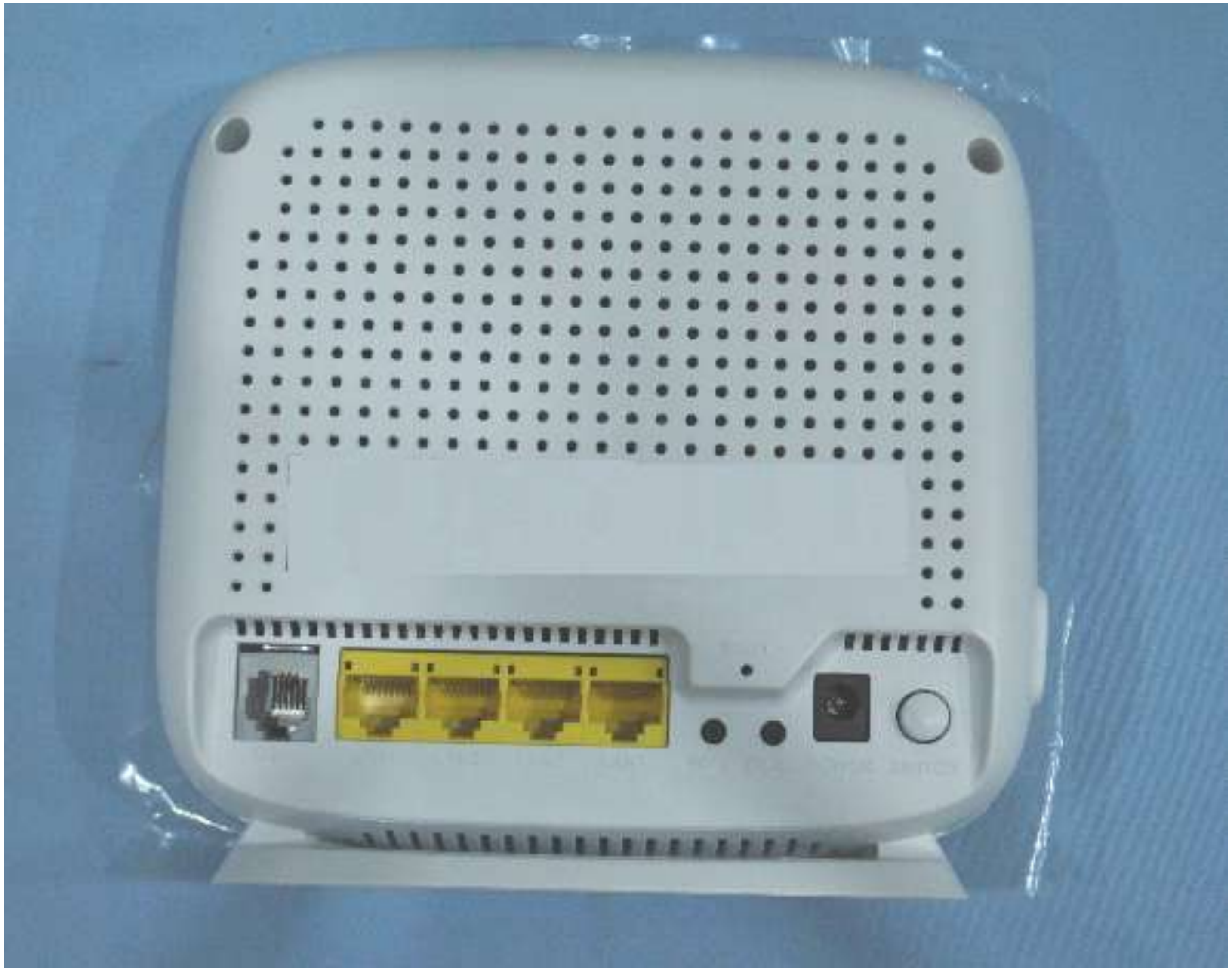
User Manual

4 port VDSL2 11n Router

Model:SR505N

Table of Contents



Device Installation

The DSL connects two separate physical interfaces, an ADSL (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 ADSL connection, if the ADSL 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 **192.168.1.1** and the subnet mask is **255.255.255.0**, the default management Username is “admin” and the default Password is “admin.”

Network Connections

Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL 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 ADSL 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 D-Link Router using the web-based configuration utility.

Web-based Configuration Utility

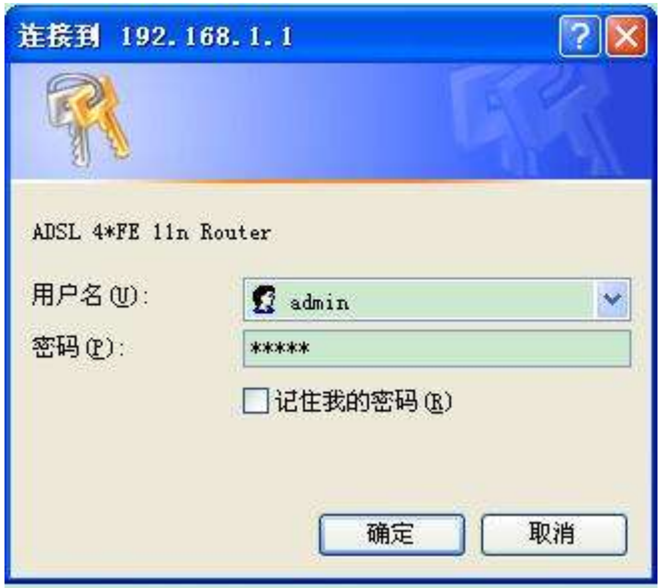
Connect to the Router

The default IP address for ADSL MODEM is: 192.168.1.1; The Subnet Mask is：255.255.255.0. Users can configure ADSL MODEM through an Internet browser. ADSL 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 ADSL MODEM, such as set the IP address of the network card to one of the "192.168.1.2" ～ "192.168.1.254".
2. Set the computer's gateway the same IP address as the ADSL Modem's.
3. Set computer's DNS server the same as ADSL 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 (**192.168.1.1**).

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.



连接到 192.168.1.1

ADSL 4*FE 11n Router

用户名(U): admin

密码(P): *****

□记住我的密码(R)

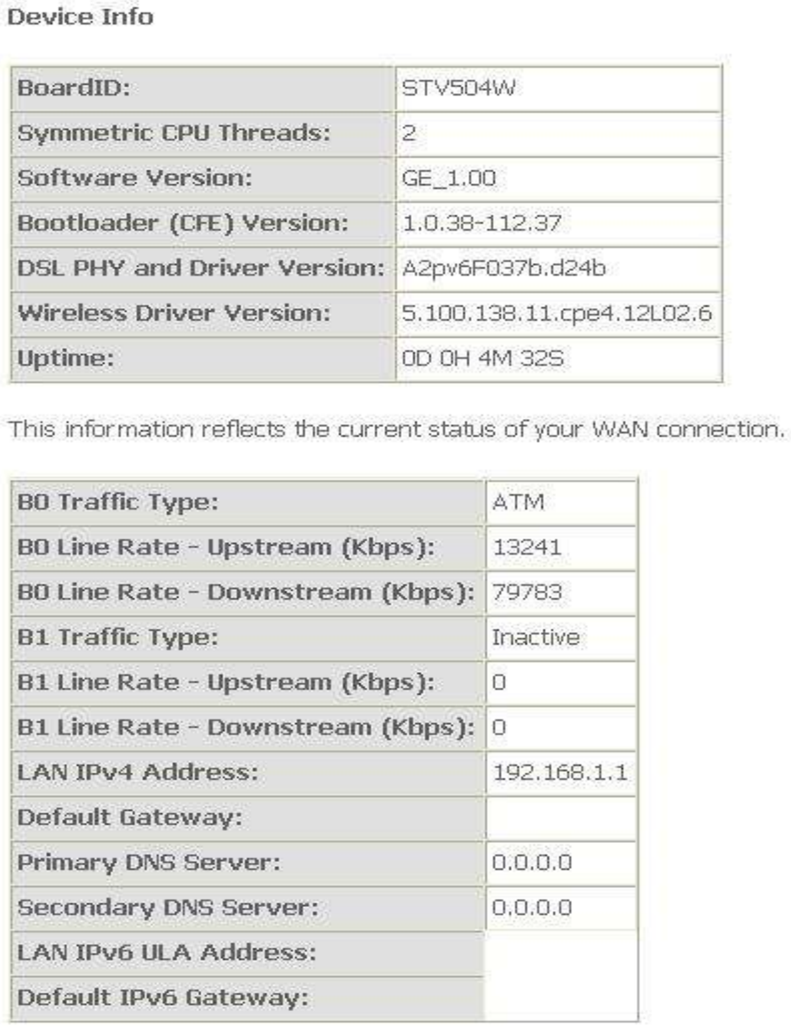
Device Info

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

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

BoardID:	STV504W
Symmetric CPU Threads:	2
Software Version:	GE_1.00
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
Uptime:	0D 0H 4M 32S

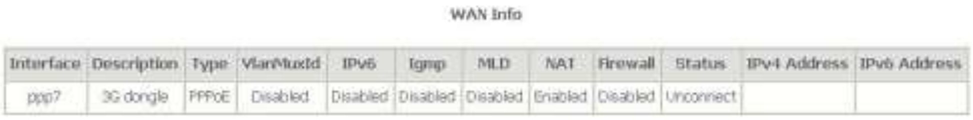
This information reflects the current status of your WAN connection.

B0 Traffic Type:	ATM
B0 Line Rate - Upstream (Kbps):	13241
B0 Line Rate - Downstream (Kbps):	79783
B1 Traffic Type:	Inactive
B1 Line Rate - Upstream (Kbps):	0
B1 Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	

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.

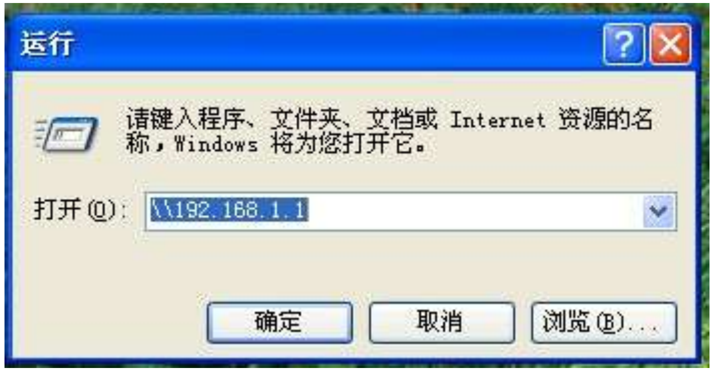


WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ppp7	3G dongle	PPPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	Unconnect		

USB Access Methods

We can access the USB devices and handle some files with the following steps. We access the USB devices through the samba as the following pictures.



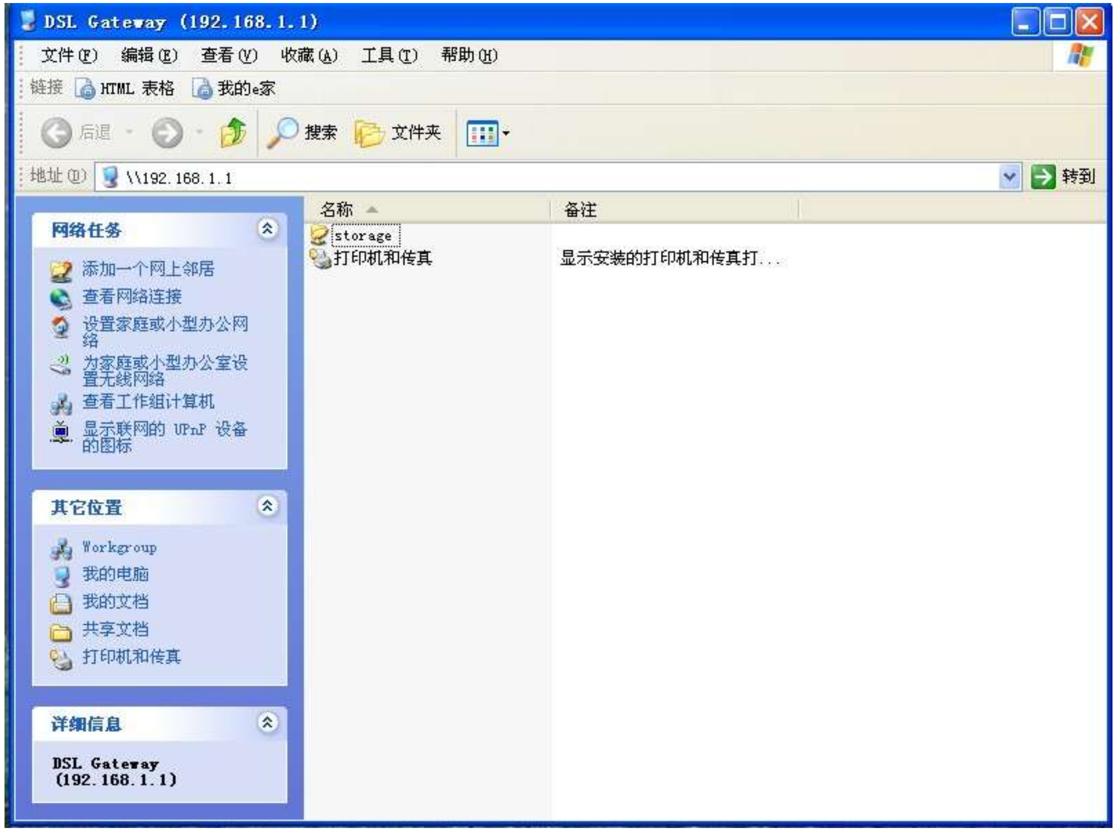
运行

请键入程序、文件夹、文档或 Internet 资源的名称，Windows 将为您打开它。

打开(O): \\192.168.1.1

Picture 1

As the picture 1 show, we enter the route of the ONT.

