

TeleWell TW-EAV510

XDSL ROUTER

RELEASE 1.3

USER MANUAL

CONTENTS

Device Installation	4
Power on Router	4
Factory Reset Button	4
Network Connections	5
Configuration	5
Web-based Configuration Utility	6
Device Info	7
Summary	8
WAN	8
Statistics	9
Route	12
ARP	12
DHCP	12
Quick Setup	12
Advanced Setup	13
Layer2 Interface	13
WAN Service	17
LAN	21
Ethernet Port	23
NAT	23
Security	26
Parental Control	29
3G	31
Quality of Service	33
Routing	35
DNS	37
DSL	40
UPNP	41
DNS Proxy	41
DLNA	42
Storage service	42
Interface Grouping	43
IP Tunnel	44
IPSec	45
Power Management	46

Multicast	47
Wireless	48
Basic	48
Security	49
MAC Filter	50
Wireless Bridge	51
Advanced	51
Station Info	52
Diagnostics	53
Diagnostics	53
Fault Management	53
Management	54
Settings	54
System Log	55
Security Log	56
TR069 client	57
Internet Time	57
Access Control	58
Reboot	60
Tools	60
Troubleshooting	61
Glossary	63

Device Installation

The TW-EAV510 connects two separate physical interfaces, an xDSL (WAN) and an Ethernet (LAN) interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Power on Router

The Router must be used with the power adapter included with the device.

1. Insert the DC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a suitable nearby power source.
2. Depress the Power button into the on position. You should see the Power LED indicator light up and remain lit. The Status LED should light solid green and begin to blink after a few seconds.
3. If the Ethernet port is connected to a working device, check the LAN LED indicators to make sure the connection is valid. The Router will attempt to establish the xDSL connection, if the xDSL line is connected and the Router is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Router can establish a connection.

Factory Reset Button

The Router may be reset to the original factory default settings by using a ballpoint or paperclip to gently push down the reset button in the following sequence:

1. Press and hold the reset button while the device is powered off.
2. Turn on the power.
3. Wait for **10** seconds and then release the reset button.

Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address **192.168.0.254** and the subnet mask is **255.255.255.0**, the default management Username is "admin" and the default Password is "admin."

Network Connections

Connect xDSL Line

Use the xDSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the xDSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The xDSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

Connect Router to Ethernet

The Router may be connected to a single computer or Ethernet device through the 10BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

Hub or Switch to Router Connection

Connect the Router to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable. If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

Computer to Router Connection

You can connect the Router directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided.

Configuration

This section will show you how to configure your new Router using the web-based configuration utility.

Web-based Configuration Utility

Connect to the Router

The default IP address for xDSL MODEM is: 192.168.0.254; The Subnet Mask is : 255.255.255.0. Users can configure xDSL MODEM through an Internet browser. xDSL MODEM can be used as gateway and DNS server; users need to set the computer's TCP/IP protocol as follow:

1. Set the computer IP address at same segment of xDSL MODEM, such as set the IP address of the network card to one of the "192.168.0.100"~ "192.168.0.200".
2. Set the computer's gateway the same IP address as the xDSL Modem's.
3. Set computer's DNS server the same as xDSL Modem's IP address or that of an effective DNS server.

To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.0.254).

Type "**admin**" for the User Name and "**admin**" in the Password field. If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



Device Info

To access the **Device Info** window, click either the **Device Info** or **Summary** button in the **Device Info** directory. The following page opens:

Device Info Summary WAN Statistics Route ARP DHCP Quick Setup Advanced Setup Wireless Diagnostics Management	Device Info																		
	<table border="1"><tr><td>Model Name:</td><td>TW-EAV510 ADSL2+/VDSL2 WLAN router</td></tr><tr><td>Symmetric CPU Threads:</td><td>2</td></tr><tr><td>Build Timestamp:</td><td>06/06/2012</td></tr><tr><td>Software Version:</td><td>TW-EAV510_1.02</td></tr><tr><td>Bootloader (CFE) Version:</td><td>1.0.38-112.37</td></tr><tr><td>DSL PHY and Driver Version:</td><td>A2pv6F037b.d24b</td></tr><tr><td>Wireless Driver Version:</td><td>5.100.138.11.cpe4.12L02.6</td></tr><tr><td>MAC Address:</td><td>02:10:18:01:00:01</td></tr><tr><td>Uptime:</td><td>0D 16H 32M 15S</td></tr></table>	Model Name:	TW-EAV510 ADSL2+/VDSL2 WLAN router	Symmetric CPU Threads:	2	Build Timestamp:	06/06/2012	Software Version:	TW-EAV510_1.02	Bootloader (CFE) Version:	1.0.38-112.37	DSL PHY and Driver Version:	A2pv6F037b.d24b	Wireless Driver Version:	5.100.138.11.cpe4.12L02.6	MAC Address:	02:10:18:01:00:01	Uptime:	0D 16H 32M 15S
	Model Name:	TW-EAV510 ADSL2+/VDSL2 WLAN router																	
	Symmetric CPU Threads:	2																	
	Build Timestamp:	06/06/2012																	
	Software Version:	TW-EAV510_1.02																	
	Bootloader (CFE) Version:	1.0.38-112.37																	
	DSL PHY and Driver Version:	A2pv6F037b.d24b																	
	Wireless Driver Version:	5.100.138.11.cpe4.12L02.6																	
	MAC Address:	02:10:18:01:00:01																	
	Uptime:	0D 16H 32M 15S																	
	<p>This information reflects the current status of your WAN connection.</p>																		
	<table border="1"><tr><td>Line Rate - Upstream (Kbps):</td><td>0</td></tr><tr><td>Line Rate - Downstream (Kbps):</td><td>0</td></tr><tr><td>LAN IPv4 Address:</td><td>192.168.0.254</td></tr><tr><td>Default Gateway:</td><td></td></tr><tr><td>Primary DNS Server:</td><td>0.0.0.0</td></tr><tr><td>Secondary DNS Server:</td><td>0.0.0.0</td></tr><tr><td>LAN IPv6 ULA Address:</td><td></td></tr><tr><td>Default IPv6 Gateway:</td><td>ptm0.1</td></tr></table>	Line Rate - Upstream (Kbps):	0	Line Rate - Downstream (Kbps):	0	LAN IPv4 Address:	192.168.0.254	Default Gateway:		Primary DNS Server:	0.0.0.0	Secondary DNS Server:	0.0.0.0	LAN IPv6 ULA Address:		Default IPv6 Gateway:	ptm0.1		
	Line Rate - Upstream (Kbps):	0																	
Line Rate - Downstream (Kbps):	0																		
LAN IPv4 Address:	192.168.0.254																		
Default Gateway:																			
Primary DNS Server:	0.0.0.0																		
Secondary DNS Server:	0.0.0.0																		
LAN IPv6 ULA Address:																			
Default IPv6 Gateway:	ptm0.1																		

Summary

To access the Router's first **Summary** window, click the **Summary** button in the **Device Info** directory.

