Provided by ISP	N/A	N/A
PPP User	N/A	Provided by ISP	N/A	N/A
name				
PPP	N/A	Provided by ISP	N/A	N/A
Password				
DHCP Client	Unchecked	Unchecked	Checked	Unchecked
enable				

Table-2

Rx Entity	Packet Class	TTL	Action	Notes
ADSL	IGMP query	1	Relay to Ethernet	
	IGMP report	1	Ignore	
	IGMP leave	1	Ignore	
	General Multicast IP	-	Relay it to Ethernet.	
Ethernet	IGMP query	1	Ignore	
	IGMP report	1	Relay to all ADSL PVC	
	IGMP leave	1	Relay to all ADSL PVC	
	General Multicast IP	-	Ignore	

PPP: The current release supports multiple PPP sessions per PVC. The PPP configuration in the WAN configuration page is for the first PPP session for each PVC. The predefined PPP Account Name (Account ID) is "Simple PPP Account 0" for PVC0 and predefined PPP Connection Name is "Simple PPP Session 0" for PVC0. For the other PVC X, the predefined account name and connection name will be Simple PPP Account X and Simple PPP Session X. X is the PVC number from 1 to 7.

It can support up to total of 16 PPP sessions, and each PVC can support up to 8 PPP sessions, the multiple PPP sessions may be configured with any combination over 8 PVCs.

Service Name: The service name of PPP is required by some ISPs. If the ISP does not provide the Service Name, please leave it blank.

Username: Your user name provided by your ISP.

- Password: Your password provided bye your ISP.
- **Disconnect Timeout:** The Disconnect Timeout allows the user to set the specific period of time to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.
- *MRU:* Maximum Receive Unit indicates the peer of PPP connection the maximum size of the PPP information field this device can be received. The default value is 1492 and is used in the beginning of the PPP negotiation. In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.
- *MTU:* Maximum Transmission Unit indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicates its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1492.
- **MSS:** Maximum Segment Size is the largest size of data that TCP will send in a single IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their MSS during the TCP connection handshake. The default value is 1432.
- *Automatic Reconnect:* When it is checked, it will maintain the PPP connection all the time. If the ISP shut down the PPP connection, it will automatically reconnect PPP session.

DHCP: Use Table-1 to configure a valid setting for each PVC.

Host Name: Required by some ISPs. If the ISP does not provided the Host name,

please leave it blank.

Note: Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

Advanced Setting

ADMINISTRATION

The links under the ADMINISTRATION column are associated to the pages that represent the configurations of system and interfaces.

Note: When the configurations are changed, please click the **Save Setting** and **Reboot** button.

WAN

The WAN configuration page allows the user to set the configuration for WAN/ADSL ports.

Main Menu (Advanced)	WAN Conf	iguration (Pvc 0)
BASIC OnePage Setup hide advanced settings	Cha	ngt Adapter
ADMINISTRATION WAN LAN LAN NAT NAT Port Forwarding	Virtual Circuit Enabled Bridge Disabled IGMP Disabled Enconsulation FPF0FULC	Static IP Settings IP Address 192.168.241.101 Subnet Mask 255.255.0 Galeway 00.00
ADSL Configuration RIP Configuration Firewall Diagnostic Test Route Table	ATM VPI 8	PPP Advanced PPP configuration Service Name
MAC Filtering SECURITY Admin Password User Password Misc Configuration	VCI 33 Service UBR ¥	Username Password Disconnect D
System Log Code Update Status	Peak Cell Rate 0 kbps Sustainable 0 kbps Cell Rate	Timeout P minutes (Max:32767) <u>PPP Disconnect Timer Config</u> MRU [1492
Router ADSL WAN ATM TCP connections	DHCP Client Disabled	MTU 1492 MSS 1432 Lcp Echo Interval 10 seconds
Learned MAC Table	Host Name	Lop Echo

	VPI	8	Service Name		
Main Menu (Advanced)	VCI	35	Username		
BASIC	Corrigo		Deserved		
OnePage Setup bids advanced actions	Category	UBR 💌	rassword		
ADMINISTRATION	D L G N D .		Disconnect	minutes (Max:32767)	
• WAN	Peak Cell Rate	10 kbps	Timeout	i initiales (Max.S2101)	
• LAN	Sustainable	0 khne		PPP Disconnect Timer Config	
DNS NAT	Cell Rate	, KDPo	MRU	1492	
Port Forwarding	Max Burst Size	0	MTH	1492	
ADSL Configuration			MIO	1492	
RIP Configuration	DHCP Client	Disabled -	MSS	1432	
<u>Firewall</u>	Differ chem		Lcp Echo Interval	10 seconds	
Diagnostic Test Route Table	Host Name		Les Debe	- Seconds	
MAC Filtering			LCD ECNO Maximum	6	
SECURITY	MAC	Disabled -	Consecutive Failure	2	
Admin Password	Spoofing		Authentication	Auto	
User Password Mice Configuration	Mac Address	0.00.00.00.00	Humenneanon		
System Log			Automatic		
Code Update			Reconnect		
Status					
Boutor	Submit Reset				
ADSL	Continue and the larger of the Theology of the sector way do to be achieved for the sector by the off of				
WAN	Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.				
• <u>ATM</u>	Save Configuration				
TCP connections					
Learned WAL Table					-

Per VC Settings

Virtual Circuit: Selection Enable or Disable.

- *VPI:* If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = **0**.
- VCI: If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = 0
- **MAC Spoofing:** MAC Spoofing is developed to solve the scenario when the ISP only recognizes one MAC address. Copy the ISP-recognized MAC address here.

ATM

Service Category: UBR and CBR are supported from the ATM.

Bandwidth: Bandwidth setting takes effect only when the CBR is selected. The maximum available bandwidth is from the upstream data rate of ADSL status page.

ENCAPSULATION: Selection follow as Table-1 Configuration

BRIDGE: Enabling bridge mode will place the unit into Transparent bridge mode (like a Ethernet ADSL modem) to use this mode you should also set your WAN type to

a Bridging option (e.g RFC1482 Bridge using LLC).

IGMP: IGMP relay/proxy specification and environment:

Support IGMP proxy/relay function for ADSL modem, based on the following requirement and case:

On CO side, there must be at least one IGMP querier (router) present. IGMP querier will send IGMP query packet. The ADSL modem is responsible to relay these IGMP query to Ethernet.

End-user multicast application device send IGMP report while receiving IGMP query or being activated by user, the ADSL modem should be responsible to proxy (that is, change source IP to ADSL modem's WAN IP) the IGMP report to ADSL WAN side, include all PVCs. The same case is for IGMP leave packet. Not necessary to relay multicast routing between two ADSL PVCs or two interfaces in LAN side.

Special purpose multicast packet (such as RIP 2 packet) should run without interference.

Table-1 Configuration

WAN	Bridge Mode	Router Mode	Router Mode	Router Mode
Configuration		(PPPoA/PPPoE)	(Dynamic IP)	(Static IP)
IP address	N/A	Automatically	Automatically	Provided by ISP
		assigned by ISP	assigned by ISP	
Subnet Mask	N/A	Automatically	Automatically	Provided by ISP
		assigned by ISP	assigned by ISP	
WAN Type	1483 Bridged	PPPoA	1483	1483
	IP LLC,	LLC/VC-Mux,	Bridged/Routed	Bridged/Routed
	1483 Bridged	PPPoE	IP LLC,	IP LLC,
	IP VC-Mux	LLC/VC-Mux	1483	1483
			Bridged/Routed	Bridged/Routed
			VC-Mux,	VC-Mux,
			Classical IP over	Classical IP over
			ATM	ATM
Bridge	Enabled	Disabled	Disabled	Disabled
PPP Service	N/A	Provided by ISP	N/A	N/A
PPP User	N/A	Provided by ISP	N/A	N/A
name				
PPP	N/A	Provided by ISP	N/A	N/A
Password				
DHCP Client	Unchecked	Unchecked	Checked	Unchecked
enable				

Table-2

Rx Entity	Packet Class	TTL	Action	Notes
ADSL	IGMP query	1	Relay to Ethernet	
	IGMP report	1	Ignore	
	IGMP leave	1	Ignore	
	General Multicast IP	-	Relay it to Ethernet.	
Ethernet	IGMP query	1	Ignore	
	IGMP report	1	Relay to all ADSL PVC	
	IGMP leave	1	Relay to all ADSL PVC	
	General Multicast IP	-	Ignore	

PPP: The current release supports multiple PPP sessions per PVC. The PPP configuration in the WAN configuration page is for the first PPP session for each PVC. The predefined PPP Account Name (Account ID) is "Simple PPP Account 0" for PVC0 and predefined PPP Connection Name is "Simple PPP Session 0" for PVC0. For the other PVC X, the predefined account name and connection name will be Simple PPP Account X and Simple PPP Session X. X is the PVC number from 1 to 7.

It can support up to total of 16 PPP sessions, and each PVC can support up to 8 PPP sessions, the multiple PPP sessions may be configured with any combination over 8 PVCs.

Service Name: The service name of PPP is required by some ISPs. If the ISP does not provide the Service Name, please leave it blank.

Username: Your user name provided by your ISP.

- Password: Your password provided bye your ISP.
- **Disconnect Timeout:** The Disconnect Timeout allows the user to set the specific period of time to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.
- *MRU:* Maximum Receive Unit indicates the peer of PPP connection the maximum size of the PPP information field this device can be received. The default value is 1492 and is used in the beginning of the PPP negotiation. In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.
- *MTU:* Maximum Transmission Unit indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicates its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1492.
- **MSS:** Maximum Segment Size is the largest size of data that TCP will send in a single IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their MSS during the TCP connection handshake. The default value is 1432.
- *Automatic Reconnect:* When it is checked, it will maintain the PPP connection all the time. If the ISP shut down the PPP connection, it will automatically reconnect PPP session.

DHCP: Use Table-1 to configure a valid setting for each PVC.

Host Name: Required by some ISPs. If the ISP does not provided the Host name,

please leave it blank.

Note: Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

LAN

The LAN configuration page allows you to set the configuration for the LAN port.