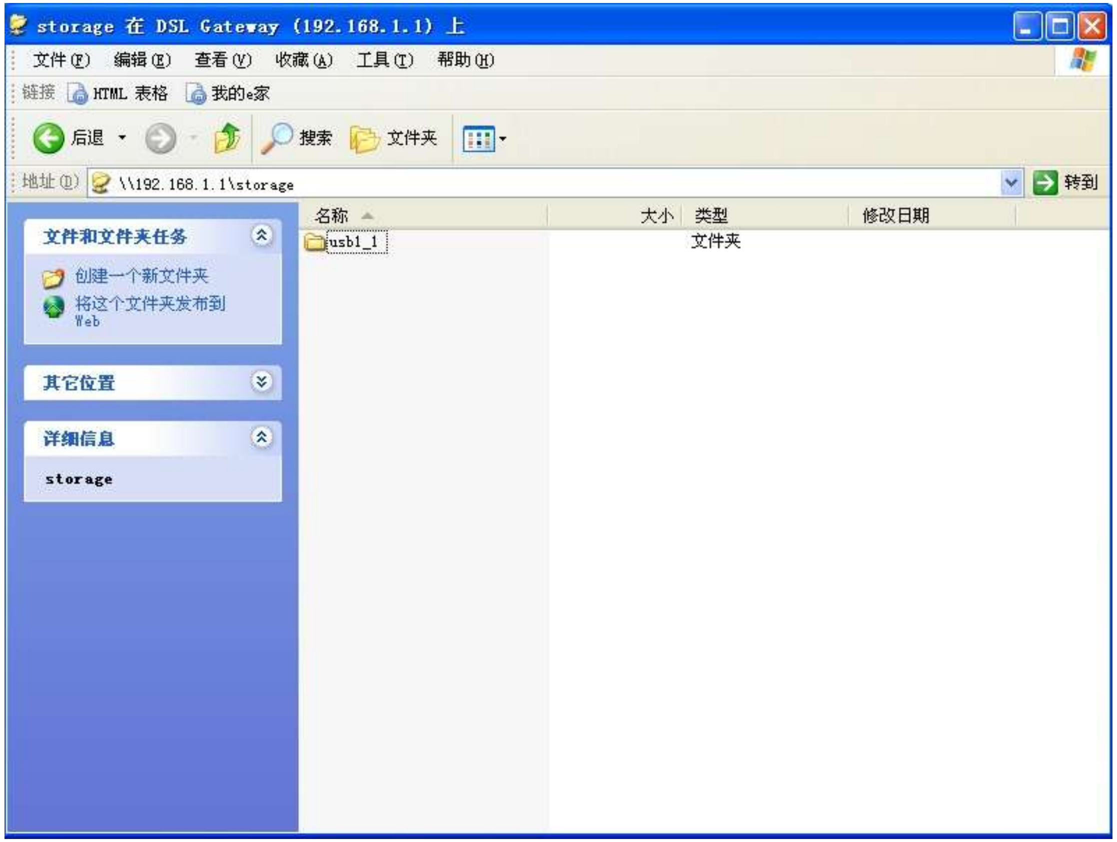


地址(D) \\192.168.1.1

名称	备注
storage	
打印机和传真	显示安装的打印机和传真打...

Picture 2

We can find the file which name is storage. Enter the file, we find the usb1_1 (As show as the Picture 3). This file is our USB device.



storage 在 DSL Gateway (192.168.1.1) 上

地址(D) \\192.168.1.1\storage

名称	大小	类型	修改日期
usb1_1		文件夹	

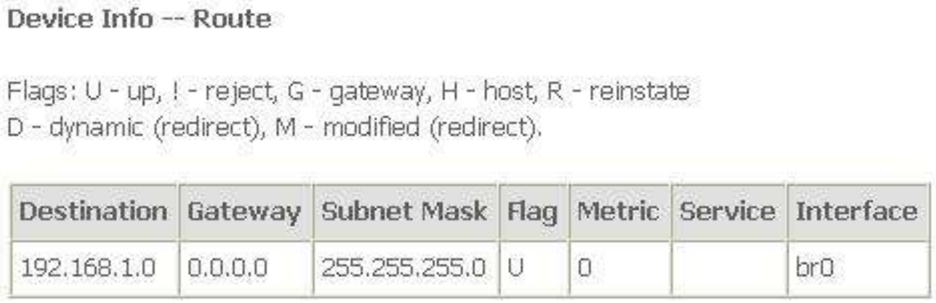
Picture 3

After accessed the usb1_1, we can do some operating what you want to do.

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

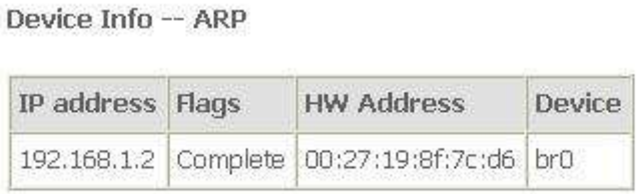
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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.



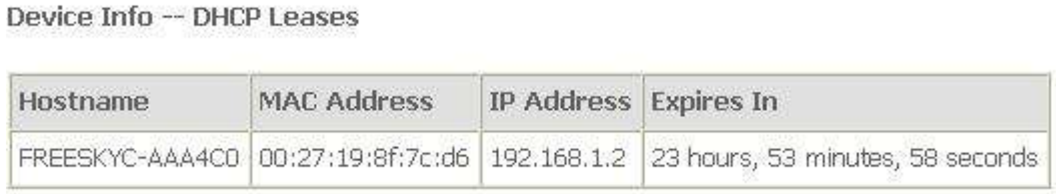
Device Info -- ARP

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

Advanced Setup

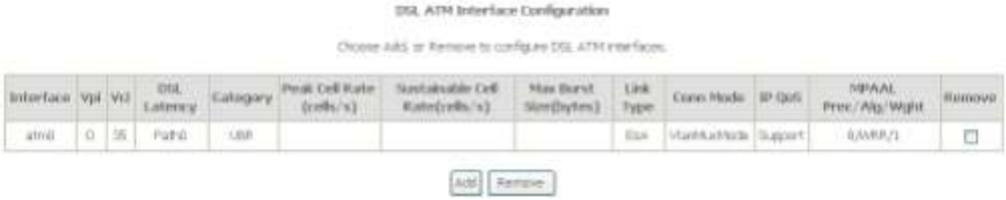
This chapter include the more advanced features used for network management and security as well as administrative tools to manage the Router, view status and other information used to examine performance and for troubleshooting.

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.

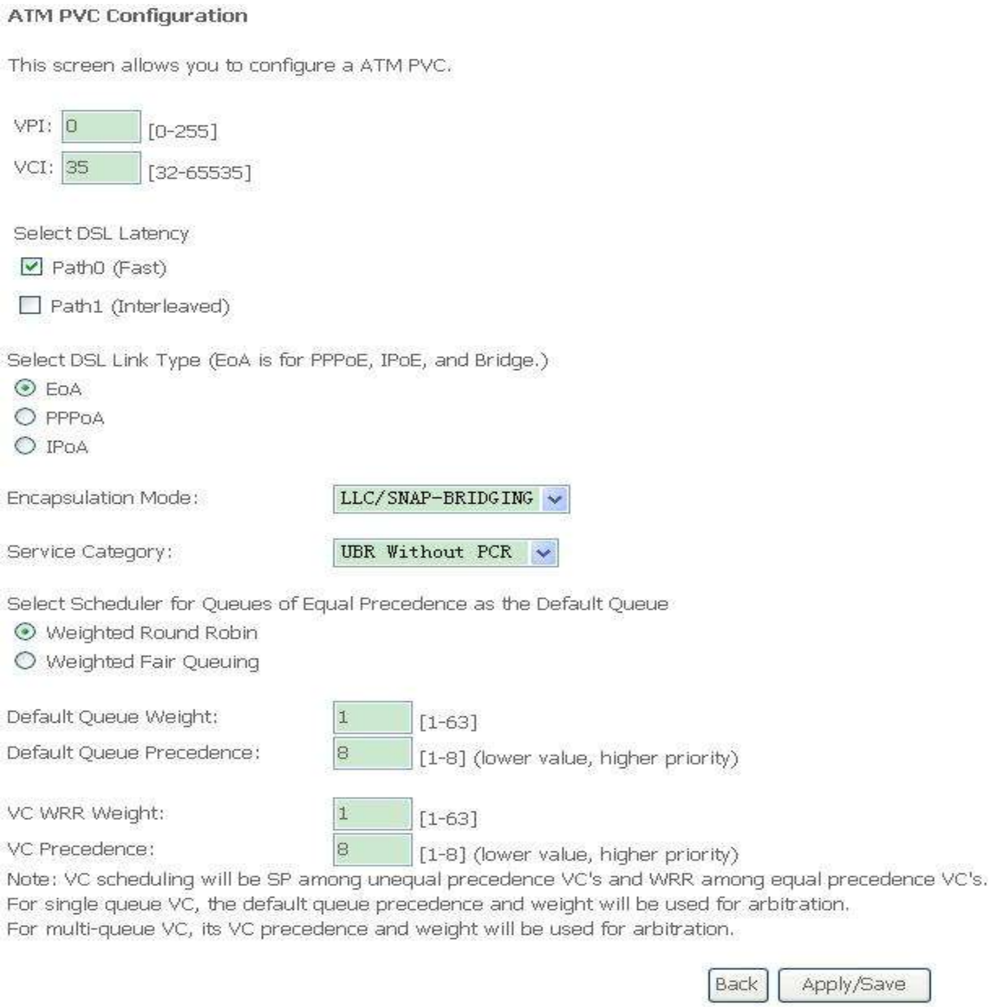
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate (cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	8/WRR/1	□

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 [0-255]

VCI: 35 [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: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select Scheduler for Queues of Equal Precedence as the Default Queue

● Weighted Round Robin

○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

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

VC WRR Weight: 1 [1-63]

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

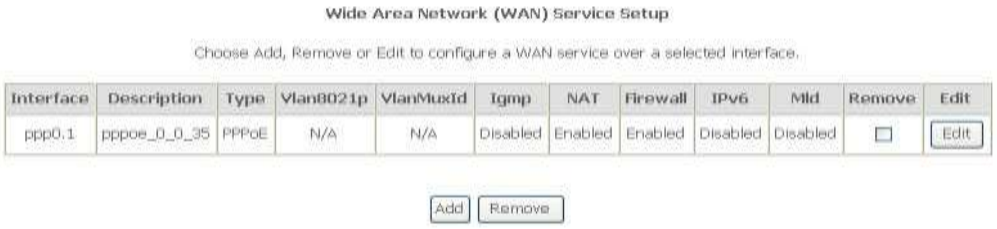
Note: VC scheduling will be SP among unequal precedence VC's and WRR among equal precedence VC's.
For single queue VC, the default queue precedence and weight will be used for arbitration.
For multi-queue VC, its VC precedence and weight will be used for arbitration.

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.

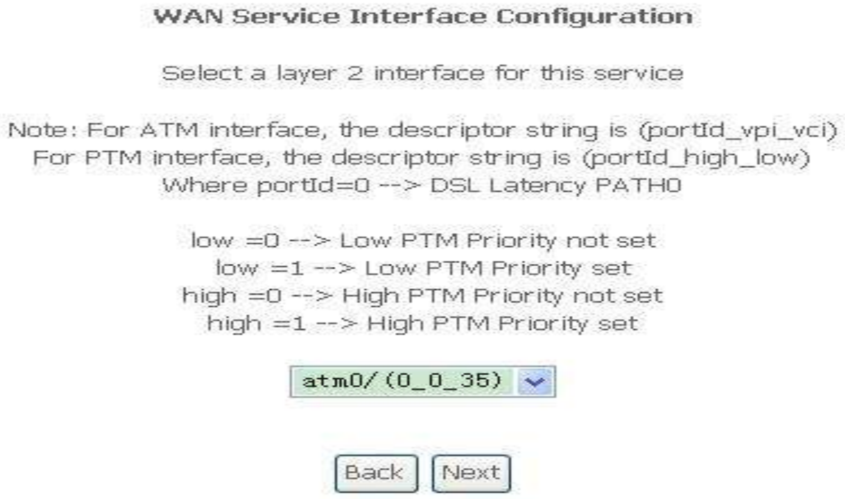


Wide Area Network (WAN) Service Setup

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	□	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

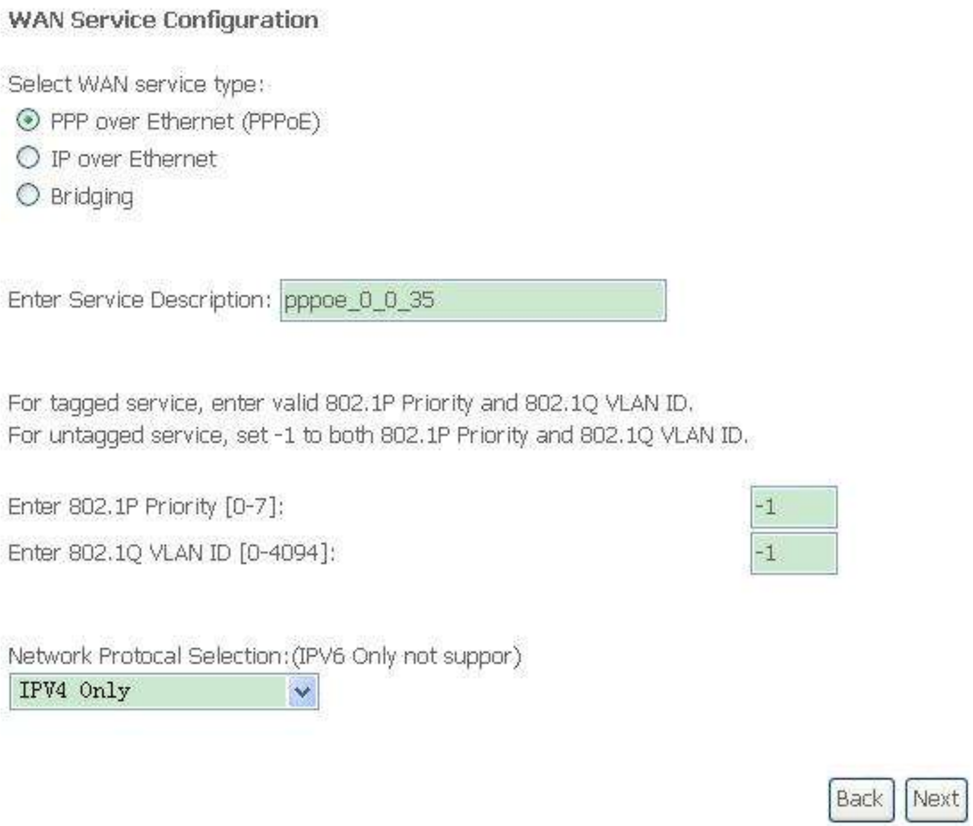
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

atm0/(0_0_35)