This window displays the current status of your DSL connection, including the software version, LAN IP address, and DNS server address.

Device Info

Model Name:	TW-EAV510 ADSL2+/VDSL2 WLAN router
Symmetric CPU Threads:	2
Build Timestamp:	06/06/2012
Software Version:	TW-EAV510_1.02
Bootloader (CFE) Version:	1.0.38-112.37
DSL PHY and Driver Version:	A2pv6F037b.d24b
Wireless Driver Version:	5.100.138.11.cpe4.12L02.6
MAC Address:	02:10:18:01:00:01
Uptime:	0D 16H 32M 15S

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.0.254
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	ptm0.1

WAN

To access the **WAN Info** window, click the **WAN** button in the **Device Info** directory.

This window displays the current status of your WAN connection.

WAN Info											
Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
atm0.1	ipoe_0_0_33	IPoE	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Unconnect		
atm1.1	ipoe_0_0_100	IPoE	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Unconnect		
ptm0.1	ipoe_4_1_1	IPoE	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Unconnect		
ppp7	3G dongle	PPPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	Unconnect		

Statistics

The **Statistics** menu contains statistical information about the LAN, WAN service, and Optical. Select **Statistics** in the **Device Info** menu to open the Statistics submenu.

LAN

The LAN window displays the statistics for the information received and transmitted over the LAN interface.

Click **LAN** in the **Statistics** submenu to open the LAN window;

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN1	0	0	0	0	0	0	0	0
LAN2	0	0	0	0	0	0	0	0
LAN3	7271527	49587	0	0	35022993	73756	0	0
LAN4	0	0	0	0	0	0	0	0
wlan0	0	0	3	0	0	0	420	0

Reset Statistics

WAN Service

The WAN window displays the statistics for the information received and transmitted over the WAN interface.

Click **WAN Service** in the **Statistics** submenu to open the WAN window;

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm0.1	ipoe_0_0_33	0	0	0	0	0	0	0	0
atm1.1	ipoe_0_0_100	0	0	0	0	0	0	0	0
ptm0.1	ipoe_4_1_1	0	0	0	0	0	0	0	0
ppp7	3G dongle	0	0	0	0	0	0	0	0

Reset Statistics

xTM

To access the **Device Info – xTM** window, click the **xTM** button in the **Device Info** directory. This read-only window displays xTM info.

Interface Statistics										
Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
<input type="button" value="Reset"/>										

xDSL

To access the **Device Info – xDSL** window, click the **xDSL** button in the **Device Info** directory.

This read-only window displays xDSL info.

Statistics -- xDSL

Mode:		
Traffic Type:		
Status:	NoSignal	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test

Reset Statistics

Route

To access the **Device Info – Route** window, click the **Route** button in the **Device Info** directory.

This read-only window displays routing info.

Device Info -- Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

ARP

To access the **Device Info – ARP** window, click the **ARP** button in the **Device Info** directory.

This read-only window displays Address Resolution Protocol info.

Device Info -- ARP			
IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:27:19:8f:7c:d6	br0

DHCP

To access the **Device Info – DHCP Leases** window, click the **DHCP** button in the **Device Info** directory.

This read-only window displays DHCP lease info.

Device Info -- DHCP Leases			
Hostname	MAC Address	IP Address	Expires In
FREESKYC-AAA4C0	00:27:19:8f:7c:d6	192.168.1.2	23 hours, 53 minutes, 58 seconds

Quick Setup

The Quick Setup will help you to configure the device eazily. If you want Automatic Configuration, click the checkbox of **Automatic Configuration**. When you are finished, click the **Apply/Save** button to save.

Quick Setup

Automatic Configuration

ATM PVC Configuration

VPI: [0-255]

VCI: [32-65535]

Encapsulation Mode: LLC/SNAP-BRIDGING

WAN Service Configuration

Protocol: PPPoE

PPP Configuration

PPP Username:

PPP Password:

Use Static IP Address

Wireless SSID

SSID:

Advanced Setup

This chapter includes the more advanced features used for network management and security as well as administrative tools to manage the Router, view status and other information used to examine performance and for troubleshooting.

Layer2 Interface

To access the **DSL ATM Interface Configuration** window, click the **ATM Interface** button in the **Layer2 Interface** directory.

This window is used to configure the ATM interface. You can add and delete ATM interface on this window.

If you are setting up the ATM interface for the first time, click the **Add** button.

DSL ATM Interface Configuration												
Choose Add, or Remove to configure DSL ATM interfaces.												
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate (cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	8/WRR/1	<input type="checkbox"/>

ATM Interface

The **ATM PVC** Configuration window allows you to set up ATM PVC configuration. Enter Virtual Path Identifier, and Virtual Channel Identifier. The VPI and VCI values should be provided by your ISP. This window also allows you to select DSL Link Type, PPPoA·IPoA and EoA (EoA is for PPPoE, IPoE, and Bridge) Use the drop-down menu to select the desired Encapsulation Mode. Click the **Apply / Save** button to save.

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: [0-255]

VCI: [32-65535]

Select DSL Latency

Path0 (Fast)

Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA

PPPoA

IPoA

Encapsulation Mode: ▾

Service Category: ▾

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin

Weighted Fair Queuing

Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)

VC WRR Weight: [1-63]

VC Precedence: [1-8] (lower value, higher priority)

Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's. For single queue VC, the default queue precedence and weight will be used for arbitration. For multi-queue VC, its VC precedence and weight will be used for arbitration.

VDSL2 (ptm) interface

The **VDSL2 (ptm) interface** Configuration window enables you to add, delete, or modify up to one VDSL WAN Layer 2 interface connections.

Click **VDSL2 (ptm) Interface** in the Layer2 Interface menu to open the VDSL(ptm) WAN Interface Configuration window

VDSL2(ptm) Interface Configuration

Choose Add, or Remove to configure VDSL2(ptm) interfaces.

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0&1	Normal&High	VlanMuxMode	Support	<input type="checkbox"/>

VDSL WAN Configuration

If you have selected to add or modify a VDSL interface connection, the VDSL WAN Configuration window opens. Click the **Apply/Save** button to save.