	-	T	AN Configuration	^
Main Menu (Advanced)		L	An Computation	
OnePage Setup		IP Address	10.0.2	
hide advanced settings				
ADMINISTRATION • WAN		Subnet Mask	255.255.255.0	
• LAN				
DNS NAT		DHCP Server	Enabled 💌	
Port Forwarding		DHCP address need selection	Statem Allocated	
ADSL Configuration BIR Configuration		Differ address poor selection		
Firewall		User Defined Start Address	10.0.0.4	
Diagnostic Test Doute Table		User Defined End Address	10.0.0.15	
MAC Filtering		DHCP Cotoway Selection	Automatic -	
ECURITY Admin Paceword		Dricr Galeway Selection	Protoniado Y	
User Password		User Defined Gateway Address		
<u>Misc Configuration</u> System Log		Lease Time	1 days hours minutes seconds	
<u>Code Update</u>				
Status		DUGD D.L.		_
Router		DHUR Kelay	Disader	
ADSL WAN	1	DHCP Relay Target IP	0.0.0	
• <u>ATM</u>				
<u>TCP connections</u> Learned MAC Table		User Mode	Multi-User 🔻	_
	11			-
Main Menu (Atama)	-	DHCK Selvel	13x000 ×	
Main Menu (Advanced) BASIC		DHCP Server	System Allocated 💌	
Main Menu (Advanced) BASIC • OnePage Setup	<u>-</u>	DHCP Server DHCP address pool selection User Defined Start Address	System Allocated V	
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings administration		DHCP Server DHCP address pool selection User Defined Start Address User Defined Red Address	System Allocated [100.0.4	
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings ADMINISTRATION • WAN	2	DHCP selver DHCP address pool selection User Defined Start Address User Defined End Address	System Allocated Image: Control of the system	
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings ADMINISTRATION • V/AN • V/AN • DNIS		DHCP server DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection	System Allocated JO00.4 JO00.15 Automatic	
Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION WAN WAN NAT		DHCP server DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address	System Allocated	
Main Menu (Advanced) BASIC OnePage Setup hidia advanced settings ADMINSTRATION WAN WAN LAN ONS NAT Port Forwarding ADSL Confouration		DHCP server DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address	System Allocated	
Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration		DHCP Server DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time	System Allocated V 1000.04 1000.05 Automatic V 1 days 0 hours 0 minutes 0 seconds	
Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION WAN WAN WAN NAT Port Forwarding ADSL Configuration RIP Configuration Fireward Diagnostic Test		DHCP server DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time	System Allocated J00004 J000015 Automatic I days 0 hours 0 minutes 0 seconds	
Main Menu (Advanced) BASIC OnePage Setup hidia advanced settings ADMINSTRATION VAAN VAAN VAAN NAT Poot Forwarding ADSL Configuration RIP Configuration Firewall Diagnostic Test Pootus Table		DHCP Selver DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay	System Allocated V 1000.04 1000.015 Automatic V 1 days 0 hours 0 minutes 0 seconds Disabled V	
Adin Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION VAAN VAAN VAAN VAAN DNS NGT Port Forwarding ADSL Configuration RIPL Configuration Firewall Diagnostic Test Route Table MAC Fittering SECURITY		DHCP Selver DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay Target IP	System Allocated V System Allocated V 100004 1000015 Automatic V Automatic V Automatic V Disabled V Disabled V 00000	
Main Menu (Advanced) BASIC OnePage Setup In idie advanced settings Administration VAN EAN UNS NAT Port Forwarding ADSL Configuration Firewall Disgonostic Test Rouce Table MAC Filtering SECURITY Admin Password		DHCP Selver DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay Target IP	System Allocated System Allocated 1000.04 1000.015 Automatic 1 days 0 hours 0 minutes 0 seconds Disabed • 50000	
Main Menu (Advanced) BASIC OnePage Setup In idie advanced settings ADMINISTRATION VAN EAN DNS NAT Port Forwarding ADSIL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password		DHCP Selver DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay Target IP	System Allocated System Allocated I000.04 I000.015 Automatic I days hours seconds Disabled I use	
Main Menu (Advancet) BASIC OnePage Setup Inide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSIL Configuration Firewal Diagnostic Test Boute Table MAC Filtering SECURITY Admin Password User Password User Password System Log		DHCP Selver DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay Target IP User Mode	System Allocated System Allocated 1000.01 Automatic	
Main Menu (Advanced) BASIC OnePage Setup Inide advanced settings ADMINISTRATION VAN EASI DNS NAT Port Forwarding ADSL Configuration Firewal Diagnostic Test Boute Table MAC Filtering SECURITY Admin Password User Password Misc Configuration Stytem Log Code Update		DHCP Selver DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay Target IP User Mode Eff	System Allocated System Allocated	
Main Menu (Advanced) BASIC 0. OnePage Setup hide advanced settings ADMINISTRATION VMAN ADMINISTRATION VAN ADMINISTRATION NAT Port Forwarding ADSL Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration SECURITY Admin Password User Password Mac Centinguration Status		DHCP Selver DHCP address pool selection User Defined Start Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay Target IP User Mode EH	System Allocated System Alloc	
Main Menu (Advance) BASIC OnePage Setup hide advanced settings ADMINISTRATION V/AN LAN DNS NAT Pont Forwarding ADSL Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration Security MAC Filtering SECURITY SecURITY Masc Configuration System Log Code Update Status Router AdSL		DHCP Selver DHCP address pool selection User Defined Start Address User Defined End Address DHCP Cateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay Target IP User Mode Effect	System Allocated [00.0.4 [00.0.15 Automatic days hours minutes seconds Disabled [Disabled] [Disabled] [Muls-User] hermet Mode Setting [Subard Rest]	
Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION V/AN LANA DNS NAT Port Forwarding ADSL Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration Status Status Router Admin Password Mac Citiering Scole Update Status	Settin	DHCP Server DHCP address pool selection User Defined Start Address User Defined End Address DHCP Cateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay DHCP Relay Eli Ser Mode Eli Ser Mode	System Allocated System Allocated 100.0.4 100.0.15 Automatic days hours minutes seconds Deabled Deabled Mult-User hernet Mode Setting Stemit Rect he system needs to be rebooted for changes to take effect.	
Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION VAN CAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration RIP Configuration Security Admin Password User Password User Password User Password Mac Ciffering Security Admin Password User Password System Log Code Update Status Router ADSL NAN Status ROUTER Passon Status ROUTER Passon Status ROUTER Passon Passon Passon Passon Passon Password	Settin	DHCP Server DHCP address pool selection User Defined Start Address User Defined End Address DHCP Gateway Selection User Defined Gateway Address Lease Time DHCP Relay DHCP Relay DHCP Relay Estimation User Mode Estimation	System Allocated	

LAN IP Address & Subnet Mask: The default is 10.0.0.2 and 255.0.0.0 you can change it to another private IP address, such as 211.22.10.191 and 255.255.255.0. For most configurations it is recommended to leave it as default.

- **DHCP Server:** System Allocated. The DHCP address pool is based on LAN port IP address plus 12 IP address. For example, the LAN IP address is 10.0.0.2; the DHCP address pool is at the range of 10.0.0.3 to 10.0.0.14.
- **User Defined:** The DHCP address pool is at the range of User Defined Start Address and User Defined End Address. The maximum pool size can be 253 IP address:255 total IP address-1 broadcast address-1 LAN port IP address.

- **DHCP Gateway Selection:** The default setting for the DHCP Gateway Selection is "Automatic". The user can select the "User Defined" to specify "User Defined Gateway Address". The DHCP server will issue the "User Defined Gateway Address" to the LAN DHCP client.
- *Lease time:* The lease time is the amount of time of a network user will be allowed to connect with DHCP server. If all fields are 0, the allocated IP address will be effective forever.
- **User mode:** Under the Single User mode, the DHCP server only allocates one IP address to local PC. Under the Multiple User mode, the DHCP server allocates the IP addresses specified by the DHCP address pool.
- *Ethernet Mode Setting:* The Ethernet Mode Configuration page allows the user to set the LAN port into Auto Sense, 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex or 10 Mbps Half Duplex.



Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

DNS

Main Menu (Advanced)	DNS Configuration
BASIC • OnePage Setup • hide advanced settings ADMINISTRATION • WAN • UAN • DNS	DNS Proxy Esabled ▼ Auto Discovery マ User Configuration □ DNS Server
NAT Port Forwarding ADSL Configuration RIP Configuration Firewall Diagnostic Test Route Table MACE Filtering SECURITY Admin Password User Password	DNS Server Disabled - Url Name Host Ip Add - Apply Reset
<u>Misc Configuration</u> <u>System Log</u> <u>Code Update</u> Status	DNS Proxy Setting DNS Server Setting # DNS Server IP # Url Name (Host,Domain) Host IP
Router ADSL WAN ATM TOP connections Learned MAC Table	Settings take effect immediately, no system reboot is required <u>Save Configuration</u>

The DNS Configuration page allows you to set the configuration of DNS proxy.

- **Disable DNS Proxy:** The LAN port does not process the DNS query message. For the DHCP requests from local PCs, the DHCP server will set the user-configured preferred DNS sever or alternate DNS server whichever is available as the DNS server. Then all DNS query messages will be directly sent to the DNS servers.
- Use Auto Discovered DNS Servers Only: The DNS proxy will store the DNS server IP addresses obtained from DHCP client or PPP into the table. And all DNS query messages will be sent to one of the dynamically obtained DNS servers.
- Use User Configured DNS Servers Only: The DNS proxy will use the user-configured preferred DNS server and alternate DNS server. And all DNS query message will be sent to one of DNS servers.
- **Auto Discovery + User Configured:** The DNS proxy's table has all the IP addresses of dynamically obtained and user configured DNS servers.
- User Configuration: Place your primary and secondary DNS addresses here.

NAT

The NAT Configuration page allows users to set the configuration for the Network Address Translation. The default setting is Dynamic NAPT. It provides dynamic Network Address Translation capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP address and Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections. When the Dynamic NAPT is chosen, there is no need to configure the NAT Session and NAT Session Name Configuration.