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: pppoe_0_0_35

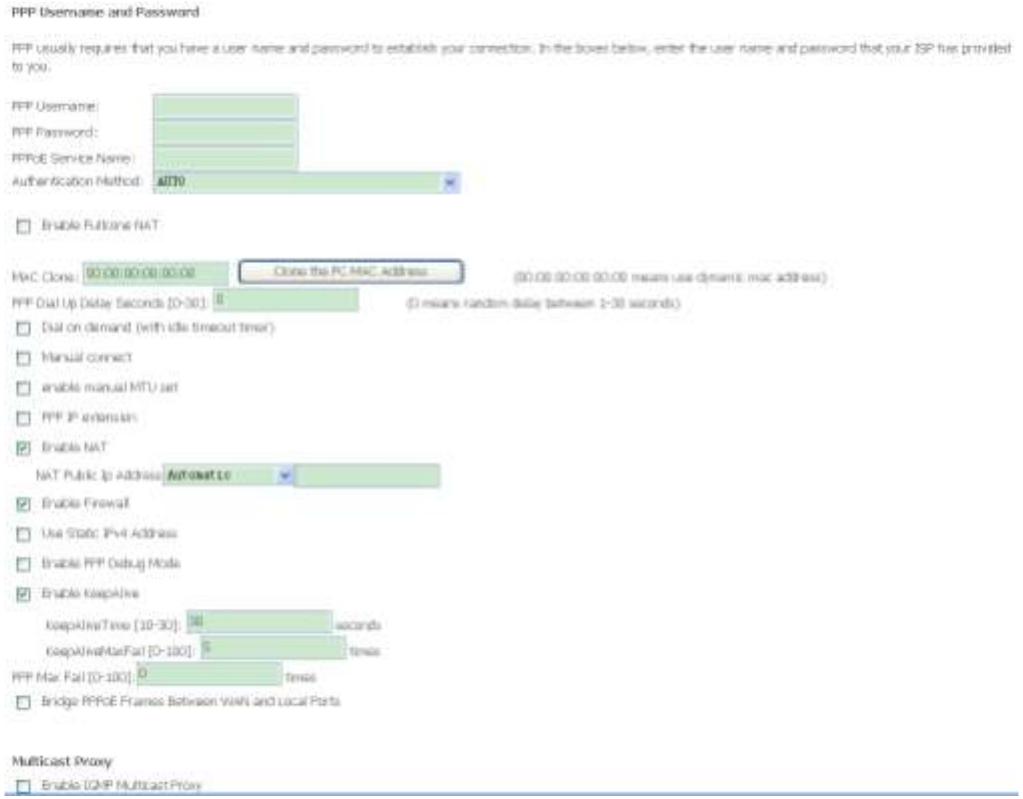
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1

Network Protocal Selection:(IPV6 Only not suppor)
IPV4 Only

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 and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

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

□ Enable Fullcone NAT

MAC Clone: 00:00:00:00:00:02 (00:00:00:00:00:00 means use dynamic mac address)
PPP Dial Up Delay Seconds [0-30]: 0 (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]: 30 seconds
KeepAliveMaxFail [0-100]: 5 times
PPP Max Fail [0-100]: 0 times

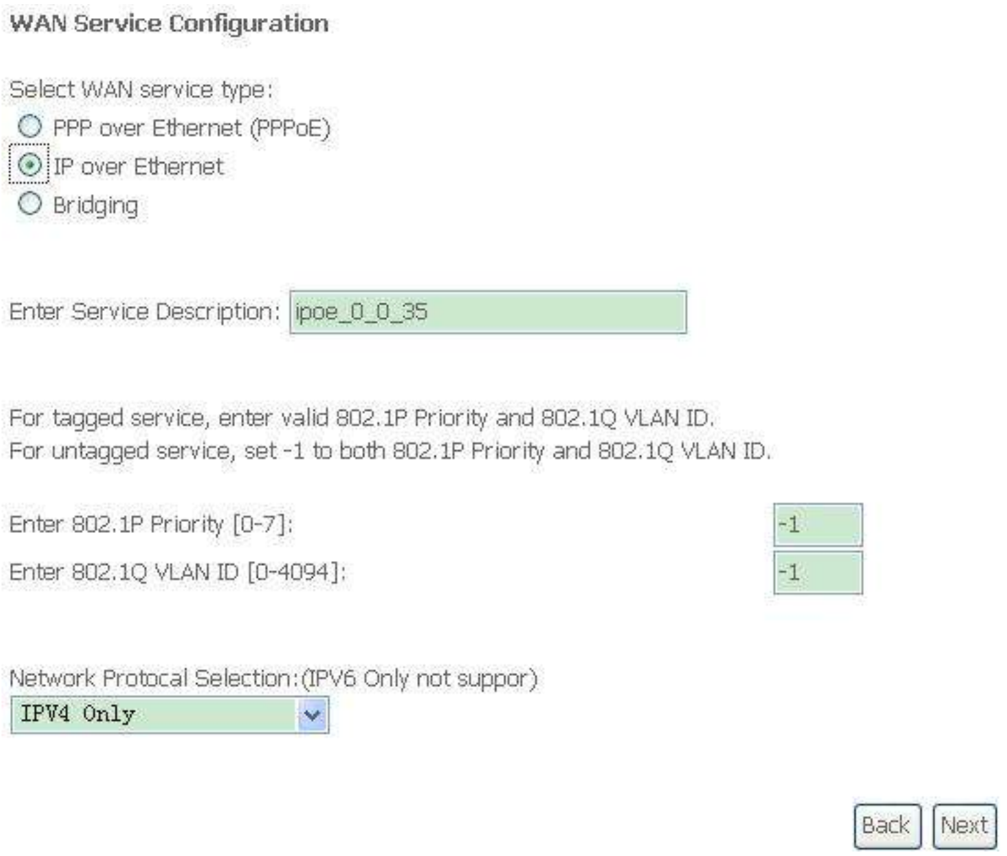
□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

WAN Service Configuration – IPoE

Click the IP over Ethernet 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: ipoe_0_0_35

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.

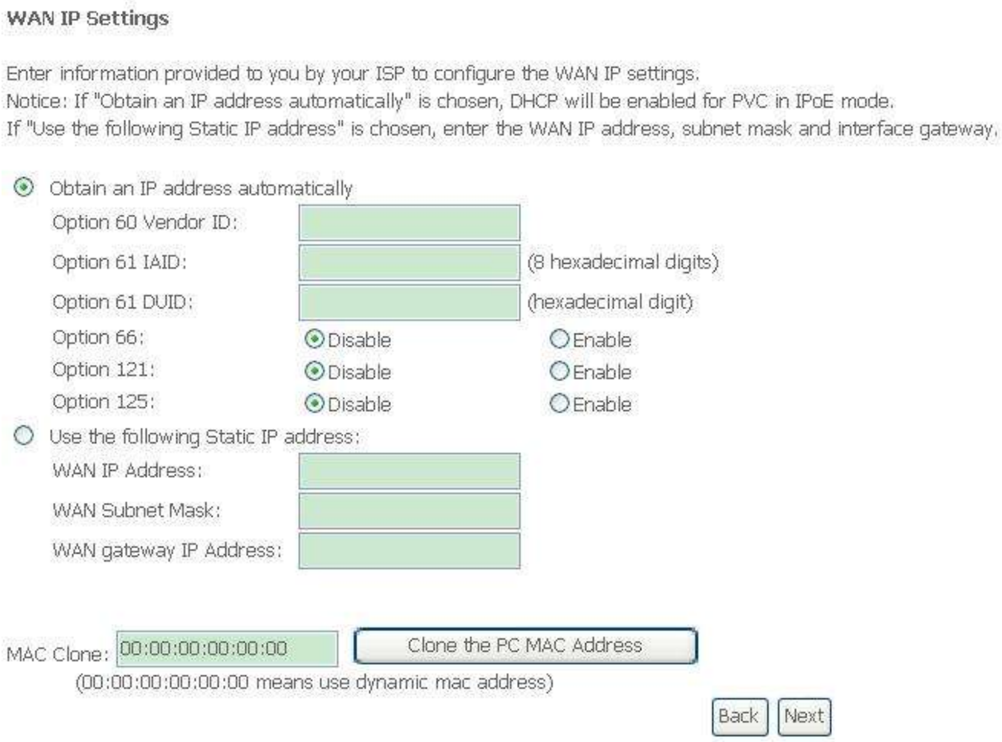
Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Network Protocal Selection:(IPV6 Only not suppor)
IPV4 Only

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

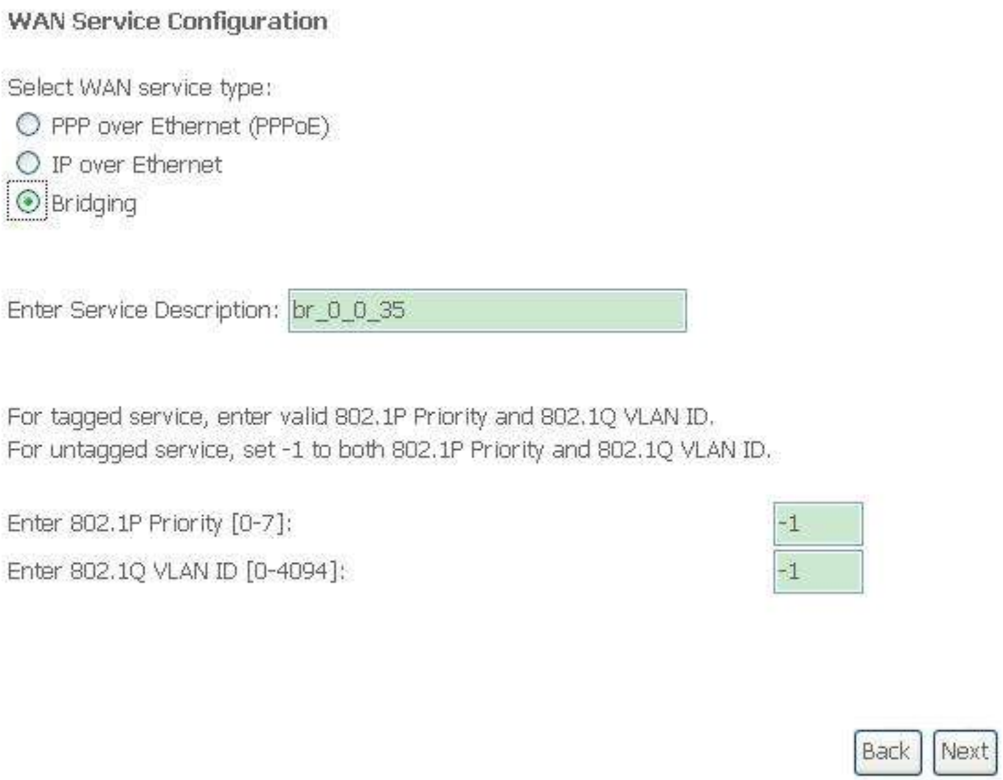
○ Use the following Static IP address:

WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

MAC Clone: 00:00:00:00:00:00
(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: br_0_0_35

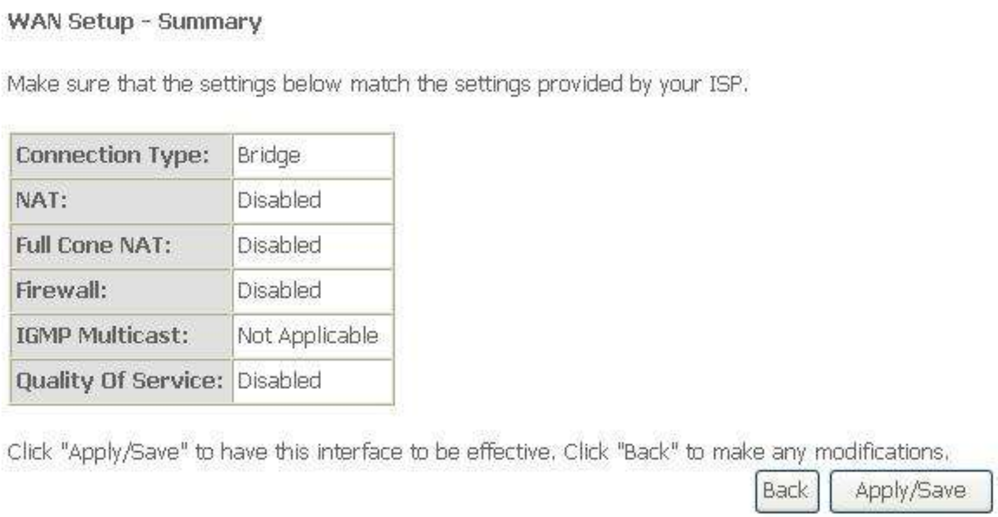
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

WAN Service Configuration – BRIDGING

This summary window allows you to confirm the bridging settings you have just made. Click the **Apply /Save** button to save your new bridging settings and restart the Router.



WAN Setup - Summary

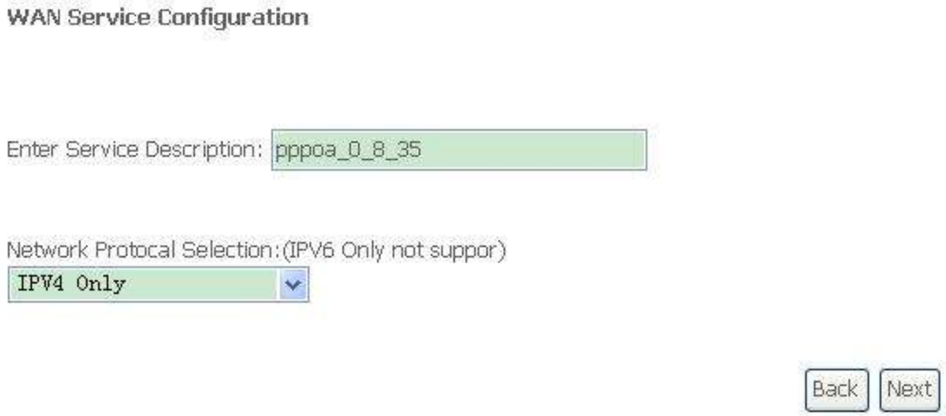
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

WAN Service Configuration – PPPoA

This window allows you to enter service description. Click the **Next** button to continue.