VDSL2(ptm) Configuration

This screen allows you to configure a VDSL2(ptm) flow.

Select DSL Latency

- Path0 (Fast)
- Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue

- Weighted Round Robin
- Weighted Fair Queuing

Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)

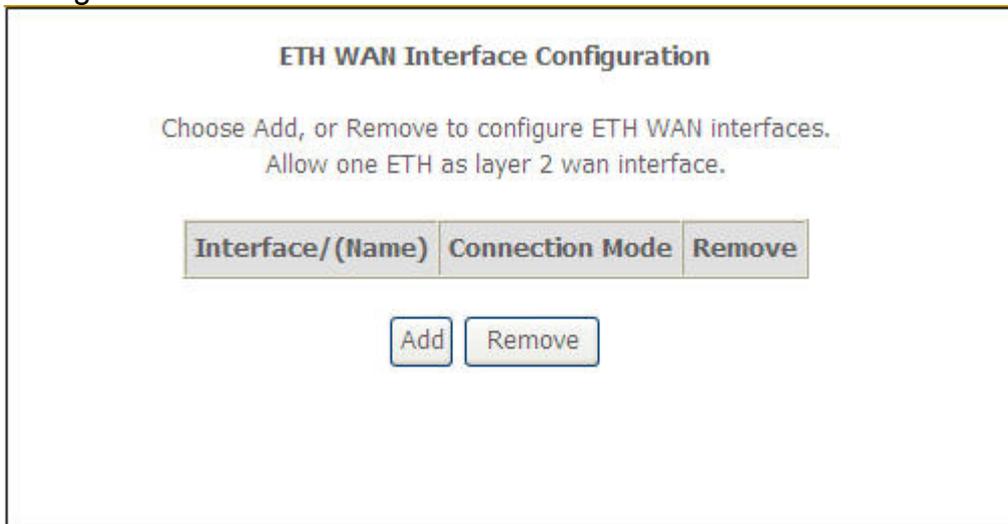
Default Queue Shaping Rate: [Kbits/s] (blank indicates no shaping)

Default Queue Shaping Burst Size: [bytes] (shall be >=1600)

ETH interface

The ETH WAN Interface Configuration window enables you to add, delete, or modify up to one ETH WAN Layer 2 interface connections.

Click **ETH Interface** in the Layer2 Interface menu to open the ETH WAN Interface Configuration window



The screenshot shows the 'ETH WAN Interface Configuration' window. At the top, it says 'ETH WAN Interface Configuration'. Below that, it instructs the user to 'Choose Add, or Remove to configure ETH WAN interfaces. Allow one ETH as layer 2 wan interface.' There is a table with three columns: 'Interface/(Name)', 'Connection Mode', and 'Remove'. Below the table are two buttons: 'Add' and 'Remove'.

Interface/(Name)	Connection Mode	Remove
------------------	-----------------	--------

ETH WAN Configuration

If you have selected to add or modify an ETH interface connection, the ETH WAN Configuration window opens



The screenshot shows the 'ETH WAN Configuration' window. It says 'ETH WAN Configuration' and 'This screen allows you to configure a ETH port .'. Below that, it says 'Select a ETH port:'. There is a dropdown menu with 'eth0/eth0' selected. Below the dropdown are two buttons: 'Back' and 'Apply/Save'.

Select a ETH port:

eth0/eth0 ▼

WAN Service

To access the **Wide Area Network (WAN) Service Setup** window, click the **WAN Service** button in the **Advanced Setup** directory.

This window is used to configure the WAN interface. You can add and delete WAN interface on this window.

If you are setting up the WAN interface for the first time, click the **Add** button.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

The **WAN Service Interface Configuration** Configuration window allows select a layer 2 interface for this service. Click the **Next** button to continue

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0

low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

This window allows you to select the appropriate connection type. The choices include PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), IP over Ethernet (IPoE), IP over ATM (IPoA), and Bridging.

WAN Service Configuration – PPPoE

Click the PPP over Ethernet (PPPoE) radio button on this window. This window also allows you to use the drop-down menu to enable IPv6 service. Click the **Next** button to continue.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection: (IPv6 Only not support)

Back

Next

WAN Service Configuration – PPPoE

This window allows you to set the username and the password for your PPP connection. This information is obtained from your ISP. Additional settings on this window will also depend on your ISP. And you can input 2nd IP on this page. Click the **Next** button to continue.

PPP Username:
 PPP Password:
 PPPoE Service Name:
 Authentication Method: **AUTO**

Enable Fullcone NAT

MAC Clone: (00:00:00:00:00:00 means use dynamic mac address)

PPP Dial Up Delay Seconds [0-30]: (0 means random delay between 1-30 seconds)

Dial on demand (with idle timeout timer)

Manual connect

enable manual MTU set

PPP IP extension

Enable NAT

NAT Public Ip Address: **Automatic**

Enable Firewall

Use Static IPv4 Address

Enable PPP Debug Mode

Enable KeepAlive

KeepAliveTime [10-30]: seconds

KeepAliveMaxFail [0-100]: times

PPP Max Fail [0-100]: times

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

WAN Service Configuration – IPoE

This window allows you to configure the WAN IP settings. This information is obtained from your ISP. Click the **Next** button to continue

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:

(8 hexadecimal digits)

Option 61 DUID:

(hexadecimal digit)

Option 66:

Disable

Enable

Option 121:

Disable

Enable

Option 125:

Disable

Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

MAC Clone:

(00:00:00:00:00:00 means use dynamic mac address)

WAN Service Configuration – Bridging

Click the Bridge radio button on this window. Click the **Next** button to continue.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

LAN

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router.

LAN setting

To access the **Local Area Network (LAN) Setup** window, click the **LAN** button in the **Advanced Setup** directory.

This window allows you to set up a LAN interface. When you are finished, click the **Apply / Save** button.

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName Default ▾

IP Address:

Subnet Mask:

Enable IGMP Snooping

Standard Mode

Blocking Mode

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour): [1-596000] (only support integer!)

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
-------------	------------	--------

IPv6 Autoconfig

The IPv6 Autoconfig window enables you to configure the settings for the LAN interface with IPv6.

Click IPv6 Autoconfig in the LAN submenu to open the IPv6 Autoconfig window;

This window allows you to configure IPv6. When you are finished, click the **Apply / Save** button.

IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

Enable DHCPv6 Server

Stateless
 Stateful

Start interface ID:

End interface ID:

Leased Time (hour):

Enable RADVD

Enable ULA Prefix Advertisement

Randomly Generate
 Statically Configure

Prefix:

Preferred Life Time (hour):

Valid Life Time (hour):

Enable MLD Snooping

Standard Mode
 Blocking Mode

Ethernet Port

To access the **Ethernet Port** window, click the **Ethernet Port** button in the **Advanced Setup** submenu. You can configure the Media Type of Ethernet port in the new page and it will show you the Link Status of each Ethernet port. When you are finished, click the **Save/Apply** button

Ethernet Configuration

Select a preferred media type of ethernet port.

Interface Name	Media Type	Link Status
LAN1	Auto Negotiate	Disconnect
LAN2	Auto Negotiate	Disconnect
LAN3	Auto Negotiate	Connected
LAN4	Auto Negotiate	Disconnect

NAT

Virtual Servers

Select **Virtual Servers** from the **Advanced Setup** menu to open the NAT submenu.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

If you have selected to **Add** a virtual server, the Add NAT – Virtual Servers window opens

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**
 Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application).

Click the **Add** button to configure port triggering.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open			WAN Interface	Remove
	Protocol	Port Range	Protocol	Port Range			
				Start	End		
<input type="text"/>							

You can configure the port settings on this window by clicking the **Select an application** radio button and then using the drop-down list to choose an existing application, or by clicking the **Custom application** radio button and entering your own Application Rule in the field provided. Click **Save/Apply** when you are finished with the port setting configuration. The new Application Rule will appear in the Port Triggering table.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it. Remaining number of entries that can be configured:32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

DMZ Host

Since some applications are not compatible with NAT, the Router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.

To designate a DMZ IP address, type in the IP Address of the server or device on your LAN, and click the **Save/Apply** button

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

ALG

To access the **ALG** window, click the **ALG** button in the **NAT** submenu. You can enable and disable the **ALG** functions in the new page. When you are finished, click the **Save/Apply** button.

ALG

Select the ALG below.

SIP ALG Enabled

FTP ALG Enabled

H323 ALG Enabled

PPTP ALG Enabled

RTSP ALG Enabled

TFTP ALG Enabled

Security

To access the **Security** window, click the **Security** button in the **Advanced Setup** directory. The **Security** button appears after configuring WAN interface in PPPoA, PPPoE, IPoE or IPoA.

IP Filtering

The **IP Filtering** button appears when configuring WAN interface in PPPoA, PPPoE, IPoE or IPoA.

IP Filtering - Outgoing

This window allows you to create a filter rule of **Outgoing**.

Click **change default policy** to change the mode of policy.

Now default policy is **BLOCK**, it means all outgoing IP traffic from LAN is blocked, but some IP traffic can be accepted by setting up filters.

If you are setting up the outgoing IP filtering, click the **Add** button.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

Now default policy is **ACCEPT**, it means all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting up filters.

If you are setting up the outgoing IP filtering, click the **Add** button.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is blocked, but some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

Enter the information in the section. Explanations of parameters are described below. Click the **Apply / Save** button to add the entry in the Active Outbound IP Filtering table.

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

IP Filtering – Incoming

This window allows you to create a filter rule of **Incoming**.
Click **change default policy** to change the mode of policy.

Now default policy is **ACCEPT**, it means all incoming IP traffic from WAN is accepted, but some IP traffic can be blocked by setting up filters.

If you are setting up the incoming IP filtering, click the **Add** button.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is blocked. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	------------	----------	---------------------	---------	---------------------	---------	--------

Now default policy is **BLOCK**, it means all incoming IP traffic from WAN is blocked, but some IP traffic can be accepted by setting up filters.

If you are setting up the incoming IP filtering, click the **Add** button.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is allowed. However, some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>								

Enter the information in the section. Explanations of parameters are described below. Click the **Apply / Save** button to add the entry in the Active Inbound IP Filtering table.

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All
 br0/br0

MAC filter

The MAC Filtering window enables you to control access to and from specific MAC addresses. Select **MAC Filtering** from the **Security** submenu to open the MAC Filtering Setup window;

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
veip0.1	FORWARD	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

If you have selected to **Add** a MAC filter, the Add MAC Filter window opens

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Parental Control

Use this window to deny access to specified MAC address.

Time Restriction

If you are setting up the MAC address blocking, click the **Add** button.

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>											

MAC address is a specially formatted text string (xx:xx:xx:xx:xx:xx) that uniquely identification of a device. This section will allow users to block devices with certain MAC addresses on the LAN.

To configure for MAC address blocking, enter the username into the **Username** field, click **Browser's MAC Address** to have MAC address of the LAN device, or click **Other MAC Address** and enter a MAC address manually. Tick the checkboxes for the desired individual days of the week and enter desired **Start Blocking Time** and **End Blocking Time**. Click the **Save/Apply** button to save the configuration

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name:

Browser's MAC Address:

Other MAC Address:

(xx:xx:xx:xx:xx:xx)

Days of the week: Mon Tue Wed Thu Fri Sat Sun

Click to select:

Start Blocking Time (hh:mm):

End Blocking Time (hh:mm):

URL Filter

This window allows you to set up **URL Filter** on the Router.
Choose URL List Type **Exclude** or **Include** first and click **Add** button.

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

Exclude -- Deny computers to access the following web sites in the list.
Include -- Allow computers to access only the following sites in the list.

URL List Type: Exclude Include

Address	Port	Remove
---------	------	--------

Enter the URL address and port number then click **Apply / Save** to add the entry to the URL filter.

Parental Control -- URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

3G

To access the **3G** window, click the **3G** button in the **Advanced Setup** directory. This window allows you to set up 3G on the Router. When you are finished, click on the **Save/Apply** button.

3G Setting

Set USB for 3G

Enable

Modem Type: TW-3G HSPA+

Username:

Password:

APN code:

Pin code:

Dialup Number: *99#

Baud Rate: 230400

MTU: 1600

MRU: 1600

LCPEchoInterval: 30

LCPEchoFailure: 10

Network Preference:

- Automatic (3G preferred)
- 3G Only
- 2G Only

If you want to add new 3G dongle, click **driver add** button, and the new page will show you how to configure a new 3G dongle. After you are finished, click on the **add** button.

add a new 3G dongle's drive

DriverList:

DeviceName:

DefaultVendor: (Hexadecimal number,Example: 12d1)

DefaultProduct:

TargetVendor:

TargetProduct:

MessageEndpoint:

DevName: (Example: /dev/ttyUSB0)

HuaweiMode:

MessageContent0:

MessageContent1:

(62 bits Hexadecimal number,Example:
555342439845f8850000000000000061b000000020000000000000000000000)

Quality of Service

QoS or Quality of Service allows your Router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs.