Main Menu (Advanced)	-	NAT Configuration
BASIC OnePage Setup hide advanced settings ADMINISTRATION		NAT Enable - Mode Dynamic NAPT -
WAN LAN DNS NAT		Submit
Port Forwarding ADSL Configuration RIP Configuration Firewall		Session Name User's IP Action
Diagnostic Test Route Table MAC Filtering SECURITY		Submit Reset
Admin Password User Password Misc Configuration System Log		Session Name User's IP
<u>Code Update</u> Status		Session Name Configuration
Kouter ADSL WAN ATM TOP		Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect. Available Sessions
ICP connections Learned MAC Table	•	# Session Name Interface

The NAT option only maps single WAN IP address to the local PC IP address. It is peer-to-peer mapping. (1x1) for each WAN interface, only one local PC IP address can be associated with each WAN interface. Click the link Session Name Configuration to add the session name for WAN interface.

The NAPT option only maps single WAN IP address to many local PCs IP address. (1xN). It is the multiple-mapping mechanism. For each WAN Interface, more than one local PC can be associated with one WAN Interface. Click the link Session Name Configuration to add the session name for WAN interface.

- **Session Name:** This field allows the user to select the session form the configured NAT Session Name Configuration.
- **User's IP:** This field allows the user to assign the IP address to map the corresponding NAT/NAPT sessions.
- Session Name Status will be displayed at the middle of this page to show the corresponding Session Name with its IP address.

- *Number of NAT Configurations*: This field displays the total number of NAT Sessions is entered.
- **Available Sessions Status** will be displayed at the end of this page to show all the Session Name with its WAN Interface.
- *Interface:* This field allows the user to choose specific WAN Interface (PVC or PPP Session) for NAT Session.
- *Number of Session:* This field displays the total number of NAT Sessions Name is entered.
- *Note:* Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

Port Forwarding

The Port Forwarding page allows the user define a port forwarding rule without using the firewall policy database definitions and apply it to the connection.



Public Port: This field allows the user to enter the port number of Public Network.Private Port: This field allows the user to enter the port number of the Private Network.Host IP Address: This field allows the user to enter the private network IP address for

the particular server.

Well Known Ports:

Port	Protocol
21	FTP
23	Telnet
25	SMTP
43	Whois
53	DNS
69	TFTP
70	Gopher
79	Finger
80	HTTP
110	POP3
115	SFTP
161	SNMP
162	SNMP traps

ADSL Configuration

The ADSL Configuration page allows users to set the configuration for ADSL protocols.

Main Menu (Advanced)	-	AD	SL Configuration
BASIC OnePage Setup		Enabled	Trellis
hide advanced settings ADMINISTRATION		Autocense - G.dmt first 💌	Handshake Protocol
<u>WAN</u> LAN		Tip/Ring •	Wiring Selection
		Enabled -	Bit Swapping (No system reboot needed)
VorAl Port Forwarding ADSL Configuration RIP Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password System Log Code Unders		Settings need to be saved to Flash and the	Submit Reset
Status			
Router ADSL WAN ATM TCP connections Learned MAC Table	_		

- *Trellis:* This field allows the user to enable or disable the Trellis Code. By default, it is always enabled.
- *Handshake Protocol:* This field allows the user to select the ADSL handshake protocol.
- *Wiring Selection:* This field allows the user to enter the wiring selection for the RJ-11. Tip/Rip is the default for the board without the inner/outer pair relay.
- *Bit Swapping:* This field allows the user to enable or disable the upstream bit swapping.
- **Note:** Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.
RIP Configuration

The RIP System Wide Configuration page allows the user to set the configuration for each Interface (PVCs, PPP Sessions, USB and LAN).

Main Menu (Advanced)	1	RIP System Wide Configuration
BASIC • OnePage Setup		RIP Duskled 💌
ADMINISTRATION		Border Gateway Enabled 🔽
WAN LAN DNO		Supply Interval Seconds
<u>DNS</u> NAT		Expire Timeout 180 Seconds
Port Forwarding ADSL Configuration		Garbage Timeout 120 Seconds
Firewall Diagnostic Test		Advanced Configuration
Route Table MAC Filtering SECURITY		Submit Reset
Admin Password User Password Misc Configuration		Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
System Log Code Update		
Status		
Router ADSL WAN ATM TCP connections Learned MAC Table		

Interface: This field allows the user to choose the Interface (PVCs, PPP Sessions, USB and LAN), for the RIP to be configured.

Enable: This field allows the user to Enable (Yes) or Disable (No) the Specified interface for RIP.

Supplier: This field allows the user to select the Supplier Mode (RIP Transmit).

□ Disabled: The supplier transmit is disabled.

- □ V1 BC: The supplier transmits in RIPv1 Broadcast.
- □ V2 BC: The supplier transmits in RIPv2 Broadcast.
- □ V2 MC: The supplier transmits in RIPv2 Multicast.

Listener: This field allows the user to select the Listener Mode (RIP Receive).

□ V1: The listener receives the RIPv1 only.

□ V2: The listener receives the RIPv2 only.

 \Box V1+V2: This listener receives the both RIPv1 and RIPv2.

Supplier and Listener are based on section 4.1 "Compatibility Switch" in RFC 1723.

Current RIP Settings: This field displays the each interface's RIP status.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Firewall

The Firewall page allows users to configure various database/firewall options and Inbound/Outbound policies for controlling Inbound/Outbound traffic.

Main Menu (Advanced)	-	Configuration Firewall
Main Menu (Advanced) BASIC OnePage Setup Inde advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration Firevail Diagnostic Test Route Tablet MAC Filtering SECURITY Admin Password		Configuration Firewall Conexant Firewall Version: 3.2.1 Conexant firewall allows users to configure various databases/firewall options and Inbound/Outbound policies for controlling Inbound/Outbound traffic. Advanced Options: The following firewall options are configurable for advanced firewall feature: - Protection Folicy Hacker Log - Service Filtering Firewall Databases: The following databases are configurable for setting inbound/outbound policies: - If Group - Service Croup - Service Oroup - Service Oroup - Time Window
<u>System Log</u> <u>Code Update</u>		Inbound/Outbound Policies: The following policies are configurable for controlling traffic: - Inbound Policy - Outbound Policy
Status Router ADSL WAN ATM TCP connections Learned MAC Table		Firewall Disabled 💌 Submit

Firewall: This field allows the user to Disabled or Enabled Firewall.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Protection Policy



IP Spoofing checking: IP spoofing is when an unauthorized user inserts the IP address of an authorized user into the IP packets in order to gain access to a network. Selecting this option will allow the firewall to check for and filter out this discrepancy.

- **Ping of Death checking:** Ping of Death is a type of DoS attack that uses a malformed ICMP data packet that contains unusually large amounts of data that causes TCP/IP to crash or behave irregularly. Enabling this will allow the firewall to filter out packets containing Ping of Death properties.
- Land Attack checking: Land attack is a type of DoS attack that works by sending a spoofed packet containing the same source and destination IP address and port (the victim's IP address). This packet contains a connection request, resulting in a handshake process. At the end of the handshake, the victim sends out an ACK (ACKnowledge) request. Since the source and the destination are the same, the victim receives the ACK request it just sent out. The received data does not match what the victim is expecting, so it retransmits the ACK request. This process repeats until the network crashes. Enabling the will allow the firewall to filter out possible Land Attack packets.
- **Reassembly Attack checking:** Reassembly Attack is a type of DoS attack that exploits the weakness of the IP protocol reassembly process. As discussed earlier in this user guide, packets undergo fragmentation when they exceed a certain maximum size. Certain criteria define the packet fragmentation process so that packets can be reassembled properly. In reassembly attack, the sub-packets have malformed criteria (fragment offset), which can easily cause a system to crash, freeze, or reboot. Enable this option to check for and filter out Reassembly Attack packets.
- **SYN Flooding checking:** Syn flooding is a type of DoS attack that is accomplished by not sending the final acknowledgement to the receiving server's SYN-ACK (SYN chronize-ACKnowledge) in the final part of the handshake process. This causes the serve to keep signaling until it is timed out. When a flood (many) of these attacks are sent simultaneously, the server will probably overload and crash. Enable SYN Flooding checking to filter out possible SYN flood packets.
- **ICMP Redirection checking:** Also known as an ICMP storm attack or smurf attack, ICMP redirection is another form of DoS. This attack is performed by sending ICMP echo requests to a broadcast network node. The return IP address is spoofed and replaced by the victim's own address, causing it to send the request back to itself. This causes the broadcast address to send it out to all the network nodes in the broadcast area (usually the entire LAN). In turn, all those recipients resend it back to the broadcast. The process repeats itself, gaining more amplitude through each iteration and eventually causing a traffic overload and crashing the network. Enable ICMP Redirection checking to filter out packets

containing the threat.

- **Source Routing checking:** Source routing gives the sender of a packet the ability to determine the exact route that an IP packet takes to get to the destination. However, source routing can be used for malicious reasons. Using a source routed packet, the sender could find out important information about nodes in a network, making it easy to exploit any weakness. Enabling Source Routing checking will cause the firewall to filter out any packet with Source Routing properties.
- *WinNuke Attack checking:* WinNuke exploits a large networking bug found in Windows 95 and NT. WinNuke sends erroneous OOB (Out-of Band) data that Windows is unable to process, causing the target computer to crash. Enable this if you are running an early (95 or NT) version of Windows that is vulnerable to this attack.
- **Note:** Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Hacker Log

This page allows you to configure which Protection Policy (see previous section) violations to log for admin viewing.

Main Menu (Advanced)	1	Configuration Firewall Hacker Log	
BASIC • OnePage Setup		Alert Log:	Log Database Properties:
hide advanced settings ADMINISTRATION WAN LAN DNS NAT		SYN Flooding Fing of Death IP Spoofing Win Nuke	- Log Frequency: Every ^{[100} records/event.
<u>NAL</u> Port Forwarding <u>ADSL Configuration</u> <u>RIP Configuration</u> <u>Firewall</u> Diagnostic Test		General Log: General Attacks Deny Policies	
Route Table MAC Filtering SECURITY Admin Password User Password Misc Configuration System Log		Allow rolicies	Reset Submit
• <u>Code Opdate</u> Status			
Router ADSL WAN ATM TCP connections Learned MAC Table			

Alert Log: Enable/ Disable for SYN Flooding, Ping of Death, IP Spoofing, and WinNuke (all of these are explained in the previous section). Enable to log violations of individual policies.