WAN Service Configuration

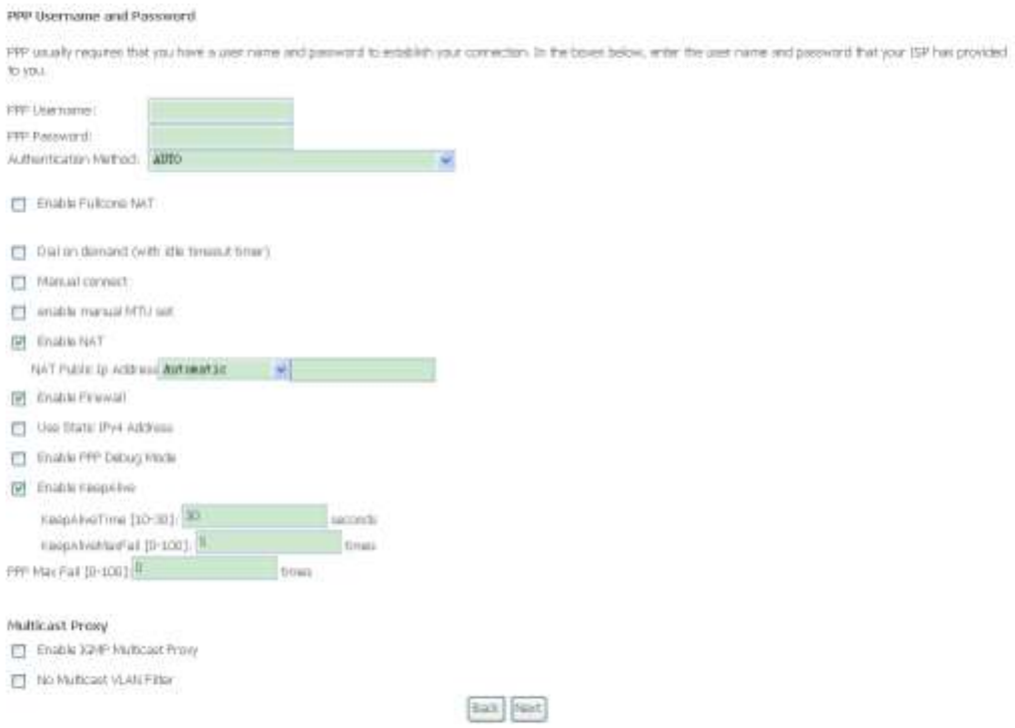
Enter Service Description: pppoa_0_8_35

Network Protocal Selection:(IPV6 Only not suppor)

IPV4 Only

WAN Service Configuration – PPPoA

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 and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
PPP Password:
Authentication Method: AUTO

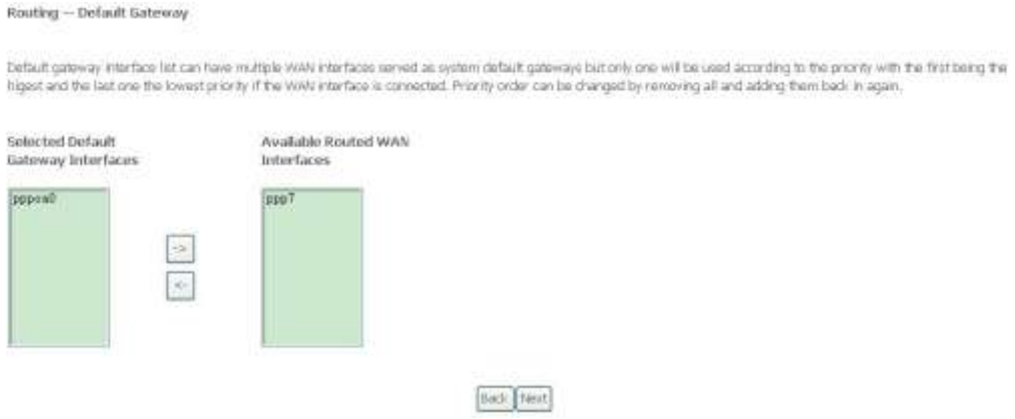
□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)
□ Manual connect
□ enable manual MTU set
☑ Enable NAT
NAT Public Ip Address Automatic
☑ Enable Firewall
□ Use Static IPv4 Address
□ Enable PPP Debug Mode
☑ Enable KeepAlive
KeepAliveTime [10-30]: 30 seconds
KeepAliveMaxFail [0-100]: 5 times
PPP Max Fail [0-100]: 0 times

Multicast Proxy
□ Enable IGMP Multicast Proxy
□ No Multicast VLAN Filter

WAN Service Configuration –PPPoA

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 higest 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 **Next** button to continue.



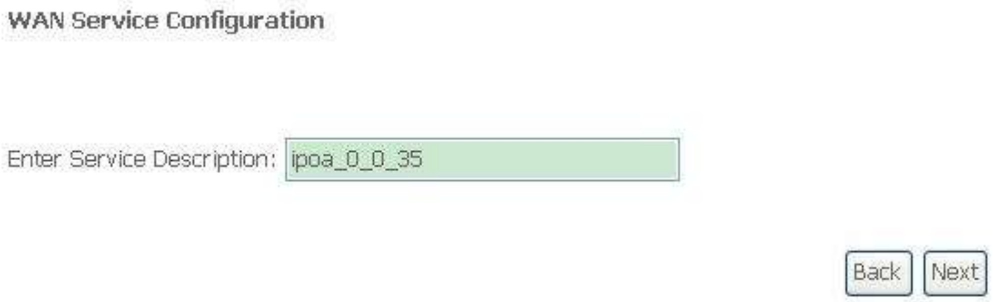
Routing -- Default Gateway

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 higest 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
pppoa0	ppp7

WAN Service Configuration – IPoA

This window allows you to enter service description. Click the **Next** button to continue.

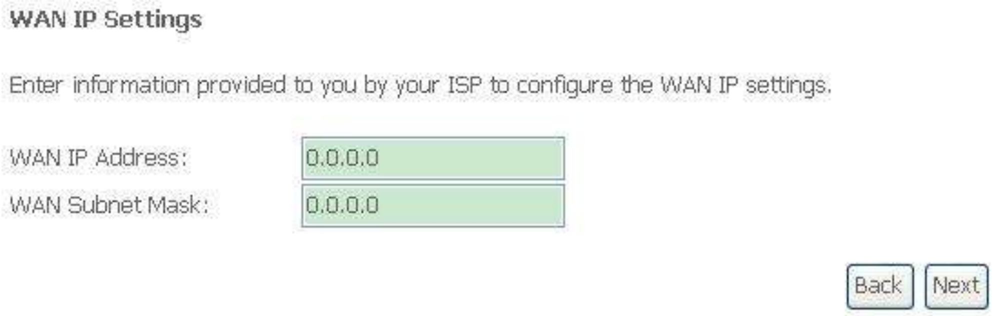


WAN Service Configuration

Enter Service Description: ipoa_0_0_35

WAN Service Configuration – IPoA

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

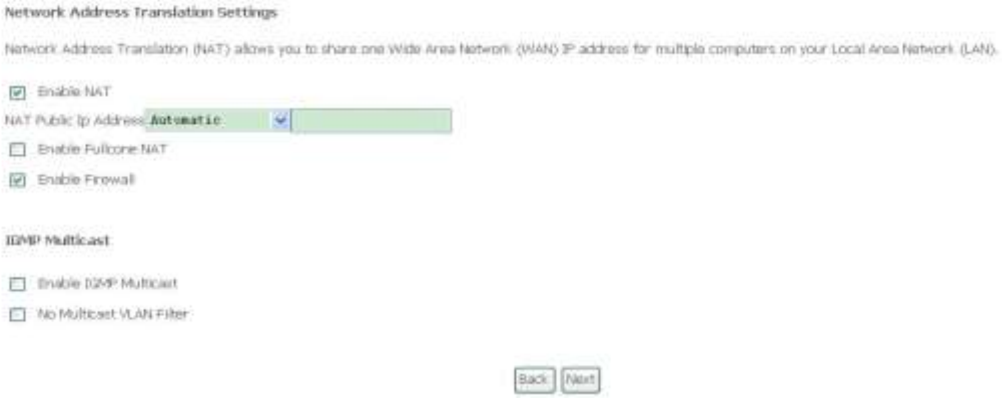
Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address: 0.0.0.0

WAN Subnet Mask: 0.0.0.0

WAN Service Configuration – IPoA

This window allows you to enable or disable Network Address Translation and a firewall for your Router. In addition, you can enable or disable IGMP multicasting. Click the **Next** button to continue.



Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☑ Enable NAT

NAT Public Ip Address Automatic

□ Enable Fullcone NAT

☑ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast

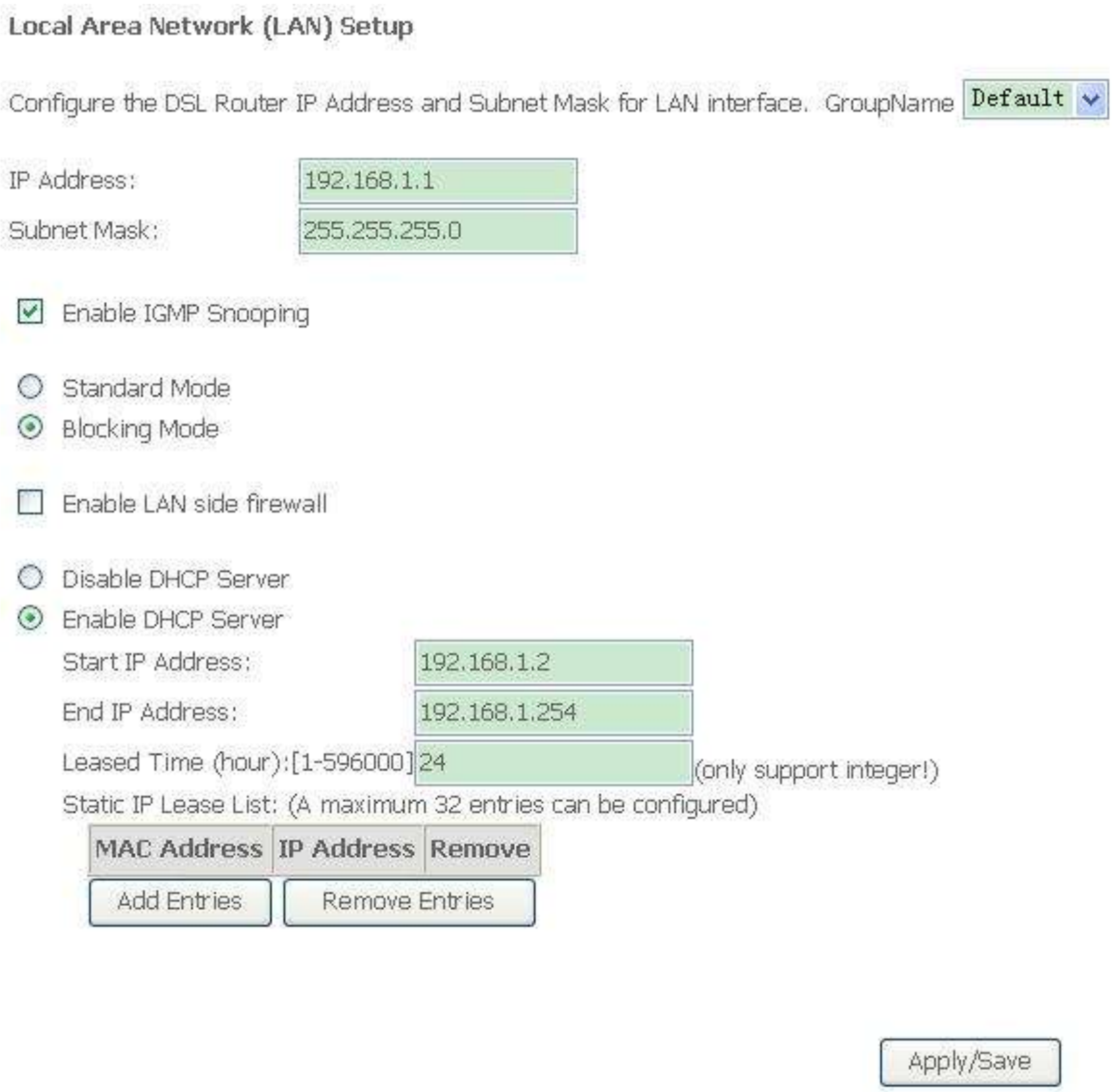
□ No Multicast VLAN Filter

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.

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: 192.168.1.1

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode

● Blocking Mode

□ Enable LAN side firewall

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

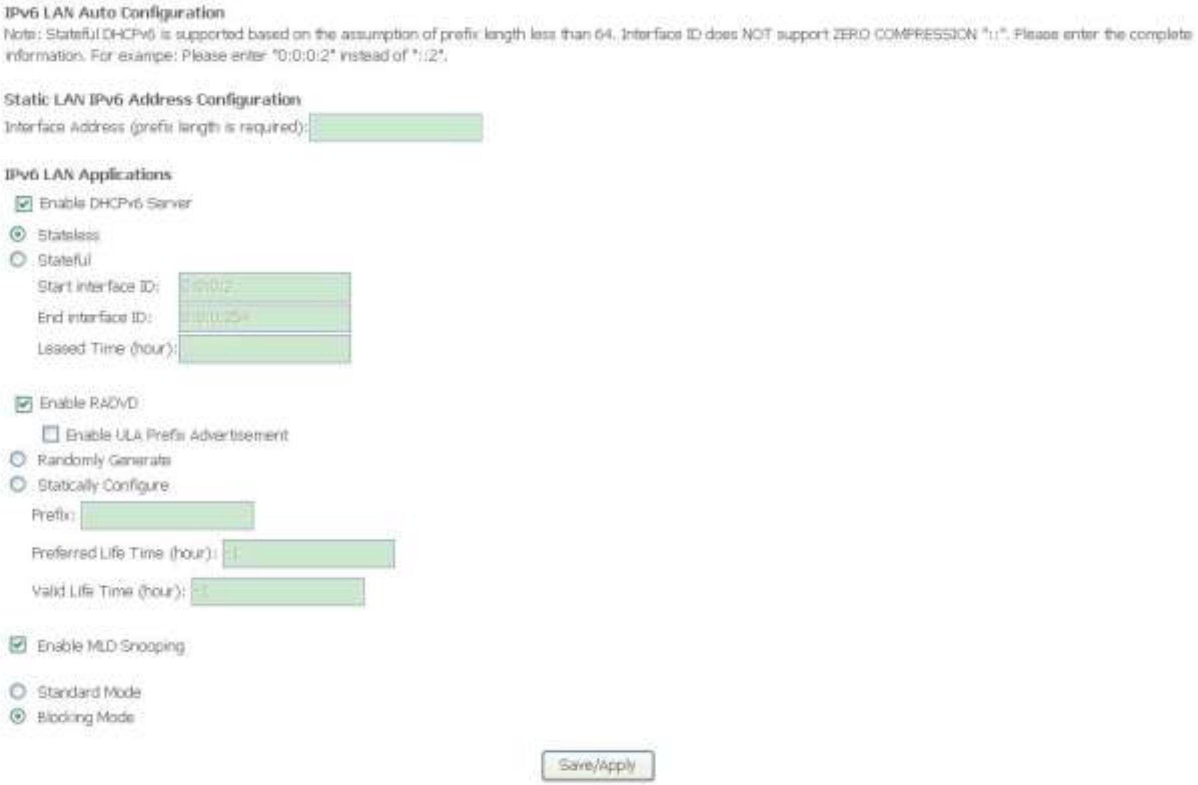
Leased Time (hour):[1-596000] 24 (only support integer!)