To access the **QoS – Queue Management Configuration** window, click the **Quality of Service** button in the **Advanced Setup** directory.

This window allows you to set up QoS on the Router. When you are finished, click on the **Save/Apply** button.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Select Default DSCP Mark: No Change (-1) ▼

QoS Queue

Click the **Add** button to add a QoS Queue Configuration table entry.

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
 In PTM mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 3 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.
 Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate(bits/s)	Burst Size(bytes)	Enable	Remove
WMM Voice Priority	1	wlan0	1	1/SP					Enabled	
WMM Voice Priority	2	wlan0	2	2/SP					Enabled	
WMM Video Priority	3	wlan0	3	3/SP					Enabled	
WMM Video Priority	4	wlan0	4	4/SP					Enabled	
WMM Best Effort	5	wlan0	5	5/SP					Enabled	
WMM Background	6	wlan0	6	6/SP					Enabled	
WMM Background	7	wlan0	7	7/SP					Enabled	
WMM Best Effort	8	wlan0	8	8/SP					Enabled	
Default Queue	35	ipoa0	1	8/WRR/1	Path0				<input type="checkbox"/>	

This window allows you to configure a QoS queue entry and assign it a specific network interface.

Click the **Apply / Save** button to save and activate the filter.

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable:

Interface:

QoS Classification

Choose **Add** or **Remove** to configure network traffic classes.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																			

Use this window to create a traffic class rule to classify the upstream traffic, assign a queue that defines the precedence and the interface, and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. Please remember that all of the specified conditions on this window must be met for the rule to take effect. Click the **Apply / Save** button to save and activate this rule.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Routing

To access the **Routing** windows, click the **Routing** button in the **Advanced Setup** directory.

Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again. Click the **Apply / Save** button when you are finished.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces **Available Routed WAN Interfaces**

ppp7

TODO: IPV6 ***** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface:

Mark 802.1p priority:

Static Route

Click the **Add** button on the **Routing – Static Route** window to access the following window displayed on the next page.

Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
------------	---------------------	---------	-----------	--------	--------

Enter the static routing information for an entry to the routing table. Click the **Apply / Save** button when you are finished.

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

Policy Routing

Click the **Add** button on the **Policy Routing Setting** window to access the following window displayed on the next page.

Policy Routing Setting -- A maximum 8 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
-------------	-----------	----------	-----	------------	--------

Enter the Policy Routing information. Click the **Apply / Save** button when you are finished.

Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.
Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface:

Default Gateway IP:

RIP

To activate RIP for the device, select the **Enabled** radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the **Save/Apply** button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP or has NAT enabled.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
WAN Interface not exist for RIP.			

DNS

To access the **DNS** windows, click the **DNS** button in the **Advanced Setup** directory. The **DNS** button appears when configuring WAN interface in PPPoA, PPPoE, MER or IPoA.

DNS Server

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again. Click the **Apply / Save** button when you are finished.

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: Available WAN Interfaces:

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

TODO: IPv6 ***** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Dynamic DNS

The Router supports Dynamic DNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form **hostname.dyndns.org**, Many ISPs assign public IP addresses using DHCP, and this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS providers. Click **Add** to see the Add DDNS Settings section.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Enter the required DDNS information, click the **Apply / Save** button to save the information.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text" value="Hostname"/>
Interface	<input type="text" value="3G dongle/ppp7"/>

DynDNS Settings

Username	<input type="text"/>
Password	<input type="text"/>



Note

DDNS requires that an account be setup with one of the supported DDNS servers prior to engaging it on the Router. This function will not work without an accepted account with a DDNS server.

DSL

The DSL window enables you to configure the DSL settings of the gateway. Select **DSL** from the **Advanced Setup** menu to open the DSL Settings window

DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled
- VDSL2 Enabled

Select the profile below.

- 8a Enabled
- 8b Enabled
- 8c Enabled
- 8d Enabled
- 12a Enabled
- 12b Enabled
- 17a Enabled
- 30a Enabled

US0

- Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

If you clicked **Advanced Settings** in the **DSL Settings** window, the DSL Advanced Settings window opens

DSL Advanced Settings

Select the test mode below.

- Normal
- Reverb
- Medley
- No retrain
- L3

If you clicked the **Tone Selection** button, the ADSL Tone Settings window opens

Note: The ADSL tone settings should only be configured with the assistance of your ISP.

ADSL Tone Settings

Upstream Tones

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Downstream Tones

32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79
 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95
 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111
 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127
 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143
 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159
 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175
 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191
 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207
 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223
 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239
 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255

UPnP

To access the **UPnP Configuration** window, click the **UPnP** button in the **Advanced Setup** directory.

This window allows you to Config UPnP Proxy. Click the **Apply / Save** button when you are finished.

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

Enable UPnP

DNS Proxy

To access the **DNS Proxy Configuration** window, click the **DNS Proxy** button in the **Advanced Setup** directory.

This window allows you to Config DNS Proxy. Click the **Apply / Save** button when you are finished.

DNS Proxy Configuration

Enable DNS Proxy

Host name of the Broadband Router:

Domain name of the LAN network:

DLNA

Select **DLNA** from the **Advanced Setup** menu to open the DLNA window. This window allows you to config DLNA function. Click the **Apply / Save** button when you are finished.

Digital Media Server settings

This page allows you to enable / disable digital media server support.

Enable on-board digital media server.

Interface

Media Library Path

Storage service

The Storage Service window displays Storage Device information from USB interface. Select **Storage Service** from the **Advanced Setup** menu to open the Storage Service window

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	FileSystem	Total Space	Used Space

Interface Grouping

Interface Group supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.

To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Click **Add** to do advanced settings.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			eth0	
			eth1	
			eth2	
			eth3	
			wlan0	

To create a new mapping group, enter **Group Name**, add interfaces to **Grouped Interfaces**. Click **Apply / Save** to save the changes.

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Apply/Save button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped WAN Interfaces:

Available WAN Interfaces: PPP7

Grouped LAN Interfaces:

Available LAN Interfaces: eth0, eth1, eth2, eth3, wlan0

Automatically Add Clients With the following DHCP Vendor IDs:

IP Tunnel

Select **IP Tunnel** from the **Advanced Setup** menu to open the IP Tunnel submenu.