General Log

Deny Policies: Enabling this will add Deny Policy violations to the log.

Allow Policies: Enabling this will add Allow Policy acceptances to the log.

- Log Frequency: This field lets you specify how many records to keep of each event. Default is 100. Range for Log Frequency Field is 1-65535.
- **Note:** Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Service Filtering

Service Filtering allows you to disable service request from certain sources.



Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Firewall Databases:

IP Group

The IP Group lets you specify IP Addresses (Single or Range) and Subnet Masks and assign them to a group name for easy use when configuring inbound and out bound policies for the firewall.

Main Menu (Advanced)	- <u>-</u>	Configuration Firewall I	P Group			
BASIC OnePage Setup 			No Entri	es in IP Group Data	ubase	
hide advanced settings ADMINISTRATION		IP Entry Name	IP addr. 1	IP addr. 2	IP/Mask	
VVAN LAN DNC					Single IP 💌	Add/Modify this entry
NAT Rott Forwarding						
ADSL Configuration RIP Configuration						
Firewall Diagnostic Test						
Route Table MAC Filtering						
ECURITY Admin Password						
<u>User Password</u> <u>Misc Configuration</u>						
System Log Code Update						
Status						
<u>ADSL</u>						
<u>VVAN</u> <u>ATM</u> <u>TCD</u>						
Learned MAC Table	-					

- *IP Entry Name:* This is the name you assign to the group of IP addresses and subnet masks. (The IP Entry Name can be up to 19 characters.)
- *IP addr. 1:* This is the IP address or subnet mask you are specifying when creating a groups.
- *IP addr. 2:* This field is only active if you select to group a range of IP addresses or subnet masks, in which case this is the end address of that range whereas the IP addr 1 is the first address of that range.
- *IP/Mask:* This field allows you to specify the address type assigned to the group.

Single IP: This will let you specify one IP address for a given group.

- *IP Range:* This will let you specify a range of IP addresses for a given group, starting with IP addr 1 and ending with IP addr 2.
- Subnet Mask: This will let you specify a range of subnet masks for a given group.

Service Group

The Service Group lets you specify a Port and assign it to a group name for easy use when configuring inbound and outbound policies for the firewall.

Main Menu (Advanced)	Configu	ration Firewall Service (Group			
BASIC OnePage Setup		No E	intries in Sei	vice Group	Database	
hide advanced settings ADMINISTRATION		Service Entry Name	TCP/UDP	Port #		[
WAN LAN					Add/Modify this entry	
DNS NAT Det Ferunding						
ADSL Configuration BIP Configuration						
Firewall Diagnostic Test						
Route Table MAC Filtering						
ECURITY Admin Password						
<u>User Password</u> <u>Misc Configuration</u>						
System Log Code Update						
Status						
Router ADSL WAN ATM						
TCP connections Learned MAC Table						

Service Entry Name: This is the name you assign to the group containing the port number. (The Service Entry Name can be up to 19 characters.)

TCP/UDP: This specifies whether the port goes through TCP or UDP.

Port #: This is the port number associated with the group name. Range for Port # 1-65535.

Time Window

The Time Window lets you specify certain time periods and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

Main Menu (Advanced)	<u>Config</u> u	<u>ıration</u> <u>Firewall</u> Time Gr	oup	
BASIC OnePage Setup			No Entries in Time Window Database	•
hide advanced settings ADMINISTRATION		Time Window Name	Time Period	
VWAN LAN DNS NAT			from Monday •, 01 • : 00 • AM • to Monday •, 01 • : 00 • AM •	Add/Modify this entry
Port Forwarding ADSL Configuration RIP Configuration Firowall		,		<u></u>
Diagnostic Test Route Table MAC Filtering				
ECURITY Admin Password User Password Misc Configuration System Log Code Update				
Status				
Router ADSL WAN ATM TCP connections Learned MAC Table	1			

Time Window Name: This is the name you assign to the group that is given the time designation. (The Time Window Name can be up to 19 characters.)

Time Period: This field allows you to specify the time period for both start time and end time by selecting the day, hour, minute, and AM/PM.

Inbound/ Outbound Policies:

Inbound Policy

The Inbound Policy allows you to filter inbound (from the WAN into the user side LAN) packets based on a set of rules. This enables you to deny access from different sources and thus increase security.

Main Menu (Advanced)	Configuration Firewall Inbound Policy	
BASIC	Inbound Policy	
<u>OnePage Setup</u> <u>hide advanced settings</u> ADMINISTRATION	No Entries in Inbound Policy Database	
WAN LAN DNS	Adding New Policy	
NAT Port Forwarding ADSL Configuration	SIC IP: ~ Any P J DB:	None 💌
ADSE Configuration RIP Configuration Firewall	Dest IP: ~ Any P J DB:	None -
Diagnostic Test Route Table MAC Eiltering	Src Port: Aay Port	
SECURITY Admin Password	Dest Port: ~ Any Port V DB:	None 💌
User Password Misc Configuration System Log	Transport Protocol: All Protocol	
Code Update Status	Filtering Action: Allow -	
<u>Router</u> <u>ADSL</u>	Time Window Filtering: None 💌	
WAN ATM TCP connections Learned M&C Table	AddModify Inbound Policy	

- *Src IP:* This specifies the Source IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and Subnet Masks that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu has four options:
- **Any IP:** Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.
- **Single IP:** Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.
- *IP Range:* Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.
- *Mask Range:* Selecting this will enable you to select a network to which the policy will apply. The Network IP Address must be entered into the first entry field and the Subnet Mask of Network IP address must be entered into the second entry field.
- **Dest IP:** This specifies the Destination IP for the Inbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and network that will be

affected by the policy. See Src IP above for configuration detail.

- *Src Port:* This specifies the Source Port for the Inbound Policy. This is the external (WAN side, outside of the firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:
- *Any Port:* Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.
- *Single Port:* Selecting this will cause only one Port to be affected by the policy. This port will need to be specified by the user in the first Port entry field.
- *Port Range:* Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

Safe Ports: Any port greater than 1024 (1025-65535) is considered a safe port.

- **Dest Port:** This specifies the Destination Port for the Inbound Policy. This is the internal (LAN side, behind the firewall) Port that will be affected by the policy. See Src Port above for configuration detail.
- *Transport Protocol:* This specifies the Transport/ Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP and GRE.

Filtering Action: This specifies what action the policy takes:

- **Allow:** Selecting this will cause the policy to allow packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.
- **Deny:** Selecting this will cause the policy to deny packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.
- *Time Window Filtering:* This field allows you to select a certain time frame from the Time Group in which this policy will be active.
- **DB:** Short for Database, this field allows you to select a user-defined IP Group for the Src IP and Dest IP fields and user-defined Service Group for the Dest Port. User-defined IP and Service Groups are created in IP Group and Service Group pages.

Outbound Policy

The Outbound Policy allows you to filter outbound (from the user side LAN to the WAN) packets based on a set of rules. This enables you to deny access to different sources and thus increase security.

Main Menu (Advanced)	1	Configuration	Firewall Outbound Policy
BASIC			Outbound Policy
hide advanced settings ADMINISTRATION			No Entries in Outbound Policy Database
<u>WAN</u> <u>LAN</u> DNS			Adding New Policy
NAT Port Forwarding			Src IP: ~ Any IP V DB: None V
ADSL Configuration RIP Configuration Firewall			Dest IP: ~ Any P V DB: None V
Diagnostic Test Route Table MAC Eiltering			Src Port: ~ Any Port V
SECURITY Admin Password			Dest Port: ~ Any Port • DB: None •
<u>User Password</u> <u>Misc Configuration</u> System Log			Transport Protocol: All Protocol
Code Update			Filtering Action: Allow 💌
Router ADSL			Time Window Filtering: None -
• ADSL • WAN • ATM			Add/Modify Outbound Policy
<u>TCP connections</u> <u>Learned MAC Table</u>	•		

- *Src IP:* This specifies the Source IP for the Outbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu has four options:
- **Any IP:** Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.
- **Single IP:** Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.
- *IP Range:* Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.
- *Mask Range:* Selecting this will enable you to select a network to which the policy will apply. The Network IP Address must be entered into the first entry field and the Subnet Mask of Network IP address must be entered into the second entry field.
- **Dest IP:** This specifies the Destination IP for the Outbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and network that will be affected by the policy. See Src IP above for configuration detail.

- *Src Port:* This specifies the Source Port for the Outbound Policy. This is the internal (LAN side, behind firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:
- *Any Port:* Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.
- *Single Port:* Selecting this will cause only one Port to be affected by the policy. This port will need to be specified by the user in the first Port entry field.
- **Port Range:** Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

Safe Ports: Any port greater than 1024 (1025-65535) is considered a safe port.

- **Dest Port:** This specifies the Destination Port for the Outbound Policy. This is the external (WAN side, outside of the firewall) Port that will be affected by the policy. See Src Port above for configuration detail.
- *Transport Protocol:* This specifies the Transport/ Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP and GRE.

Filtering Action: This specifies what action the policy takes:

- **Allow:** Selecting this will cause the policy to allow packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.
- **Deny:** Selecting this will cause the policy to deny packet transfer from the Src IP through the Src Port to travel through the Dest Port to the Dest IP. All of these are specified above and must be configured by the user.
- *Time Window Filtering:* This field allows you to select a certain time frame from the Time Group in which this policy will be active.
- **DB:** Short for Database, this field allows you to select a user-defined IP Group for the Src IP and Dest IP fields and user-defined Service Group for the Dest Port. User-defined IP and Service Groups are created in IP Group and Service Group pages.

Diagnostic Test

The Diagnostic Test page shows the test results for the physical layer and protocol layer for both LAN and WAN sides.