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

MAC Address	IP Address	Remove

To access the **IPv6 LAN Auto Configuration** window, click the **IPv6 AutoConfig** button in the **LAN** directory.

This window allows you to set up IPv6 LAN Auto Configuration. When you are finished, click the **Save /Apply** 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 exampe: 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: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour):

☑ Enable RADVD

□ Enable ULA Prefix Advertisement

○ Randomly Generate

○ Statically Configure

Prefix:

Preferred Life Time (hour): -1

Valid Life Time (hour): -1

☑ Enable MLD Snooping

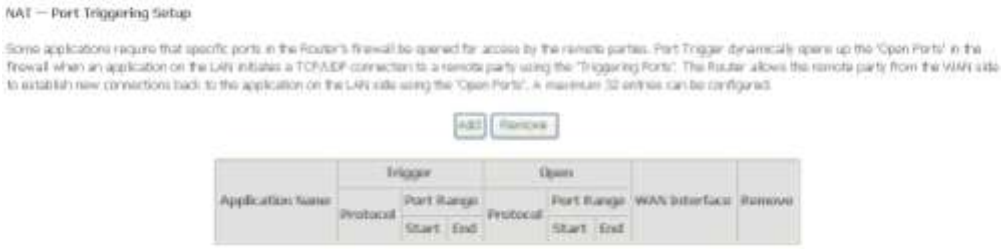
○ Standard Mode

● Blocking Mode

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.



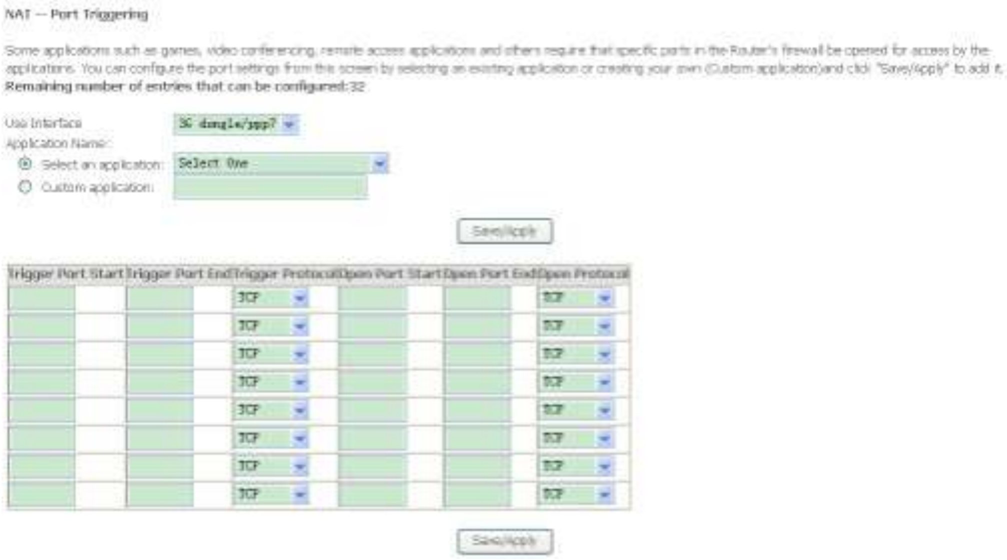
NAT -- Port Triggering Setup

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		Start	End		

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: 3G dongle/ppp7

Application Name:

● Select an application: Select One

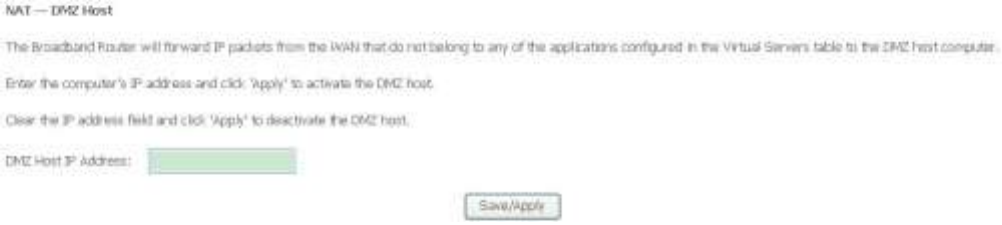
○ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			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:

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.

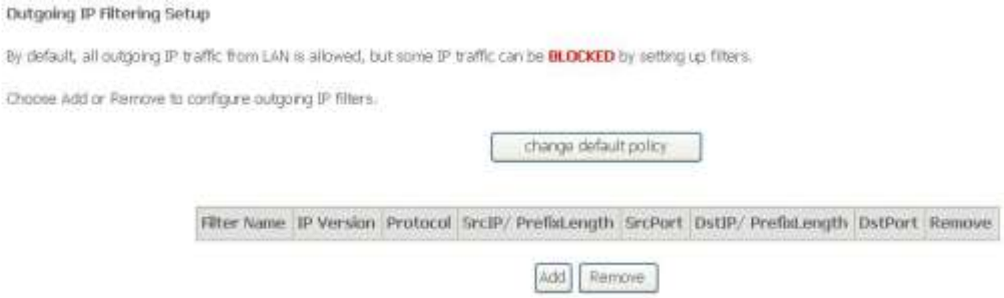
IP Filtering - Outgoing

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

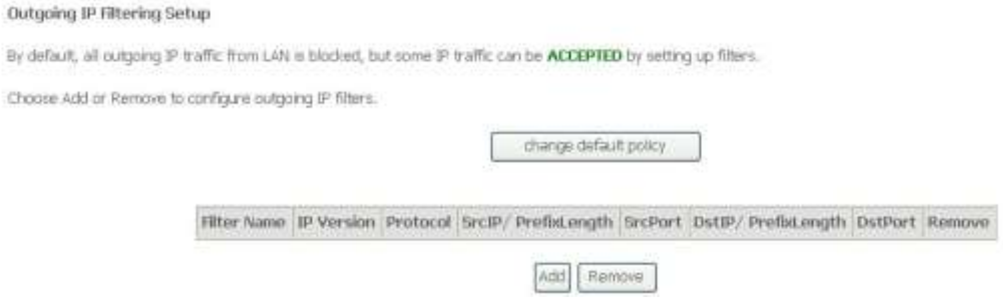
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

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

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.



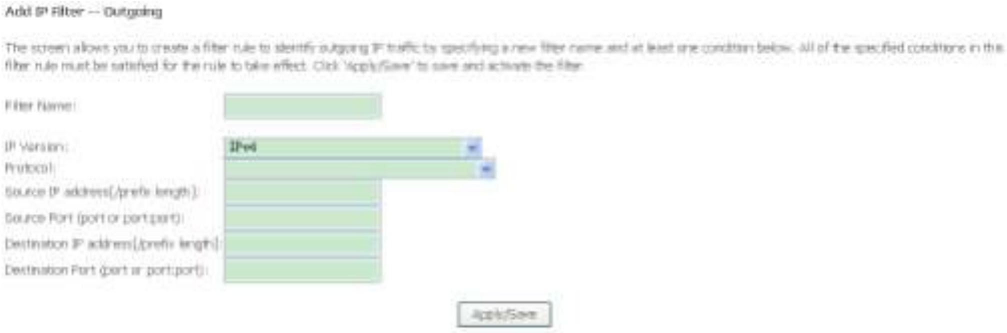
Outgoing IP Filtering Setup

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: IPv4

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

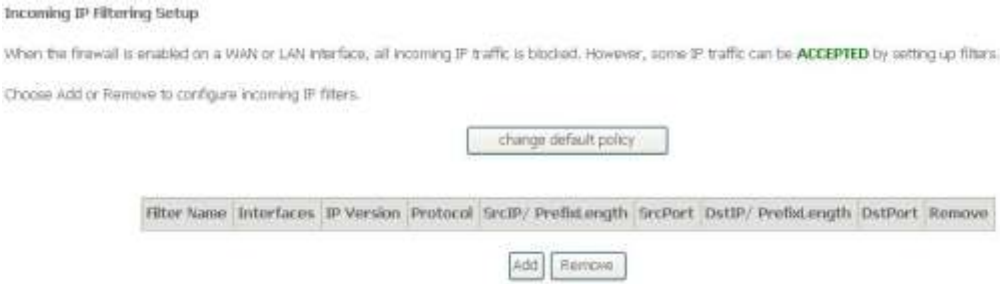
IP Filtering – Incoming

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

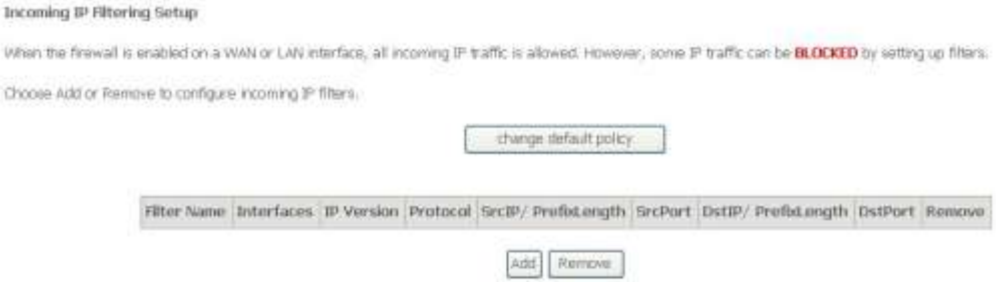
When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is blocked. However, some IP traffic can be **ACCEPTED** by setting up filters.

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.



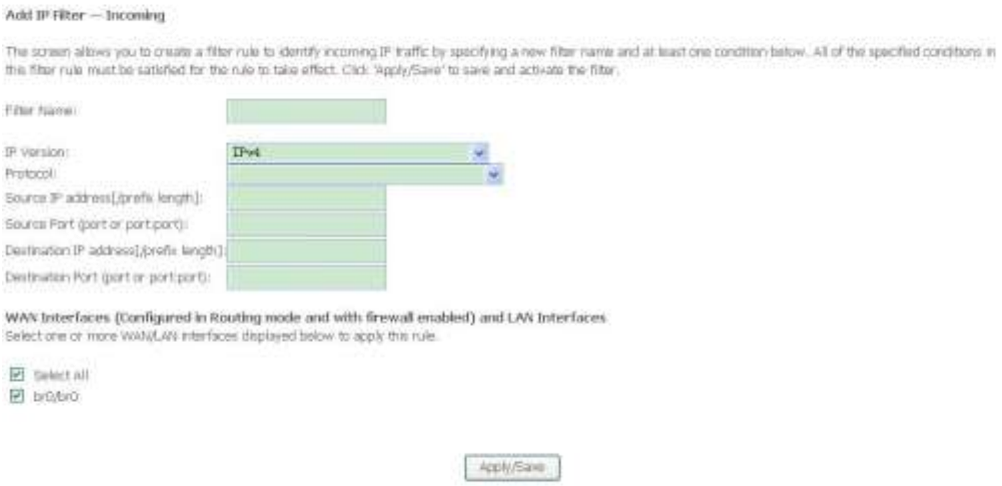
Incoming IP Filtering Setup

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

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:	IPv4
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.

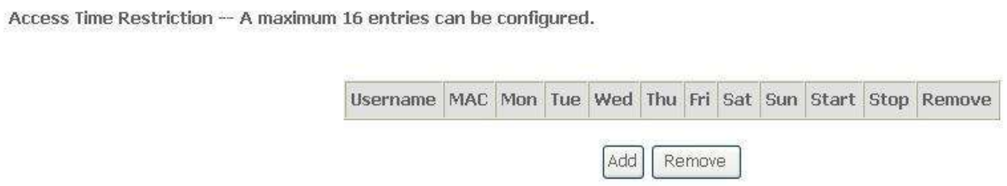
☑ Select All

☑ br0/br0

Parental Control

Use this window to deny access to specified MAC address.