IPv6inIPv4

Select **IPv6inIPv4** from the **IP Tunnel** submenu to open the IP Tunneling-6in4 Tunnel Configuration window

IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
------	-----	-----	---------	------------------	------------	----------------------	--------

If you click **Add**, the detail of the IP Tunneling-6in4 Tunnel Configuration window will open

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism: 6RD

Associated WAN Interface:

Associated LAN Interface: LAN/br0

Manual Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

IPv4inIPv6

Select **IPv4inIPv6** from the **IP Tunnel** submenu to open the IP Tunneling-4in6 Tunnel Configuration window;

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	Remote IPv6 Address	Remove
------	-----	-----	---------	---------------------	--------

If you click **Add**, the detail of the IP Tunneling-4in6 Tunnel Configuration window will open

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:

Mechanism: DS-Lite

Associated WAN Interface:

Associated LAN Interface: LAN/br0

Manual Automatic

Remote IPv6 Address:

IPSec

To access the **IPSec Tunnel Mode Connections** window, click the **IPSec** button in the **Advanced Setup** directory.

This window allows you to configure **IPSec**.

Click **Add New Connection** to edit IPSec tunnel mode connections from this page

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
<input type="button" value="Add New Connection"/> <input type="button" value="Remove"/>				

This window allows you to advanced settings.

IPSec Settings

IPSec Connection Name

Tunnel Mode

Remote IPSec Gateway Address (IPv4 address in dotted decimal)

Tunnel access from local IP addresses

IP Address for VPN

IP Subnetmask

Tunnel access from remote IP addresses

IP Address for VPN

IP Subnetmask

Key Exchange Method

Authentication Method

Pre-Shared Key

Perfect Forward Secrecy

Advanced IKE Settings

Power Management

The Power Management window enables you to control of Hardware to evaluate power consumption.

Select **Power Management** from the **Advanced Setup** menu to open the Power Management window

Power Management

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

MIPS CPU Clock divider when Idle
 Enable **Status: Enabled**

Wait instruction when Idle
 Enable **Status: Enabled**

DRAM Self Refresh
 Enable **Status: Enabled**

Ethernet Auto Power Down Number of ethernet interfaces in:
 Enable **Status: Enabled** Full power mode: 6
Low power mode: 3

Multicast

To access the **IGMP Configuration** window, click the **Multicast** button in the **Advanced Setup** directory.

Enter IGMP protocol configuration fields if you want modify default values shown below.

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="3"/>
Query Interval:	<input type="text" value="125"/>
Query Response Interval:	<input type="text" value="10"/>
Last Member Query Interval:	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="25"/>
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="25"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:	<input type="checkbox"/>
Membership Join Immediate (IPTV):	<input type="checkbox"/>

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="2"/>
Query Interval:	<input type="text" value="125"/>
Query Response Interval:	<input type="text" value="10"/>
Last Member Query Interval:	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="10"/>
Maximum Multicast Data Sources (for mldv3):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="10"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>
LAN to LAN (Intra LAN) Multicast Enable:	<input checked="" type="checkbox"/>

Wireless

Basic

The Basic menu enables you to configure basic features of the wireless LAN interface. Select **Basic** from the **Wireless** menu to open the basic submenu;

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless
 Hide Access Point
 Clients Isolation
 Disable WMM Advertise
 Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 02:10:18:01:00:03

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually or through WiFi Protected Setup(WPS)
You can select to configure WEP encryption, Shared, 802.1x, WPA, and WPA2 authentication.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable **WPS**

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

MAC Filter

This page can help you to allow or deny certain MAC addresses to pass through or block out. Click **Add** to see the following page.

Wireless -- MAC Filter

Select SSID:

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

Enter MAC Address and click **Apply / Save** to add the MAC address to MAC filter.

Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

Wireless Bridge

The Wireless Bridge menu enables you to configure wireless bridge features of the wireless LAN interface.

Select **Wireless Bridge** from the **Wireless** menu to open the wireless bridge submenu

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Advanced

This page allows you to configure advanced wireless LAN interface. Configuring these settings may increase the performance of your router but if you are not familiar with networking devices and protocols, this section should be left at its default settings.

Click **Apply / Save** to save the settings.

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band:

Channel: Current: 1 (interference: acceptable)

Auto Channel Timer(min):

Standard Mode:

Bandwidth: Current: 20MHz

Control Sideband: Current: None

802.11n Rate:

802.11n Protection:

Support 802.11n Client Only:

RIFS Advertisement:

OBSS Co-Existence:

RX Chain Power Save: Power Save status: **Full Power**

RX Chain Power Save Quiet Time:

RX Chain Power Save PPS:

Standard Rate:

Multicast Rate:

Basic Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Global Max Clients:

XPress™ Technology:

Transmit Power:

WMM(Wi-Fi Multimedia):

WMM No Acknowledgement:

WMM APSD:

Station Info

This page shows the authenticated wireless stations and their status. Click **Refresh** to update the information.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Diagnostics

Diagnostics

Your modem is capable of testing your DSL connection with access to **Diagnostics**. This window is used to test connectivity of the Router.

ipoe_0_0_33 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	FAIL	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	PASS	Help
Test your LAN4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

Fault Management

Fault Management enables you to test the connectivity of the xDSL PTM mode.

Note: Fault management should only be run with assistance from your ISP.

Select **Fault Management** from the **Diagnostics** menu to open the 802.1ag Connectivity Fault Management window

802.1ag Connectivity Fault Management

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level:

Destination MAC Address:

802.1Q VLAN ID: [0-4095]

VDSL Traffic Type:

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Find Maintenance End Points (MEPs)

Linktrace Message (LTM):				

Management

The Management directory features an array of options designed to help you get the most out of your Router.

Settings

To access the **Settings - Backup** window, click the **Settings** button in the **Management** directory.

This window allows you to backup your DSL Router configurations.

Click the **Backup Settings** button to save your Router configurations to a file on your computer.

Settings - Backup

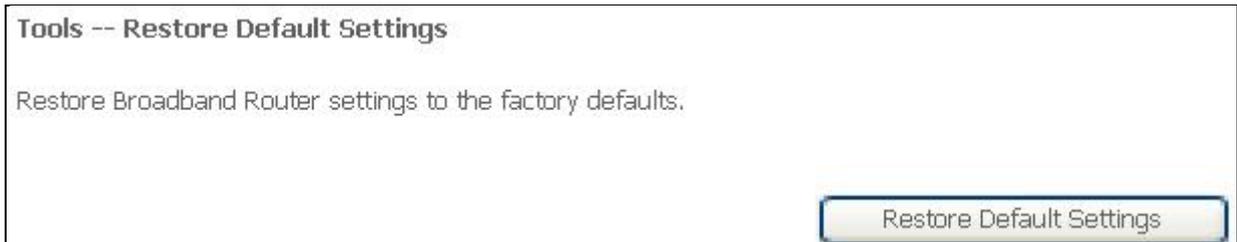
Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

This window allows Update DSL router settings. You may update your router settings using your saved files.