Main Menu (Advanced)	Diagnostic Test: Test	Complete
BASIC OnePage Setup hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration Firewall Diagnostic Test ROUT Fable MAC Filtering SECURIY Admin Password User Password User Password Misc Configuration System Log Code Update	Checking LAN Connection Testing Ethernet LAN connection Checking ADSL Connection Testing ADSL Synchronization Checking Circuit O for Network Connection Test ATM OAM Segment Loop Back Test ATM OAM Segment Loop Back Test ATM OAM Segment Loop Back Test Ethernet connect to ATM Test PPRoPvc 0 PPPOE connection Test PPRoPvc 0 PPP Dayer connection Test PPPoPvc 0 PPP Dayer Connection Ping primary DNS Query DNS for www.conexant.com Ping www.conexant.com	PASS HELP FAIL HELP SKIPPED HELP SKIPPED HELP SKIPPED HELP SKIPPED HELP SKIPPED HELP SKIPPED HELP SKIPPED HELP SKIPPED HELP SKIPPED HELP
Status • Router • ADSL • WAN • TCP connections • Learned MAC Table		

- **Testing Ethernet LAN Connection:** This test checks the Ethernet LAN interface connection.
- *Testing ADSL Synchronization:* This test checks the ADSL showtime. If this test returns FAIL, all other tests will be skipped.
- **Test ATM OAM segment Loop Back:** This test sends ATM OAM F5 Segment loop-back request cells to the CO. This test will pass if response cell is received. Some service providers might not support this test. If this test fails consistently and the ADSL modem does not seem to be working, make sure the VPI and VCI are configured correctly.
- **Test ATM OAM End-to-End Loop Back:** This test sends ATM OAM F5 End to End loop back request cells to the CO. This test will pass if response cell is received. Some service providers might not support this test. If this test return FAIL consistently and the ADSL modem does not seem to be working, make sure the VPI and VCI are configured correctly.
- Test Ethernet Connect to ATM: This test checks the ATM AAL5 module is loaded correctly.
- Test PPP Layer Connection: This test checks the PPP authentication.
- **Test IP Connect to PPP:** This test checks a valid IP address assigned from the service provider. Please note that on some ADSL services this test may fail despite the fact that you have connected correctly.

- *Ping Primary DNS:* This test checks the primary DNS can be reached through pin request.
- *Query DNS for <u>www.conexant.com</u>:* This test checks the host name can be resolved to IP address though domain name servers.
- *Ping <u>www.conexant.com</u>:* This test checks the specified host can be reached through pin request.

Router Table

The Router Table page displays routing table and allows the user to manually enter the routing entry. The routing table will display the routing status of Destination, Netmask, Gateway and Interface. The interface br0 means the USB interface; Io0 means the loopback interface and ppp1 means the PPP interface. The Gateway is the learned Gateway.

Main Menu	Route Table						
BASIC							
OnePage Setup hide advanced settings	Destination Netmask Gateway Interface						
	10.0.0.0 255.255.255.0 10.0.0.2 br0						
• <u>LAN</u>	127.0.0.1 255.0.0.0 127.0.0.1 100						
NAT							
Port Forwarding ADSL Configuration	System Default Gateway Configuration						
RIP Configuration Firewall	o None						
Diagnostic Test Route Table	· Auto						
MAC Filtering SECURITY	C Select Interface						
Admin Password	C Specify IP						
<u>Misc Configuration</u>	execute						
System Log Code Update	Route Configuration						
Status							
Router ADSL	© Specify IP						
WAN ATM	C Select Interface Prc0						
TCP connections	Add V Submit Reset						
Main Menu (Advanced)	System Default Gateway Configuration						
Main Menu (Advanced) BASIC	System Default Gateway Configuration						
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings	System Default Gateway Configuration C None C Auto						
Main Menu (Advanced) BASIC • OnePage Setup • bide advanced settings ADMINISTRATION • WAN	System Default Gateway Configuration C None C Auto C Select Interface						
Main Menu (Advanced) BASIC OnePage Setup	System Default Gateway Configuration None Auto Select Interface Specify IP						
Main Menu (Advanced) BASIC • • OnePage Setup • Main Stratton • MAN	System Default Gateway Configuration C None C Auto C Select Interface Prc0 Specify IP C Specify IP						
Main Menu (Advanced) BASIC • OnePage Setup • Idle advanced settings ADMINISTRATION • WAN • LAN • DNIS • NAT • Port Forwarding • ADSL Configuration • BIP Configuration • BIP Configuration	System Default Gateway Configuration None Auto Select Interface Specify IP Excoute						
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings ADMINISTRATION • WAN • UNA • UNA • NAT • Port Forwarding • ADSL Configuration • RIP Configuration • RIP Configuration • RIP Configuration • RIP Configuration	System Default Gateway Configuration None Auto Select Interface Select Interface C Specify IP						
Main Menu (Advanced) BASIC Defage Setup bide advanced settings ADMINISTRATION WAN LAN DNS NAT Port Forwarding ADSL Configuration Firewall Diagnostic Test Route Table WAN Bottoman	System Default Gateway Configuration C None C Auto C Select Interface Ip Pico C Specify IP C Sp						
Main Menu (k-dvanced) BASIC • OnePage Setup • bide advanced settings ADMINISTRATION • WAN • LAN • DNS • NAT • One Forwarding • ADSL Configuration • Firewall • Diagnostic Test • Ruck Table • MAC Filtering SECURITY	System Default Gateway Configuration None Auto Select Interface Forc0 Route Configuration Destination Netmask Gateway Select IP						
Adin Menu (Advanced) BASIC • DinePage Setup • bide advanced settings ADMINISTRATION • WAN • AN • DNS • NAT • Port Forwarding • ADSL Configuration • RPC C	System Default Gateway Configuration None Auto Select Interface Specify IP mexeme Route Configuration Destination Netmask Gateway Specify IP Select Interface Destination Netmask Gateway Select Interface Select Interface Select Interface						
Main Menu (Advanced) BASIC • • OnePage Setup • • Ide advanced settings Advantstrations ADMINISTRATION • • UAN • • DAN • • DAN • • MAN • • ANI • • Port Forwarding • • ADSL Configuration • • Firewall • • Bignostic Test • • Adamin Password • • User Password • • Mac Configuration • • System Log •	System Default Gateway Configuration None Auto Select Interface Specify IP recome Route Configuration Destination Netmask Gateway Specify IP Configuration Destination Netmask Gateway Select Interface Select Interface Add Submit Add						
Main Menu (Advanced) BASIC • OnePage Setup • Ide advanced settings ADMINISTRATION • WAN • LAN • NAS • NAT • Port Forwarding • ADSL Configuration • Firewall • Diagnostic Test • Admin Password • Lar Password • System Log • System Log • Code Update	System Default Gateway Configuration None Auto Select Interface PPCO Select Interface PPCO Select Interface PPCO Configuration Destination Netmask Gateway Select Interface PPCO Add Souther Recet Note: Save changes to flash to restore on power up.						
Main Menu (Advanced) BASIC • OnePage Setup • Ide advanced settings ADMINISTRATION • WAN • LAN • NAT • Port Forwarding • ADSL Configuration • RIP Configuration • Rive All Filtering SECURITY • Admin Password • User Password • System Log • Code Update Status	System Default Gateway Configuration None Auto Select Interface PPCO Select Interface PPCO Route Configuration Destination Netmask Gateway Add Select Interface PPCO Add Select Interface PPCO Manually Configured Routes						
Main Menu (Advanced) Advanced	System Default Gateway Configuration None Auto Select Interface []= Pxc0] Select Interface []= Pxc0] Configuration Destination Netmask Gateway Configuration Destination Netmask Gateway Configuration Destination Netmask Gateway Configuration Netmask Gateway Configuration Netmask Gateway Configuration Netmask Gateway Note: Save changes to flash to restore on power up. Manually Configured Routes						
Main Menu (Advanced) BASIC • OnePage Setup • bide advanced settings ADMINISTRATION • WAN • LAN • DNS • NAT • Port Forwarding • ADSL Configuration • Firewall • Diagnostic Test • Route Tablé • MAC Filtering SECURITY • Gate Update Status • Router • ADSL • WAN • TM	System Default Gateway Configuration None Auto Select Interface Select Interface						

Note: Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

MAC Filtering

The MAC Filtering configuration page allows the user to set the configuration of IP filtering. Enable and Disable MAC filtering by selecting the "Yes" or "No" radio buttons.

Main Menu (Advanced)	-			MAC Filtering	
BASIC OnePage Setup			Filteri	ng Enable: 🔿 Yes 💿 No	
hide advanced settings ADMINISTRATION			Filtering .	Action: 🗢 Block 🖲 Forwa	rd
• <u>WAN</u> • <u>LAN</u>		ID	SIC MAC	Dest MAC	Туре
DNS NAT Port Forwarding ADSL Configuration RIP Configuration Firewall Diagnostic Test MAC Filtering SECURITY Admin Password User Password User Password Misc Configuration System Log Conde Undate		1 (1) MAC (2) Ether (3) The t	2 address format : aab rnet type format: aabb maximum number of e	xcoddeeff, 00000000000 0000 indicates DON'T C ntries is 16	indicates DON'T CAR ARE
Status					
Router ADSL WAN ATM TCP connections Learned MAC Table					

- **Source MAC:** When the bridge filtering is enabled, enter the Source Mac address, Select Block and click Add. Then all incoming WAN and LAN Ethernet packets matched with this source MAC address will be filtered out. If the Forward is selected, then the packets will be forwarded to the destination PC.
- **Destination MAC:** When the bridge filtering is enabled, enter the Destination MAC address, select Block and click Add. Then all incoming WAN and LAN Ethernet packets matched with this destination MAC address will be filtered out. If the Forward is selected, then the packets will be forwarded to the destination PC.
- **Type:** Enter the hexadecimal number for the Ethernet type field in Ethernet_II packets.

Security

The links under Security are only to be accessed and configured, when it is login with administrator login name and password.

Admin Password

The Admin Password Configuration page allows the user to set the password for administrator.

Main Menu (Advanced)	Admin Level Username/Password Configuration
BASIC	Do not use '&' in the password
OnePage Setup	
 <u>hide advanced settings</u> 	
ADMINISTRATION	Current Password
• WAN	Chart Harmony Addition
LAN DNC	Select Username autum
DINS NAT	Salast Pasaword
Port Forwarding	
ADSL Configuration	Retype Password
RIP Configuration	
Firewall	Submit Reset
 <u>Diagnostic Test</u> 	
Route Table	Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
MAC Filtering	
SECURITY	
User Password	
Misc Configuration	
System Log	
Code Update	
Status	
Router	
ADSL	
WAN	
• <u>ATM</u>	
<u>TCP connections</u>	
Learned MAC Table	

User Name: admin

Password (default): epicrouter

Note: Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

User Password

The User Password Configuration page allows the Admin user to set the password for the general user. When logged in as a general user you can view the basic status.