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



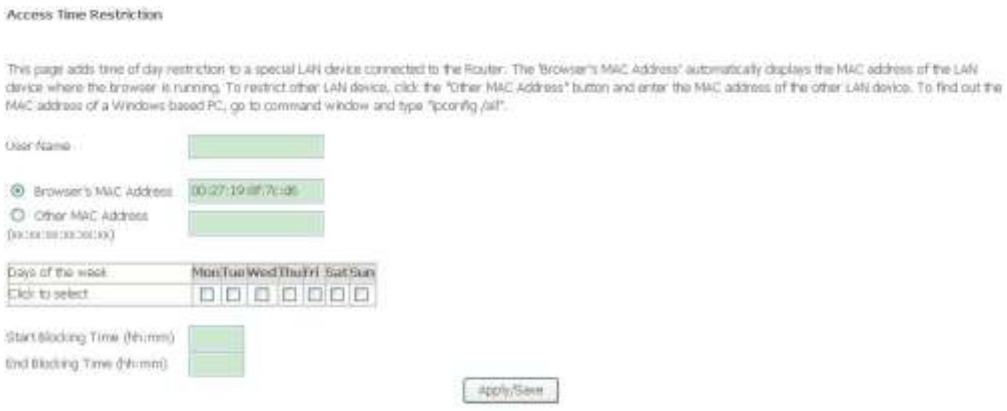
Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

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 00:27:19:8f:7c:d6

○ Other MAC Address (xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

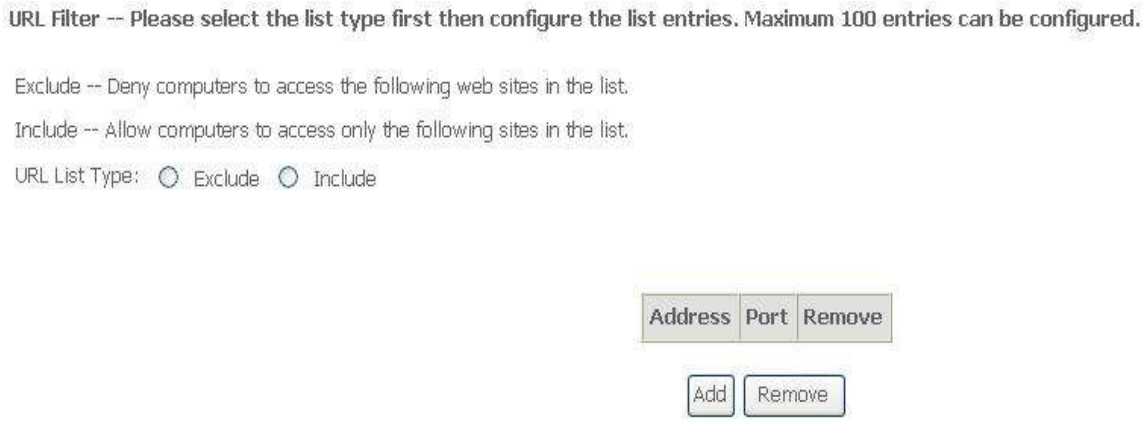
Start Blocking Time (hh:mm)

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.

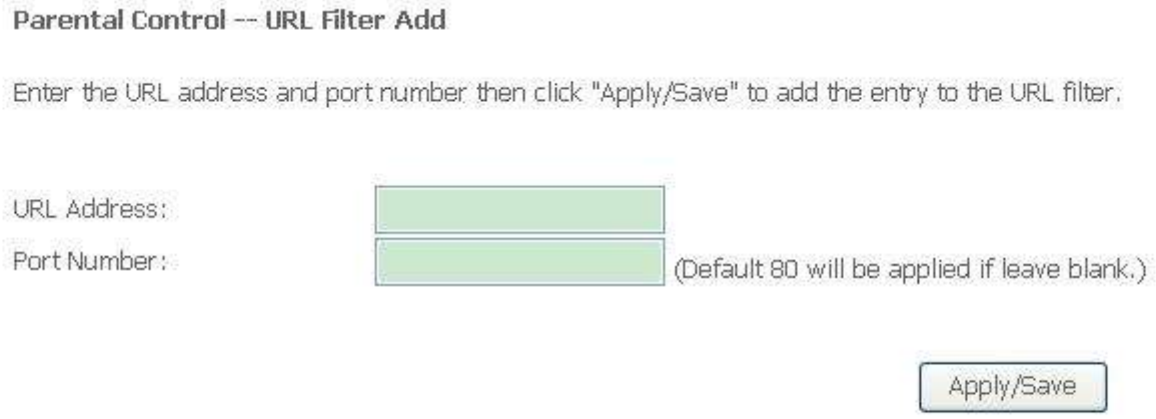
Exclude -- Deny computers to access the following web sites in the list.

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:

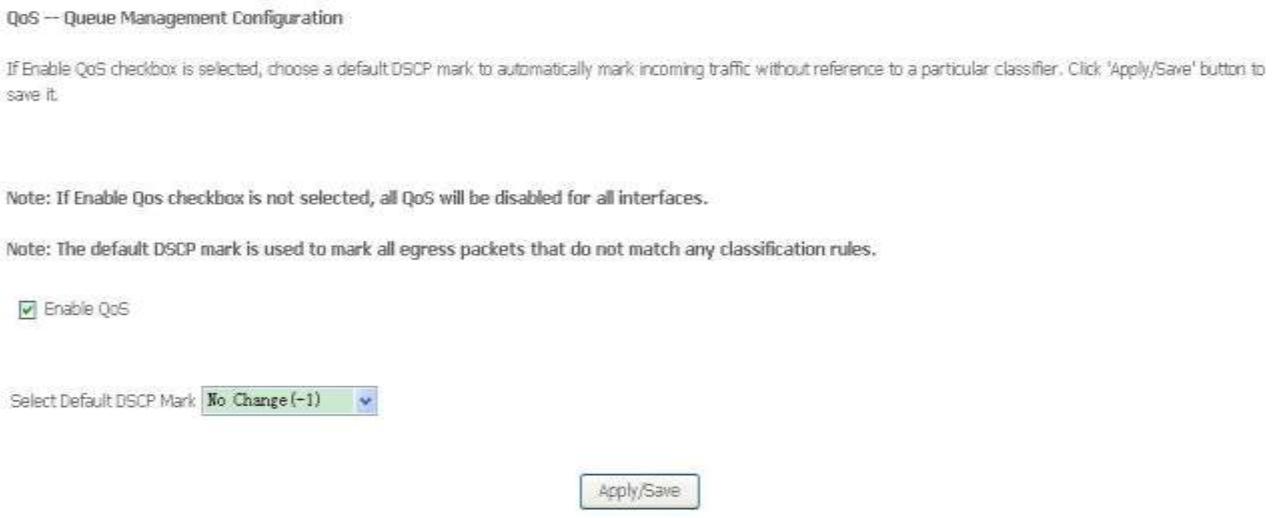
Port Number: (Default 80 will be applied if leave blank.)

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.

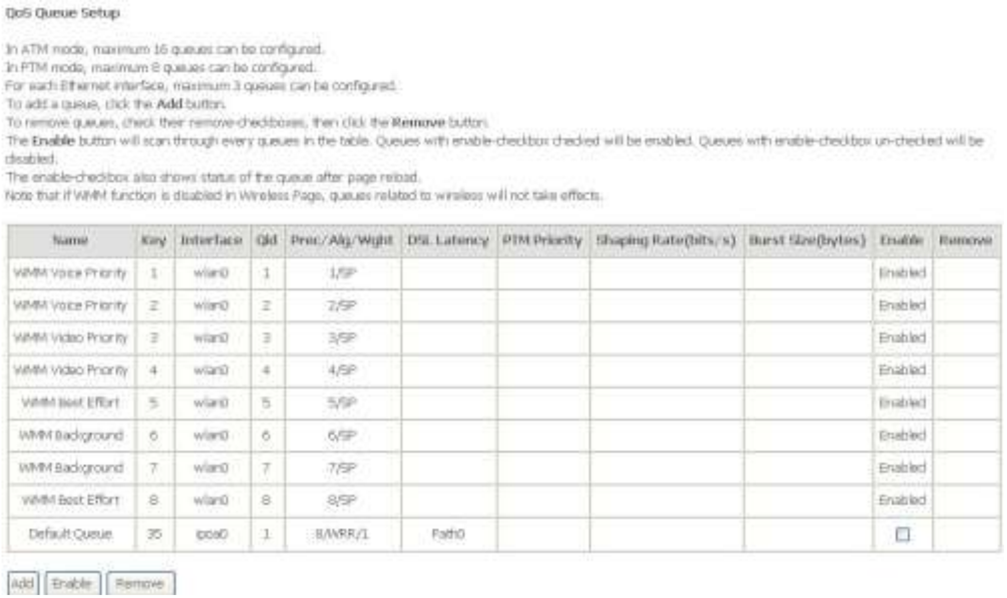
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

Queue Config

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



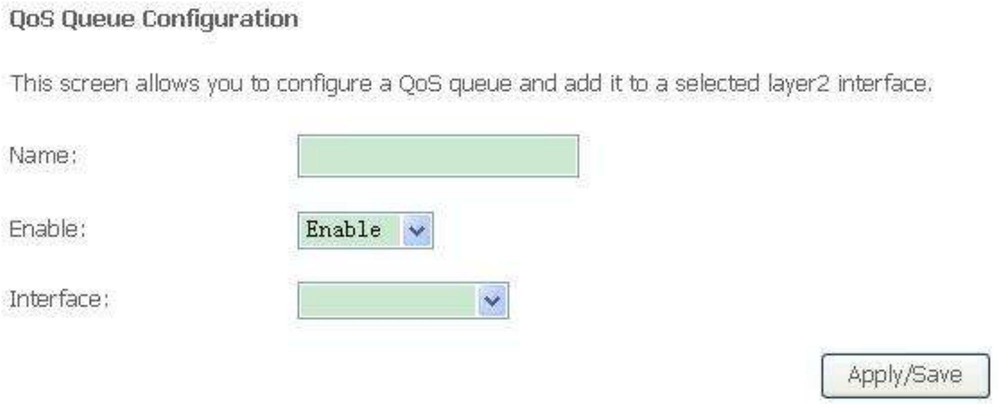
QoS Queue Setup

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				□	

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.



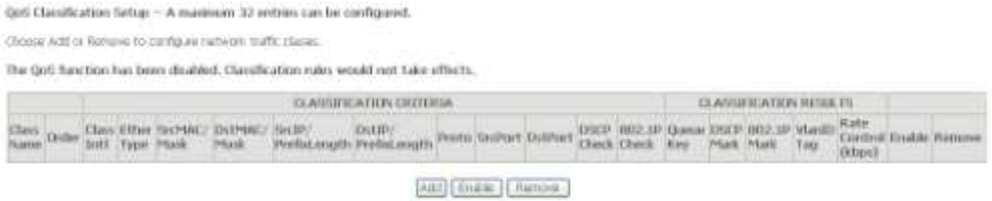
QoS Queue Configuration

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

Name:	
Enable:	Enable
Interface:	

QoS Classification

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



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

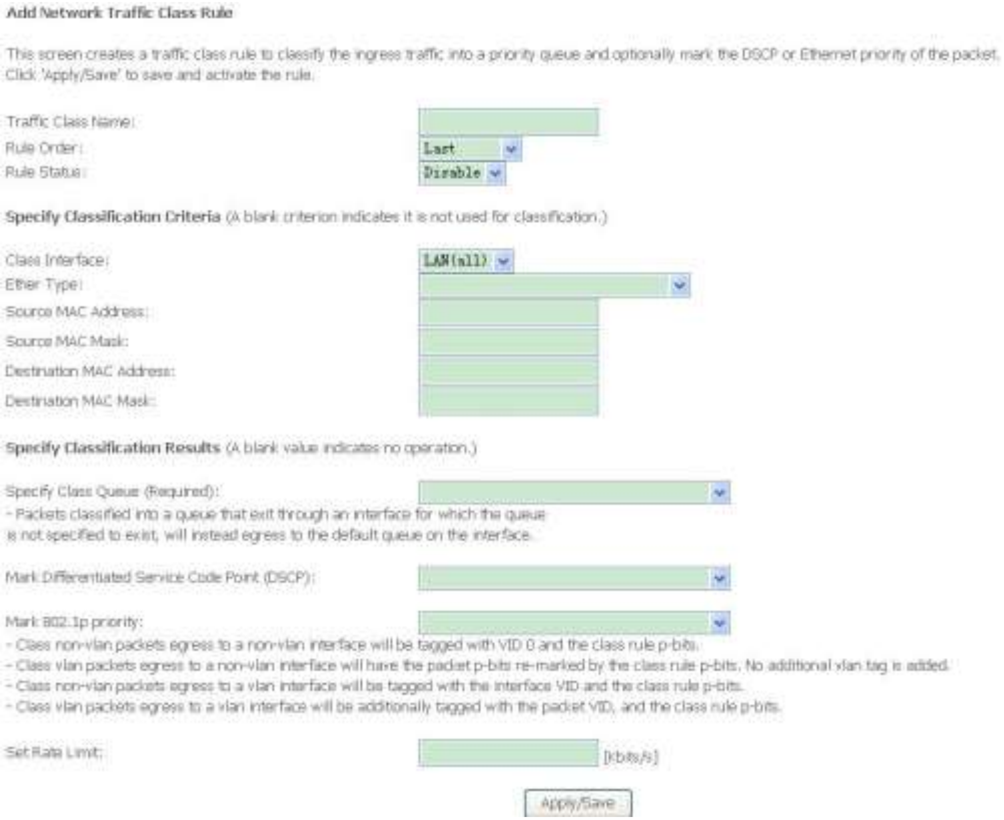
Choose Add or Remove to configure network traffic classes.

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

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: Last
Rule Status: Disable

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

Class Interface: LAN(all)
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.

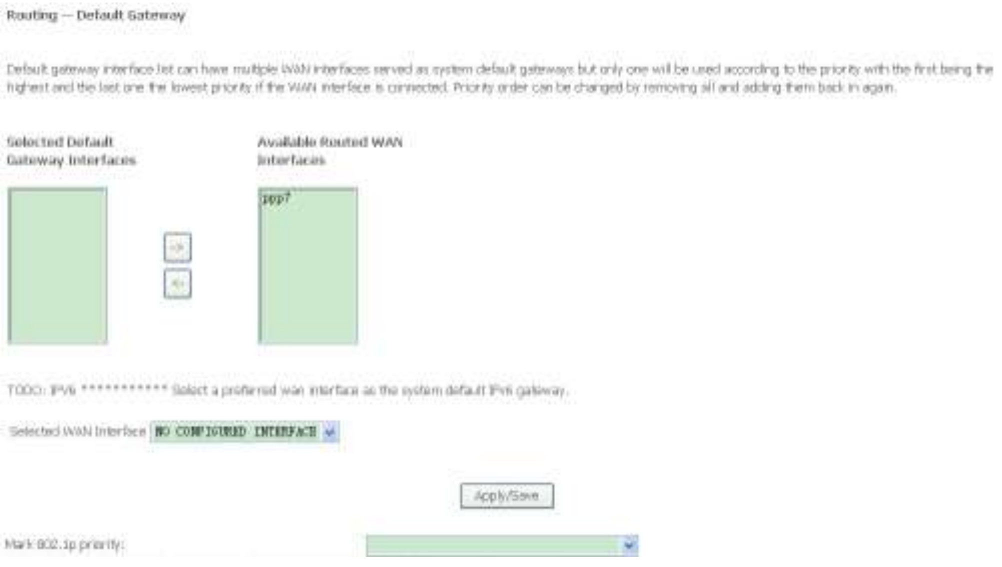
Set Rate Limit: [kbits/s]

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

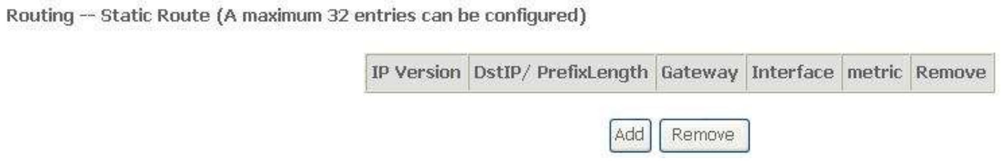
TODO: IPV6 *********** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: NO CONFIGURED 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.