Click the **Update** button to update your Router configurations with a file on your computer.

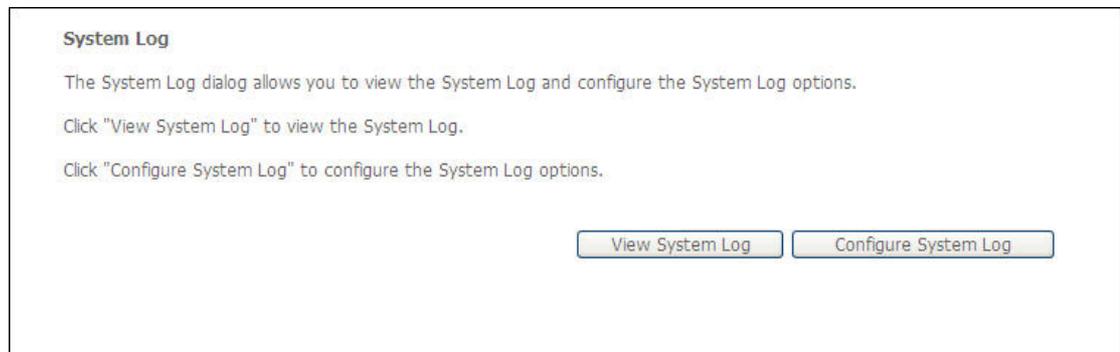


This window allows Restore DSL router settings to the factory defaults. Click the **Restore DSL Settings** button to restore DSL router settings to the factory defaults.

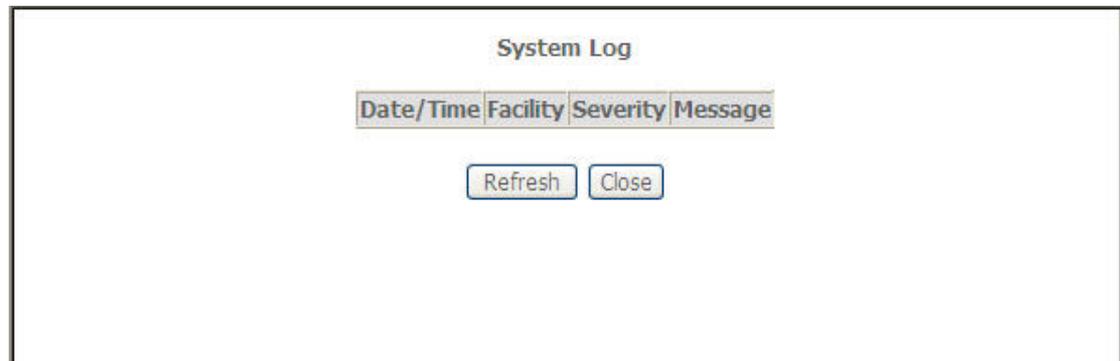


System Log

The System Log windows enable you view and configure the system log of this device. Select **System Log** in the **Management** menu to open the System Log window



If you clicked **View System Log** in the **System Log** window, the System Log information window opens;



If you clicked **Configure System Log** in the **System Log** window, the Configuration window

opens;

Note: Configuring the system log should be done with assistance from your ISP.

The screenshot shows the 'System Log -- Configuration' window. It contains a paragraph of text explaining log settings, followed by instructions to select values and click 'Apply/Save'. Below this, there are three controls: a radio button for 'Log' (with 'Disable' selected), a dropdown for 'Log Level' (set to 'Debugging'), a dropdown for 'Display Level' (set to 'Error'), and a dropdown for 'Mode' (set to 'Local'). An 'Apply/Save' button is located at the bottom center.

Security Log

The System Log windows enable you view the security log of this device.

Select **Security Log** in the **Management** menu to open the Security Log window;

The screenshot shows the 'Security Log' window. It contains a title 'Security Log', a paragraph of text explaining the dialog's purpose, and three instructions: 'Click "View" to view the Security Log.', 'Click "Reset" to clear and reset the Security Log.', and 'Right-click [here](#) to save Security Log to a file.' At the bottom right, there are two buttons: 'View' and 'Reset'.

If you clicked **View** in the **Security Log** window, the Security Log information window opens;

The screenshot shows the 'Security Log' information window. It has a title 'Security Log' and a 'Message' label. Below the message area, there are two buttons: 'Refresh' and 'Close'.

TR069 client

The TR-069 Client window enables you to configure the ACS for this device. Select **TR-069 Client** in the **Management** menu to open the TR-069 Client-Configuration window;

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Internet Time

To access the **Time settings** window, click the **Internet Time** button in the **Management** directory.

This window allows you to set the Router's time configuration. When you are finished, click the **Save/Apply** button.

Time settings

This page allows you to set the DSL Router's time configuration.

Automatically synchronize with Internet time servers

Access Control

To access the **Access Control** windows, click the **Access Control** button in the **Management** directory.

Passwords

This window allows you to change the password on the Router. When you are finished, click the **Save/Apply** button.

Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name:

Old Password:

New Password:

Confirm Password:

Services

The Services window enables you to enable or disable services
Select **Services** from the **Access Control** menu to open the Services window

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
ICMP	Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Save/Apply

IP Addresses

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

To access this window, click the **IP addresses** button in the **Access Control** directory.

Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: Disable Enable

IP Address	Subnet Mask	Remove
------------	-------------	--------

Add

Remove

Click the **Add** button, access the following window displayed on the next page.

Add IP Addresses

Enter the IP address of the management station permitted to access the local management services, and click "Apply/Save".

IP Address:

Subnet Mask:

Input the IP Address and Subnet Mask which you want to configure, and then click **Apply** to enable this IP Address.

Reboot

To access this window, click the **Reboot** button in the **Management** directory. To save your settings and reboot the system, click the **Reboot** button.

Click the button below to reboot the router.

Tools

This page will help you to diagnostic the status of your Network. You can use "Ping", "Trace Route" and "Nslookup" methods in this page. After you input the IP address or Domain name, click "**Ping**", "**Trace Route**" or "**Nslookup**" button.

Ping and Trace Route

You can use ping and trace route in this page.

Please input the IP address or Domain name and click "Ping" , "Trace Route" or "Nslookup".