Main Menu (Advanced)	User Level Username/Password Configuration
BASIC OnePage Setup	Do not use '&' in the password.
hide advanced settings ADMINISTRATION	Current Password
LAN	Select Username user
NAT Dat Featuration	Select Password
ADSL Configuration	Retype Password
Firewall Discrete Test	Submit Reset
Route Table MAC Ellevine	Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.
ECURITY	
Admin Password User Password Misc Configuration System Log	
<u>Code Update</u>	
Router	
ADSL WAN ATM TCP connections Learned MAC Table	J

User Name: user

Password (default): password

Note: Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

Misc Configuration

The Miscellaneous Configuration allows the user to set all the miscellaneous configurations.

r				
Main Menu (Advanced)	Î	Miscellaneous	Configuration	^
BASIC				
OnePage Setup bide advanced settings		HTTP server access		
ADMINISTRATION		• All		
WAN LAN		 Restricted 		
• <u>DNS</u>		🔽 LAN		
NAI Port Forwarding		WAN Specify IP	10.0.0.10	
ADSL Configuration RIP Configuration			211000	
<u>Firewall</u>		Subnet Mask	255.000	
Diagnostic Test Route Table		HTTP server port	80	
MAC Filtering SECURITY		HTTP Password Protection	Enabled	
Admin Password				
User Password Misc Configuration		FTP server	Enabled	
System Log Code Undate		Disable WAN side ETP access		
Status			Distill	
Router		IFIF SERVER		
ADSL MAN				
• <u>ATM</u>		🔽 Disable WAN side access		
<u>TCP connections</u> Learned MAC Table				
	<u> </u>		The state of the s	<u> </u>
	<u>_</u>	DMZ HOST IP	0.0.0	<u> </u>
Main Menu (Advanced)	•	DMZ HOST IP	0000	
Main Menu (Advanced) BASIC • OnePage Setup	<u>*</u>	DMZ HOST IP	0.0.0	
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings	•	DMZ HOST IP 	Disabled -	
Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION V/AN	•	DMZ HOST IP IGMP Proxy PPP Half Bridge	0.0.00 Disabled 💌	
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings ADMINISTRATION • VVAN • LAN • DNS	•	DMZ HOST IP 	0.000 Disabled • Disabled • Disabled •	
Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION VVAN LAN DNS NAT	•	DMZ HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up	0.0.00 Disabled • Disabled • Disabled •	
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings ADMINISTRATION • WAN • LAN • DNS • NAT • Port Forwarding • ADSL Configuration	<u>•</u>	DMZ HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up	0.0.00 Disabled • Disabled • Disabled •	
Main Menu (Advanced) BASIC 0.nePage Setup hide advanced settings ADMINISTRATION • WAN LAN DNS • NAT • Port Forwarding • ADSL Configuration • RIP Configuration • Firrewall	•	DMZ HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTP	0.0.00 Disabled • Disabled • Disabled •	
Main Menu (Advanced) BASIC • OnePage Setup • hide advanced settings ADMINISTRATION • WAN • LAN • DNS • NAT • Port Forwarding • ADSL Configuration • RIP Configuration • Firewall • Diagnostic Test	×	DMZ HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTP Time Zone	0.0.00 Disabled • Disabled • Disabled • Enabled •	
Main Menu (Advanced) BASIC 0 OnePage Setup 1 hide advanced settings ADMINISTRATION • WAN LAN DNS • NAT • Port Forwarding • ADSL Configuration • RIP Configuration • RIP Configuration • RIP Configuration • Rirewall Diagnostic Test • Route Table • MAC Fittering	*	DMZ HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTP Time Zone	0.0.00 Disabled • Disabled • Disabled • Enabled •	
Main Menu (Advanced) BASIC 0.0nePage Setup 1.11 ibide advanced settings ADMINISTRATION V.WAN LAN DNS NAT Port Forwarding ADSL Configuration R IP Configuration R IP Configuration Firewall Diagnostic Test Route Table MAC Firefing SECURITY	<u>•</u>	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTF Time Zone Daylight Saving Time	0.0.00 Disabled • Disabled • Disabled • Enabled • (+10) Brisbane •	
Main Menu (Advanced) BASIC 0.nePage Setup bide advanced settings ADMINISTRATION • WAN LAN DNS • NAT • Port Forwarding • ADSL Configuration • RIP Configuration • RIP Configuration • RIP Configuration • RIP Configuration • RIP Configuration • Rirewall • Diagnostic Test • Route Table • MAC Filtering SECURITY • Admin Password User Password	<u> </u>	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTF Time Zone Daylight Saving Time User defined Time server	0.0.00 Disabled • Disabled • Disabled • Esabled • (+10) Brisbane • No • 0.0.00	
Main Menu (Advanced) BASIC 0.0nePage Setup 1.11 inite advanced settings ADMINISTRATION V.WAN 1. LAN DINS NAT Port Forwarding ADSL Configuration 1.11 Configuration 1.11 Configuration 1.11 Configuration 1.12 Config	<u> </u>	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTP Time Zone Daylight Saving Time User defined Time server	0.0.0 Disabled v Disabled v Disabled v Enabled v (+10) Brisbane v No v 0.0.0	
Main Menu (Advanced) BASIC 0.0nePage Setup 1.11 inite advanced settings ADMINISTRATION V.WAN 1. LAN DINS NAT Port Forwarding ADSL Configuration 1.11 Configuration 1.11 Configuration 1.11 Configuration 1.12 Config	·	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTP Time Zone Daylight Saving Time User defined Time server ADSL Status Refresh Rate (seconds)	0.0.00 Disabled Disabled Disabled Finabled (+10) Brisbane No 0.0.00	
Main Menu (Advanced) BASIC 9. OnePage Setup 1. hide advanced settings ADMINISTRATION 9. VXAN 9. LAN 0. DNS 9. NAT 9. Onfiguration 9. RIP Configuration 9. RIP Configuration 9. Ripervall 10. Diagnostic Test 9. Advin Password 10. Security 9. Advin Password 10. Security 9. Advin Password 10. Security 10. Se	*	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTP Time Zone Daylight Saving Time User defined Time server ADSL Status Refresh Rate (seconds)	0.0.00 Disabled Disabled Disabled Finabled (+10) Brisbane No 2	
Main Menu (Advanced) BASIC 0.0nePage Setup 1. hide advanced settings ADMINISTRATION V. VAN 1. LAN DINS NAT Port Forwarding ADSL Configuration 1. RiP Configuration 1. RiP Configuration 1. RiP Configuration 1. Ripervall 0. Diagnostic Test 1. Route Table MAC Filtering SECURITY 2. Admin Password 0. User Password 0. User Password 0. User Password 0. System Log 0. Code Update Status 1. Router ADSL	*	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTP Time Zone Daylight Saving Time User defined Time server ADSL Status Refresh Rate (seconds) USB	0.0.00	
Main Menu (Advanced) BASIC 0.0nePage Setup 1. hide advanced settings ADMINISTRATION V.WAN 1. LAN DINS NAT Port Forwarding ADSL Configuration 1. RiP Configuration 1. RiP Configuration 1. RiP Configuration 1. Ripervall 0. Diagnostic Test 1. Route Table MAC Filtering SECURITY 2. Admin Password 0. User Password 0. User Password 0. User Password 0. System Log 0. Code Update Status 1. Router ADSL 1. Router 1. Rout	*	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTF Time Zone Daylight Saving Time User defined Time server ADSL Status Refresh Rate (seconds) USB	0.0.00 Disabled • Disabled • Disabled • Eastled • (+10) Bristene • No • 0.0.00 2 Eastlet •	
Main Menu (Advanced) BASIC 0.0nePage Setup 1. hide advanced settings ADMINISTRATION V.WAN 1. LAN DINS NAT Port Forwarding ADSL Configuration 8. HIP Configuration 1. HIP Configuration 1. HIP Configuration 1. HIP Configuration 1. Jaar Dessword 1. Jaa	×	DM2 HOST IP IGMP Proxy PPP Half Bridge PPP Reconnect on WAN Access Connect PPP when ADSL link is up SNTF Time Zone Daylight Saving Time User defined Time server ADSL Status Refresh Rate (seconds) USB	0.0.00 Disabled • Disabled • Disabled • Eastled • (+10) Bristene • No • 0.0.00 2 Eastled •	

HTTP server access: This field allows the user to configure the Web pages can be accessed from.

ALL: When this field is checked, it allows both WAN and LAN access to the Web pages.

Restricted LAN: This field allows the Web pages access from LAN side.

Restricted WAN Specified IP & Subnet Mask: This field allows the Web access from WAN side with a specify IP and Subnet Mask.

HTTP server port: This field allows the user to specify the port of the Web access.

FTP server: This field allows the user to Enable or Disable the FTP connection. If you want FTP access from the WAN side you must ensure there are no port forwards for port 21.

TFTP server: This field allows the user to Enable or Disable the TFTP connection.

DMZ: A DMZ (De-Militarized Zone) is added between a protected network and an external network, in order to provide an additional layer of security. When there is a suspected packet coming from WAN, the firewall will forward this packet to the DMZ host.

DMZ Host IP: The IP address of the DMZ host at LAN side.

DHCP Relay: If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on the WAN side of a network. To have this function working properly, please disable the NAT to run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

DHCP Target IP: The DHCP server runs on WAN side.

- *IGMP Proxy:* Here is the global setting for IGMP Proxy. If it is enabled, then the enabled IGMP Proxy on WAN PVCs will be working. Otherwise, no WAN PVC can have IGMP Proxy working on it.
- **PPP connect on WAN access:** If it is enabled, the PPP session will be automatically established when there is packet wants to go out the WAN.
- **PPP Half Bridge:** When the PPP Half Bridge is enabled, only one PC is able to access the Internet and the DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only the PC with the WAN IP address can access the Internet. This function should only be used if one computer will be allowed to connect to the internet (E.G a Software firewall computer or Proxy server).
- **Note:** Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

System Log

The System Log page shows the events triggered by the system.