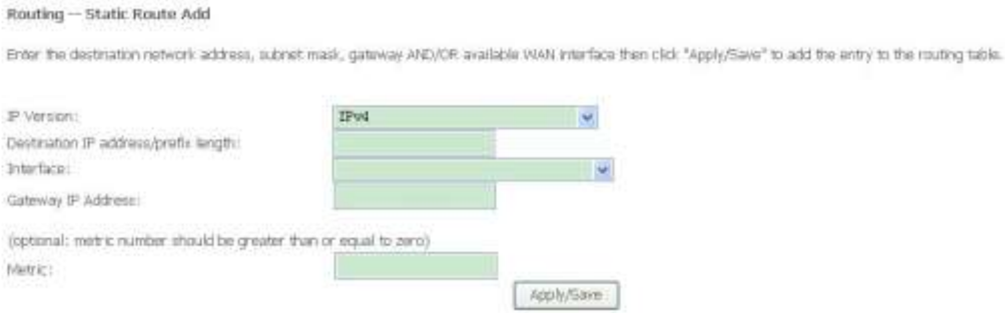


Routing -- Static Route (A maximum 32 entries can be configured)

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: IPv4

Destination IP address/prefix length:

Interface:

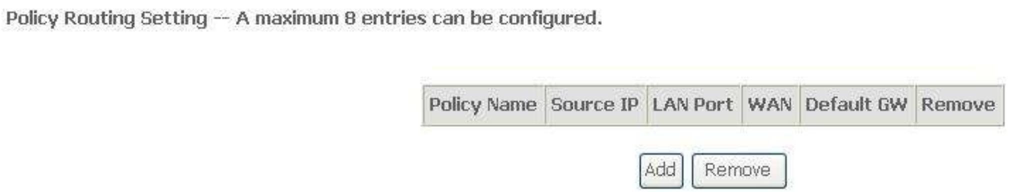
Gateway IP Address:

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

Metric:

Policy Routing

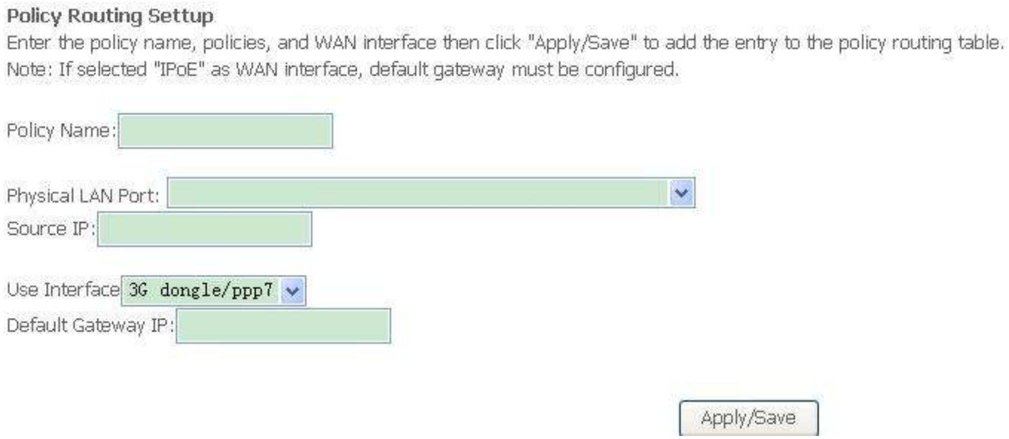
Click the **Add** button on the **Policy Routing Settup** window to access the following window displayed on the next page.



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 Settup

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:

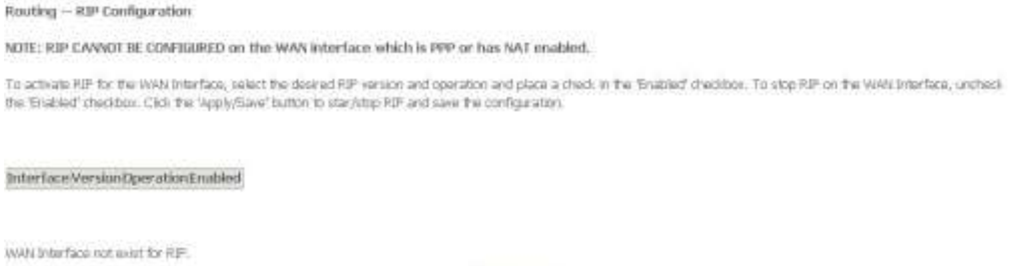
Source IP:

Use Interface 3G dongle/ppp7

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

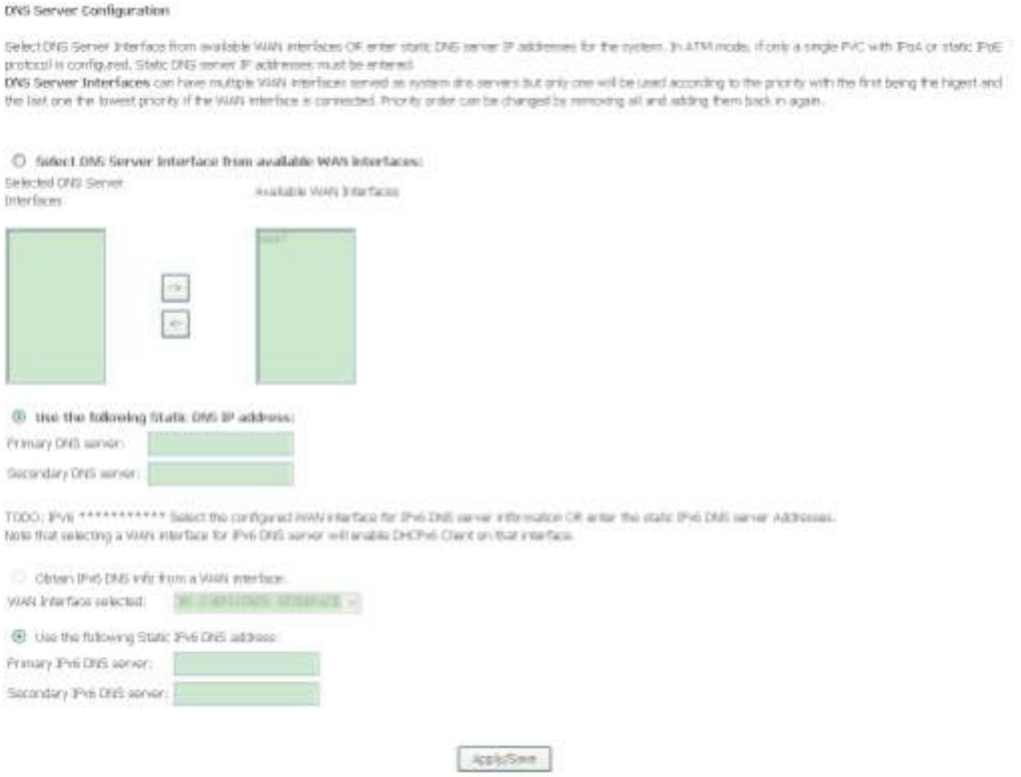
WAN Interface not exist for RIP.

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 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 higest 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 higest 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: [illegible]

● Use the following Static IPv6 DNS address:

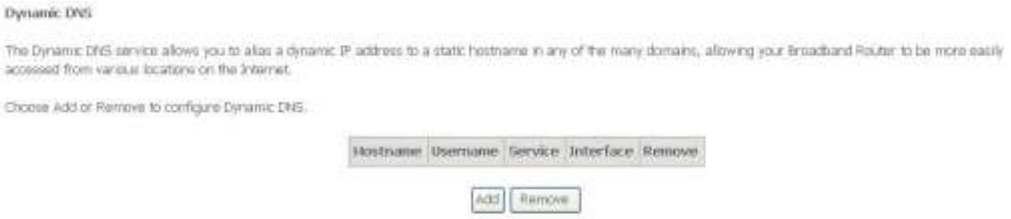
Primary IPv6 DNS server:

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, 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.



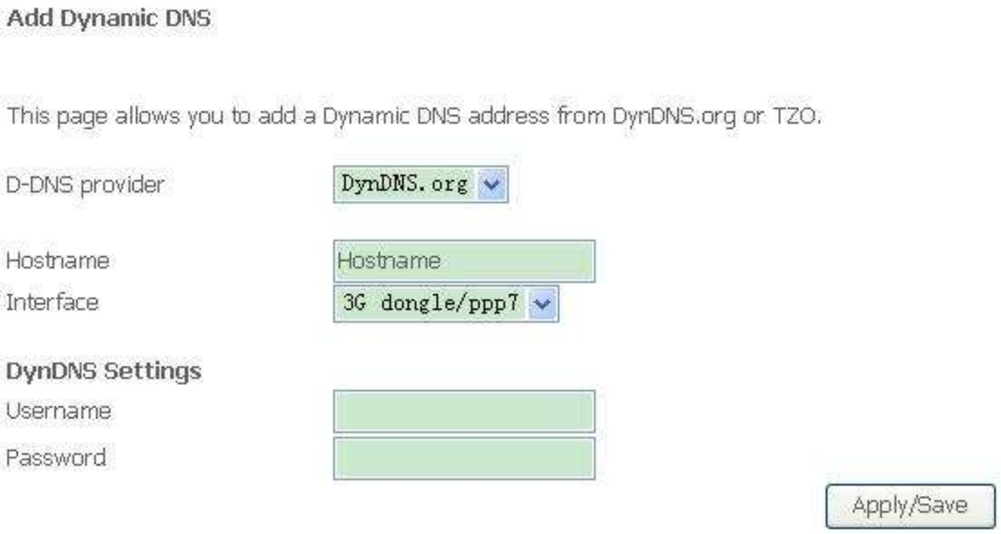
Dynamic DNS

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: DynDNS.org

Hostname: Hostname

Interface: 3G dongle/ppp7

DynDNS Settings

Username:

Password:

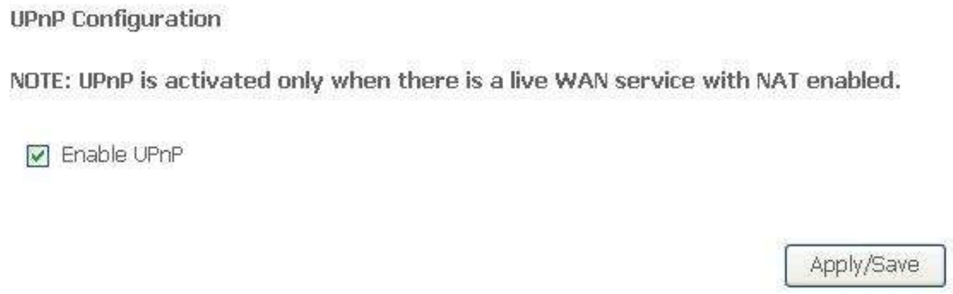
Note

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.

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

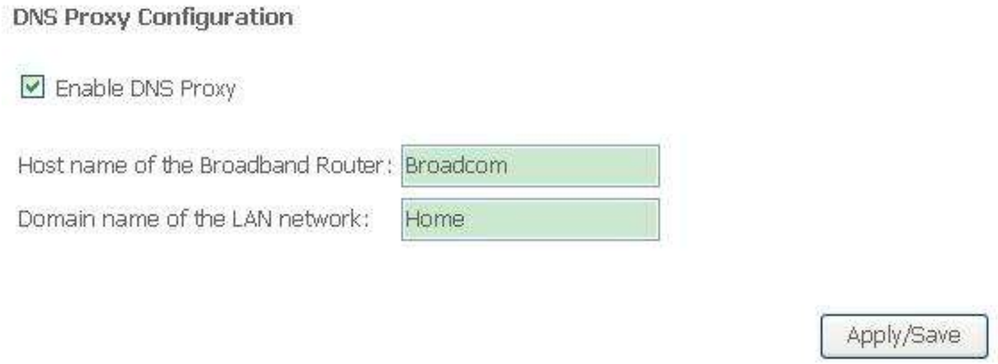
NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☑ 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: Broadcom

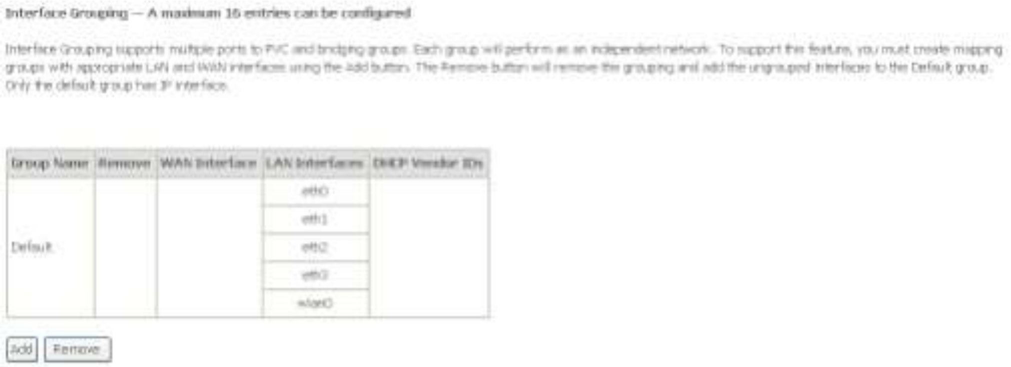
Domain name of the LAN network: Home

Interface Group

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.