IP Address/Domain Name:

Troubleshooting

1. How do I configure my TW-EAV510 Router without the CD-ROM?

- Connect your PC to the Router using an Ethernet cable.
- Open a web browser and enter the address <http://192.168.0.254>
- The default username is 'admin' and the default password is 'admin'.
- If you have changed the password and cannot remember it, you will need to reset the Router to the factory default setting (see question 2), which will set the password back to 'admin'.

Note: Please refer to the next section "Networking Basics" to check your PC's IP configuration if you can't see the login windows.

2. How do I reset my Router to the factory default settings?

- Ensure the Router is powered on.
- Press and hold the reset button on the back of the device for approximately 10 seconds.
- This process should take around 30~60 seconds.

3. What can I do if my Router is not working correctly?

There are a few quick steps you can take to try and resolve any issues:

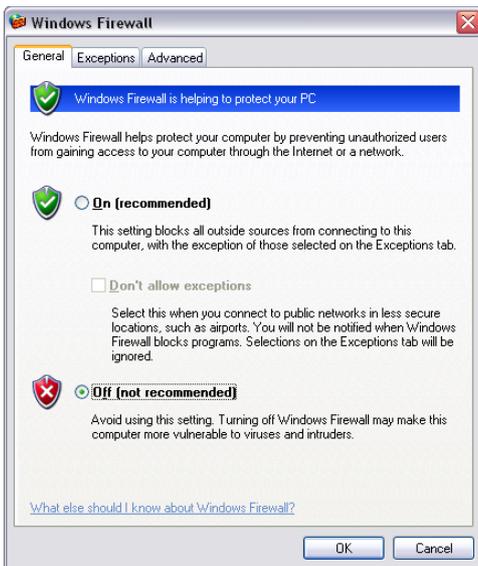
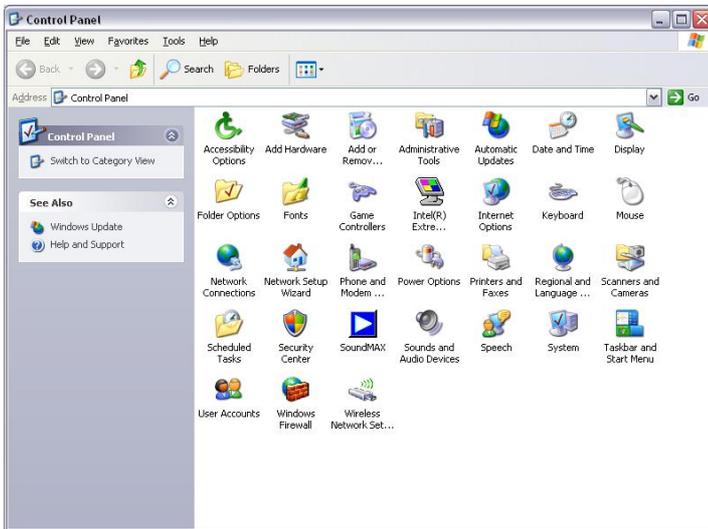
- Follow the directions in Question 2 to reset the Router.
- Check that all the cables are firmly connected at both ends.
- Check the LEDs on the front of the Router. The Power indicator should be on, the Status indicator should flash, and the DSL and LAN indicators should be on as well.
- Please ensure that the settings in the Web-based configuration manager, e.g. ISP username and password, are the same as the settings that have been provided by your ISP.

4. Why can't I get an Internet connection?

For xDSL ISP users, please contact your ISP to make sure the service has been enabled/connected by your ISP and that your ISP username and password are correct.

5. What can I do if my router can't be detected by running installation CD?

- Ensure the Router is powered on.
- Check that all the cables are firmly connected at both ends and all LEDs work correctly.
- Ensure only one network interface card on your PC is activated.
- Click on **Start > Control Panel > Security Center** to disable the setting of **Firewall**.



Note: There might be a potential security issue if you disable the setting of Firewall on your PC. Please remember to turn it back on once you have finished the whole installation procedure and can surf on Internet without any problem

Glossary

Numerics

10/100Base-T

The most widely used standard for Ethernet over twisted pair or copper-based computer networking. Runs at 10 Mb/s, 100 Mb/s, and 1000 Mb/s (1 Gb/s) respectively.

A

ACS

Auto-Configuration Server

ADSL

Asymmetric Digital Subscriber Line

ALG

Application-Level Gateway

ATM

Asynchronous Transfer Mode

C

CHAP

Challenge-Handshake Authentication Protocol

CPE

Customer Premises Equipment

D

DDNS

Dynamic Domain Name System

DHCP

Dynamic Host Configuration Protocol

DNS

Domain Name System

DSCP

Differentiated Services Code Point

DSL

Digital Subscriber Line

Dynamic Routing

The capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions.

E**Ethernet**

A family of frame-based computer networking technologies for local area networks (LANs).

F**Firewall**

An integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

G**Gateway**

A network node equipped for interfacing with another network that uses different protocols.

H**HDSL**

High-Rate Digital Subscriber Line

HTML

Hyper Text Markup Language

I**IP**

Internet Protocol

ISP

Internet Service Provider

K**Kb/s**

Kilo bit per second; a data rate unit.

L**L2TP**

Layer 2 tunneling protocol; a tunneling protocol used to support virtual private networks (VPNs).

LAN

Local Area Network

M**MAC**

Media Access Control

Mb

Megabit; a unit of information commonly used to express the rate data is transferred.

MTU

Maximum Transmission Unit

N

NAT

Network Address Translation

Net mask

The designated IP address routing prefix for a network of computers and devices.

NIC

Network Interface Controller

NTP

Network Time Protocol

O**OAM**

Operations, Administration, and Maintenance

P**PAP**

Password Authentication Protocol

Ping

A computer network tool used to test whether a particular host is reachable across an IP network.

PPP

Point-to-Point Protocol

PPPoE

Point-to-Point Protocol over Ethernet

PVC

Permanent Virtual Circuit

Q**QoS**

Quality of Service

S**Subnet**

See Net mask.

T**TCP**

Transmission Control Protocol

Telnet

Telecommunications network; a network protocol used on the internet or local area network (LAN) connections.

U

UDP

User Datagram Protocol

UPnP

Universal Plug and Play

URL

Uniform Resource Locator

USB

Universal Serial Bus

V**VCI**

Virtual Circuit ID

xDSL

Very High Bit rate Digital Subscriber Line

VLAN

Virtual Local Area Network

VPI

Virtual Path ID

W**WAN**

Wide Area Network