To clear the System Log simply click on the Clear Log button.

Note: Click the **Submit** button to save the settings in temporary memory. If you make changes the configurations.

Code Update

The code Update page allows the user to upload new firmware to the ADSL Router.

Main Menu (Advanced) BASIC OnePage Setup hide advanced settings ADMINISTRATION WAN LAN DNS NAT Port Forwarding ADSL Configuration RIP C		Code Image Update Image Download Select Image Download is selected it will take a few seconds before you can select the file to be downloaded.
User Password Misc Configuration System Log Code Update		
Status • Router • ADSL • WAN • ATM • TCP connections • Learned MAC Table	- -	

To upload new firmware:

- 1. Download the latest firmware image from the website.
- 2. Save the file to your Desktop or other location.
- 3. Select the Browse button and locate the file saved in step 2.
- 4. Click on the Update button to start the process.
- 5. Once the upgrade has been completed the router will need to reboot.

Status

Router

The Home page shows the Firmware Version and WAN and LAN interface status.

 Inde auvandeu settings 						
ADMINISTRATION			Home Page			
• <u>WAN</u>						
DNS		BootCode Version: BC_CX82xxx_4.1.0.21				
• NAT	1	Firmware Versi	on: CX8	2xxx_4.1.0.21_S		
Port Forwarding		Customer Softw	are Version: 4.1.0).21_S		
ADSL Configuration						
<u>RIP Configuration</u>						
Firewall Disgregatio Test			WAN			
Boute Table						
MAC Filtering						
SECURITY		IP Address	Subnet Mask	MAC Address		
Admin Password			·		-	
User Password Miss Configuration						
System Log			TAN			
Code Update			LAN			
Status			Cubert Mark			
Router		IL Madless	Subnet Mask	MAC Addless		
ADSL		10.0.0.2	255.255.255.0	00:09:F3:00:00:8E		
WAN						
AIM TCP connections		Tetal	Number of Lor. I-	terfaces: 1		
Learned MAC Table		TOTAL	Number of Lan II.	nenaces. 1	-	
PPP Status	N	umber of etherne	et devices connecte	ed to the DHCP serv	er: 1	
Save Setting and Reboot		IP	Address MA	C Address		
					-	
					_	
hide advanced settings	J				<u>^</u>	
hide advanced settings ADMINISTRATION WAN	l					
hide advanced settings ADMINISTRATION WAN LAN	·		WAN		<u>*</u>	
hide advanced settings ADMINISTRATION WAN LAN DNS			WAN		^	
hide advanced settings ADMINISTRATION WAN LAN DNS NAT	J		WAN		1	
hide advanced settings ADMINISTRATION WAN LAN DNS NAT Port Forwarding DDCI Conformation		IP Address	WAN Subnet Mask	MAC Address	1	
hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration DIPL Configuration		IP Address	WAN Subnet Mask	MAC Address		
hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration RiP Configuration Firewall		IP Address	WAN Subnet Mask	MAC Address	A	
hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding ADSL Configuration RiP Configuration Firewall Diagnostic Test	 	IP Address	WAN Subnet Mask	MAC Address	*	
hide advanced settings ADMINISTRATION WAIN UAN DNS NAT Port Forwarding AOSL Configuration Firewall Diagnostic Test Route Table		IP Address	WAN Subnet Mask LAN	MAC Address	•	
hide advanced settings ADMINISTRATION WAN UAN DNS NAT Port Forwarding AOSL Configuration RIP Configuration Firewall Diagnostic Test Route Table MAC Filtering SECUENTY		IP Address	WAN Subnet Mask LAN	MAC Address		
hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding AOSL Configuration Fireval Diagnostic Test Route Table MAC Filtering SECURITY Admin Password		IP Address	WAN Subnet Mask LAN Subnet Mask	MAC Address	^	
hide advanced settings ADMINISTRATION WAN UAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration Firevall Diagnositic Test Route Table MAC Filtering SECURITY Admin Password User Password		IP Address	WAN Subnet Mask LAN Subnet Mask	MAC Address		
hide advanced settings ADMINISTRATION V/AN UAN DNS NAT Pot Forwarding AOSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password		IP Address IP Address 10.0.0.2	WAN Subnet Mask LAN Subnet Mask 255.255.255.0	MAC Address MAC Address 00:09:F3:00:00:8E		
hide advanced settings ADMINISTRATION WAN UAN DNS NAT Port Forwarding AOSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password Use		IP Address IP Address 10.0.0.2	WAN Subnet Mask LAN Subnet Mask 255.255.255.0	MAC Address MAC Address 00:09:F3:00:00:8E		
hide advanced settings ADMINISTRATION VAN LAN DNS NAT Port Forwarding AOSL Configuration RIP Configuration Fireval Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password System Log Code Update		IP Address IP Address 10.0.0.2 Total	WAN Subnet Mask LAN Subnet Mask 255.255.255.0 Number of Lan Ir	MAC Address MAC Address 00:09:F3:00:00:81 iterfaces: 1		
hide advanced settings ADMINISTRATION V/AN UAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration Firevall Diagnositic Test Route Table MAC Fittering SECURITY Admin Password Misc Configuration System Log Code Update Status		IP Address IP Address I0.0.0.2 Total	WAN Subnet Mask LAN Subnet Mask 255.255.0 Number of Lan Ir	MAC Address MAC Address 00:09:F3:00:00:81 uterfaces: 1		
hide advanced settings ADMINISTRATION WAN UAN DNS NAT Port Forwarding AOSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password User Dasword System Log Code Update Status Router	 	IP Address IP Address 10.0.0.2 Total umber of etherne	WAN Subnet Mask LAN Subnet Mask 255.255.0 Number of Lan Ir t devices connected	MAC Address MAC Address 00:09:F3:00:00%E iterfaces: 1	▲	
hide advanced settings ADMINISTRATION WAIN UAN DNS NAT Port Forwarding AOSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password User Password System Log Code Update Status Router ADSL		IP Address IP Address 10.0.0.2 Total umber of etherne	WAN Subnet Mask LAN Subnet Mask 255.255.255.0 Number of Lan Ir et devices connecte	MAC Address MAC Address 00:09:F3:00:00:81 tterfaces: 1 tterfaces: 1 ed to the DHCP serv	▲	
hide advanced settings ADMINISTRATION WAN UAN DNS NAT Port Forwarding AOSL Configuration RIP Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password User Password User Password Status Router AOSL Code Update Status Router AOSL VAN VAN VAN	N	IP Address IP Address 10.0.0.2 Total umber of etherne	WAN Subnet Mask LAN Subnet Mask 255.255.255.0 Number of Lan Ir et devices connecte Address MA	MAC Address MAC Address 00:09:F3:00:00:81 iterfaces: 1 sd to the DHCP serv ic Address	▲	
hide advanced settings ADMINISTRATION VIAIN UAN UAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration Firewall Diagnositic Test Route Table MAC Fittering SECURITY Admin Password Misc Configuration System Log Code Update Status Router ADSL VVAN ATM TCP connections	N	IP Address IP Address 10.0.0.2 Total umber of etherne	WAN Subnet Mask LAN Subnet Mask 255.255.0 Number of Lan Ir et devices connecte Address MA	MAC Address MAC Address 00:09:F3:00:00:80 therfaces: 1 act to the DHCP serv AC Address	▲	
hide advanced settings ADMINISTRATION WAIN UAN DNS NAT Port Forwarding AOSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password User Password User Password Status Router AOSL Status Router AOSL WAN ATM TOP connections Learned MAC Table	N	IP Address ID Address ID 0.0.0.2 Total umber of etherner I IP I 1 I0.	WAN Subnet Mask LAN Subnet Mask 255.255.0 Number of Lan Ir et devices connecte Address MA	MAC Address MAC Address 00:09:F3:00:00:8E tterfaces: 1 tterfaces: 1 tterfaces: 2 Address Addres Address Addres	• • • • •	
hide advanced settings ADMINISTRATION WAN UAN DNS NAT Port Forwarding AOSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY Admin Password User Password User Password User Password User Password System Log Code Update Status Router ADSL WAN TCP connections Laamed MAC Table PPP Status		IP Address I0.0.0.2 Total umber of etherne I I I I I I I I I I I I I I I I I I I	WAN Subnet Mask LAN Subnet Mask 255.255.255.0 Number of Lan Ir et devices connecte Address MA 0.0.3 72:01	MAC Address MAC Address 00:09:F3:00:00:81 terfaces: 1 ed to the DHCP serv C Address 3:49:E7:2B:23	▲	
hide advanced settings ADMINISTRATION WAN UAN DNS NAT Port Forwarding AOSL Configuration RIP Configuration RIP Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURITY User Password User Pasture Router AOSL VVAN TOP connections Learmed MAC Table PPP Status	N	IP Address IP Address 10.0.0.2 Total umber of etherne IP 1 10.	WAN Subnet Mask LAN Subnet Mask 255.255.255.0 Number of Lan Ir et devices connecte Address MA 0.0.3 72:01 Ethernet Link Statt	MAC Address MAC Address 00:09:F3:00:00:81 Iterfaces: 1 ed to the DHCP serv IC Address 8:49:E7:2B:23 Is: UP	▲	
hide advanced settings ADMINISTRATION WAIN UAN UAN DNS NAT Port Forwarding ADSL Configuration RIP Configuration Firewall Diagnosite Test Route Table MAC Filtering SecURITY Admin Password User Password User Password User Password User Password Stotus Router ADSL VXAN AIM TCP connections Learned MAC Table PPP Status Save Setting and Reboot		IP Address ID.0.0.2 Total umber of etherne IP I ID	WAN Subnet Mask LAN Subnet Mask 255.255.0 Number of Lan Ir et devices connecte Address MA 0.0.3 72:0 Ethermet Link State	MAC Address MAC Address 00:09:F3:00:00:8E tterfaces: 1 tterfaces: 1 ad to the DHCP serv AC Address 3:49:E7:2B:23 ts: UP	er: 1	

Firmware Version: This field displays the Firmware Version number.

WAN: These fields display the IP Address, Subnet Mask, MAC Address for WAN interface.

LAN: These fields display the IP Address, Subnet Mask, MAC Address for LAN interface.

Number of Ethernet devices connected to the DHCP server: This field displays the

number of DHCP clients connected to the ADSL Wireless Router. It also shows the IP address and MAC address of the attached DHCP clients.

ADSL

The ADSL Status page shows the ADSL physical layer status.

hide advanced settings ADMINISTRATION WAN LAN DNS		[ADSL STAT	US ute			
NAT Port Forwarding Port Forwarding ADSL Configuration Firewall Diagnostic Test Route Table MAC Filtering SECURIV Admin Password User Password Misc Configuration System Log Code Update	Showtir Line Sta Modula Annex Statup Max Tx CO Ver Elaspse	ne Firmware Versio ate: tion: Mode: Attempts: : Power: udor: d Time:	n: 3.46 ACTIVAT N/A ANNEX_/ 0 -38 dBm/I UNUSED_ 0 days 0 ho	ION A Iz VENDOR ours 30 min	_0 utes 22	seconds	•
Status			Downstream	Upstream			
Router		SNR Margin	NA	NA	dB		
ADSL		Line Attenuation	NA	NA	dB		
ATM		Errored Seconds	0	0			
TCP connections Learned MAC Table		Loss of Signal	0	0			
PPP Status		Loss of Frame	0	0			
Save Setting and Reboot		CRC Errors	0	0			Γ
· · · ·		Data Rate	0	0	kbps		

Showtime Firmware Version: This field displays the ADSL data pump firmware version number.

Line State: This field displays the ADSL connection process and status.
 Modulation: This field displays the ADSL modulation status for G.dmt or T1.413.
 Annex Mode: This field displays the ADSL Annex modes for Annex A or Annex B.
 Startup Attempts: This field displays the ADSL connection attempts after loss of showtime.

Max Tx Power: This field displays the transmit output power level of the CPE.Co Vendor: This field displays the Central Office DSLAM vendor name. If available.Elaspsed Time: This field displays the time of the modem has been in operation.

WAN Status

The WAN Status page shows the information and status of WAN PVCs.



WAN: These fields display the IP Address, Subnet Mask and MAC Address for the WAN (ADSL) interface. Use the Virtual Circuit selection to selection different PVC for status display.

ATM Status

The ATM Status page shows all the statistics information of ATM cells.

hide advanced settings ADMINISTRATION	ATM STATUS							
<u>WAN</u> <u>LAN</u>	Reset Countes							
DNS NAT	-							
Port Forwarding ADSL Configuration	Tx B	iytes 0						
RIP Configuration Firewall	Rx B	Sytes 0						
Diagnostic Test Route Table	Tx C	ells 0						
MAC Filtering SECURITY	Rx C	Cells 0						
Admin Password User Password Misc Configuration	Rx H	IEC Errors 0	-					
System Log Code Update	Tx M	fgmt Cells 0	-					
Status	Rx M	4gmt Cells 0						
ADSL WAN	Tx C	LPO Cells 0						
ATM TCP connections	Rx C	LPO Cells 0						
Learned MAC Table PPP Status	Tx C	LP1 Cells 0						
Save Setting and Reboot	Rx C	LP1 Cells 0						
· · · · · · ·	Rx E	mors 0						

Reset Counters: This button allows user to reset the ATM Status counter.

TCP connections

The TCP Status page shows the statistics for all TCP connections.

OnePage Setup hide advanced settings ADMINISTRATION WAN	TCP STATUS Reset Countes								
LAN DNS NAT Rot Economics	Ger	ieral			Discarded Packe	ts	Connectio	ons	
ADSL Configuration		Transmit	Receive		Bad Checksum	0	Initiated	0	
<u>RIP Configuration</u> <u>Firewall</u>	Total Packets	2007	1613		Bad Header Offset	0	Accepted	244	
Diagnostic Test Route Table	Data Packets	1233	244		Too Short	0	Established	244	
MAC Filtering SECURITY	Data Bytes	797700	107479				Closed	214	
Admin Password	Out of Order Packets	N/A	242						
Misc Configuration System Log Code Update	Out of Order Bytes	N/A	0						
Status									
<u>Router</u> <u>ADSL</u> <u>VAN</u> <u>ATM</u> <u>TCP connections</u> <u>Learned MAC Table</u> <u>PPP Status</u>									
Save Setting and Reboot									

Learned MAC Table

The Learned MAC Table page shows the current learned Bridge MAC table.



Aging Timeout: This field allows the user to enter the update period for the MAC table.

Note: Click the *Submit* button to save the settings in temporary memory. If you make changes the configurations.

PPP Status

The PPP Status page shows the status of PPP for each PPP interface. See PPP.



These fields display the following information on each PPP interface:

- Connection Name (user defined)
- Interface (PVC)
- Mode (PPPoE or PPPoA)
- Status (Connected or Not Connected)
- Packets Sent
- Packets Received
- Bytes Sent
- Byte Received

Connect and Disconnect: Each PPP session can be individually controlled, simply enter the desired connection number into the "Connection #" field and select either connect or disconnect from the drop down menu and click on the "Execute" button.

Save Settings/Reboot

The Save Settings/Reboot page allows users to save the new configuration to the flash and reboot the system.

ADMINISTRATION	
• <u>WAN</u>	Sate estimate and reheat Sate & Deboat
• <u>LAN</u>	Save settings and repool.
• <u>DNS</u>	Pahoot modem without saving settings Report Only
• <u>NAT</u>	Reboot modelin without saving settings.
 Port Forwarding 	
<u>Wireless</u>	
ADSL Configuration	
RIP Configuration	
Firewall	
Diagnostic Lest	
Route Table	
MAC Filtering	
- Admin Decement	
Hoar Booward	
Misc Configuration	
System Log	
Code Undate	
Status	
Router	
ADSL	
WAN	
• <u>ATM</u>	
<u>TCP connections</u>	
 Learned MAC Table 	
PPP Status	
Save Setting and Report	
<u> </u>	

When the configurations are changed via the Web pages, the settings need to be saved into the flash, so it is necessary to go to this Save Settings/Reboot page to save and reboot the system for the changes to be taken effect.

During the Save and Reboot, the following Web page will be displayed "Your setting are being saved and the modem is being rebooted. Please wait.... After the Save and Reboot, the following Web page will be displayed "Your setting have been saved and the modem has rebooted."

The Reboot without Saving page allows the user to reboot the system without save the new configuration to the flash.

During the Reboot, the following Web page will be displayed "The modem is being rebooted. Please wait...." After the Reboot, the following Web page will be displayed "The modem has rebooted".

Appendix

Country	ISP	PVC
Australia	All Internet providers	VPI:8
		VCI:35
Polaium		VPI:0
Deigiuiti		VCI:33
Canada	Tolus	VPI:0
Canaua	Telus	VCI:35
	Cybercity	VPI:8
Danmark	Cybercity	VCI:35
Danmark	Tiscali	VPI:8
	Tiscali	VCI:35
	1 & 1 Internet DSI	VPI:1
		VCI:32
		VPI:1
		VCI:32
	Arcor DSI	VPI:8
		VCI:35
	Freenet DSI	VPI:1
		VCI:32
	Fireline networks	VPI:1
Deutschland		VCI:32
Deutoniana	GMX Internet	VPI:1
		VCI:32
	Hansenet	VPI:8
		VCI:35
	Netcologne	VPI:8
	Neteologile	VCI:35
	Schlund	VPI:1
		VCI:35
	Snafu ADSI	VPI:1
		VCI:32

Country	ISP	PVC
	Tiscali	VPI:1
		VCI:32
	Taplina	VPI:1
	r-onime	VCI:32
	Andoror Anhiotor	VPI:1
	Anderer Andieler	VCI:32
	Manadaa	VPI:8
France	vvannadoo	VCI:35
France	Tiagali	VPI:8
	TISCAII	VCI:35
		VPI:8
ISRAEL		VCI:48
	Tologom Italia	VPI:8
Italian		VCI:35
Italian	Post oil prosonto	VPI:8
	Rest on presente	VCI:35
		VPI:8
		VCI:48
Nothorlands	BRoyand Bridge LLC	VPI:0
Inclicitatios		VCI:33
	BBeyond PPPoA VC-MuX	VPI:0
		VCI:35
New Zealand	New Zealand Telecom	VPI:0
		VCI:100
Portugal	Todos os apresentador	VPI:0
T Oltugai		VCI:35
	Albura	VPI:1
		VCI:32
Snanish	Colt Teeccom	VPI:0
		VCI:35
	Earth	VPI:8
		VCI:32

Country	ISP	PVC
	Fresmas	VPI:8
	Erosmas	VCI:35
		VPI:8
	Jazztei	VCI:35
		VPI:8
		VCI:35
	Detevision	VPI:0
	Retevision	VCI:35
	Torre	VPI:8
	Terra	VCI:32
Spanish	Tiacali	VPI:1
opanish	IISCAII	VCI:32
	Telefornice	VPI:8
	Telefornica	VCI:32
	Telence	VPI:8
	Telepac	VCI:35
		VPI:1
	Uniz	VCI:33
	Va com	VPI:8
	ra.com	VCI:32
	Wanadaa	VPI:8
	Wallauoo	VCI:32
	Island ssimi	VPI:0
	1514110 551111	VCI:35
Suomi	Londooimi	VPI:8
Suomi	Lanussiini	VCI:48
	Vortox	VPI:8
		VCI:48
Switsorland		VPI:1
Switsendilu		VCI:32
Svorigo	Skapova	VPI:8
Svenge	Skalluva	VCI:35

Country	ISP	PVC
	Hinet	VPI:0
Taiwan		VCI:33
	Saadaat	VPI:0
	Seeunet	VCI:33
	Etisalat Classical IP Single	VPI:8
Lipited Arab Emirates	User	VCI:35
United Alab Emilates	Etisalat Classical IP for	VPI:8
	Business	VCI:35
Linited Kingdom	British Tolocom	VPI:0
		VCI:38