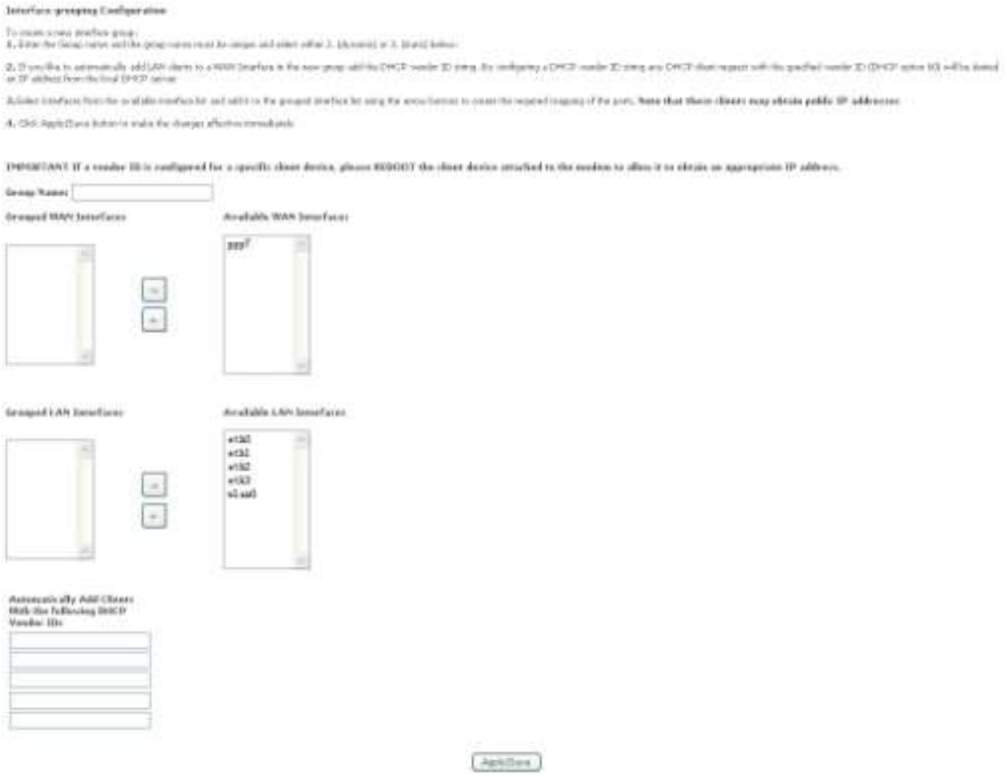
Interface Grouping -- A maximum 16 entries can be configured

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

ppp0

Grouped LAN Interfaces

Available LAN Interfaces

eth0
eth1
eth2
eth3
wl ssid

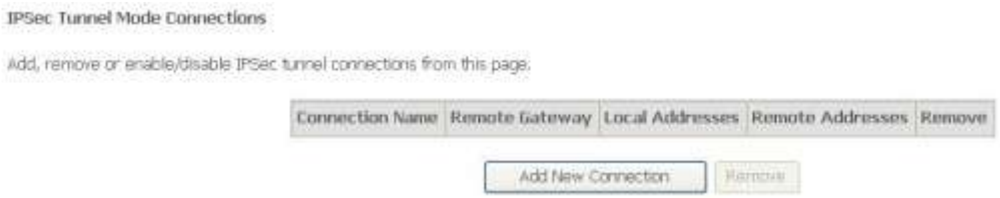
Automatically Add Clients With the following DHCP Vendor IDs

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

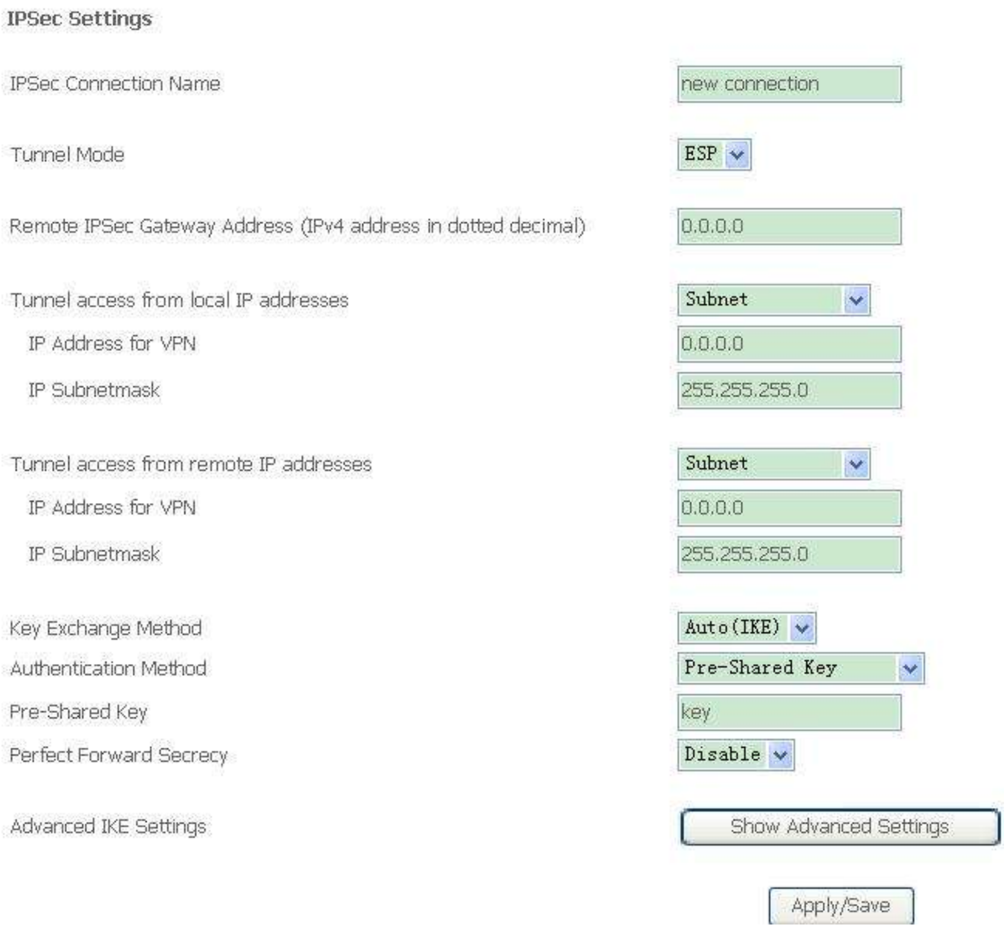


IPSec Tunnel Mode Connections

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

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove

This window allows you to advanced settings.



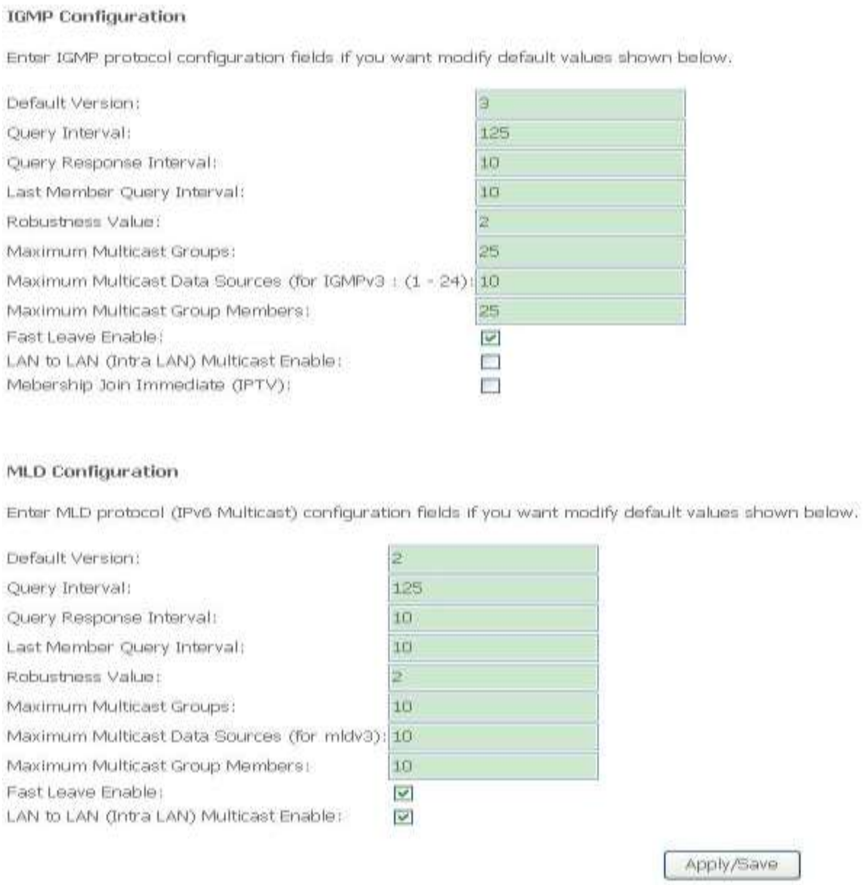
IPSec Settings

IPSec Connection Name	new connection
Tunnel Mode	ESP
Remote IPSec Gateway Address (IPv4 address in dotted decimal)	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings

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:	3
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	□
Mebership Join Immediate (IPTV):	□

MLD Configuration

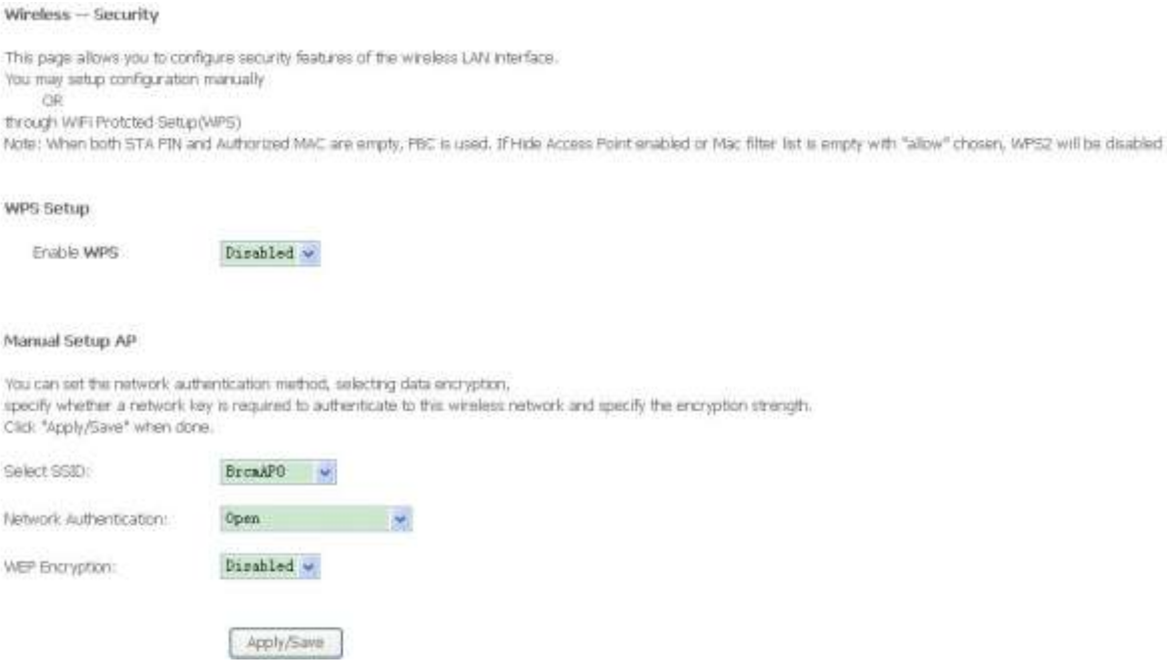
Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	10
Maximum Multicast Data Sources (for mldv3):	10
Maximum Multicast Group Members:	10
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑

Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually or through WiFi Protcted 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 Protcted 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** Disabled

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.

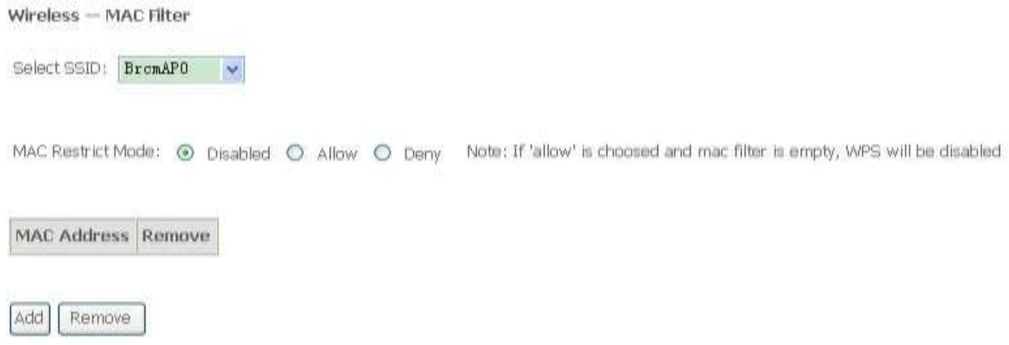
Select SSID: BrcmAP0

Network Authentication: Open

WEP Encryption: Disabled

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.



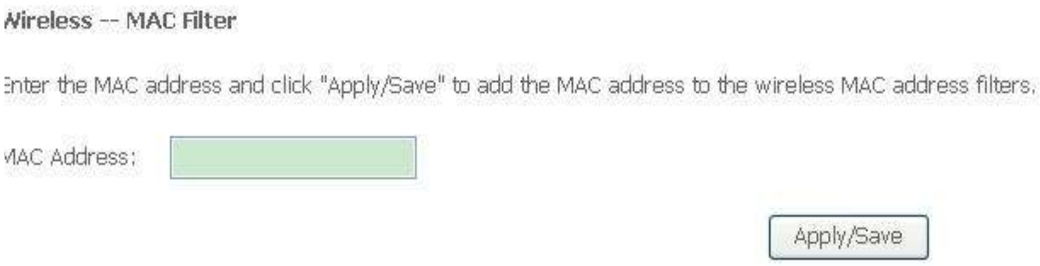
Wireless -- MAC Filter

Select SSID: BrcmAP0

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

MAC Address	Remove

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



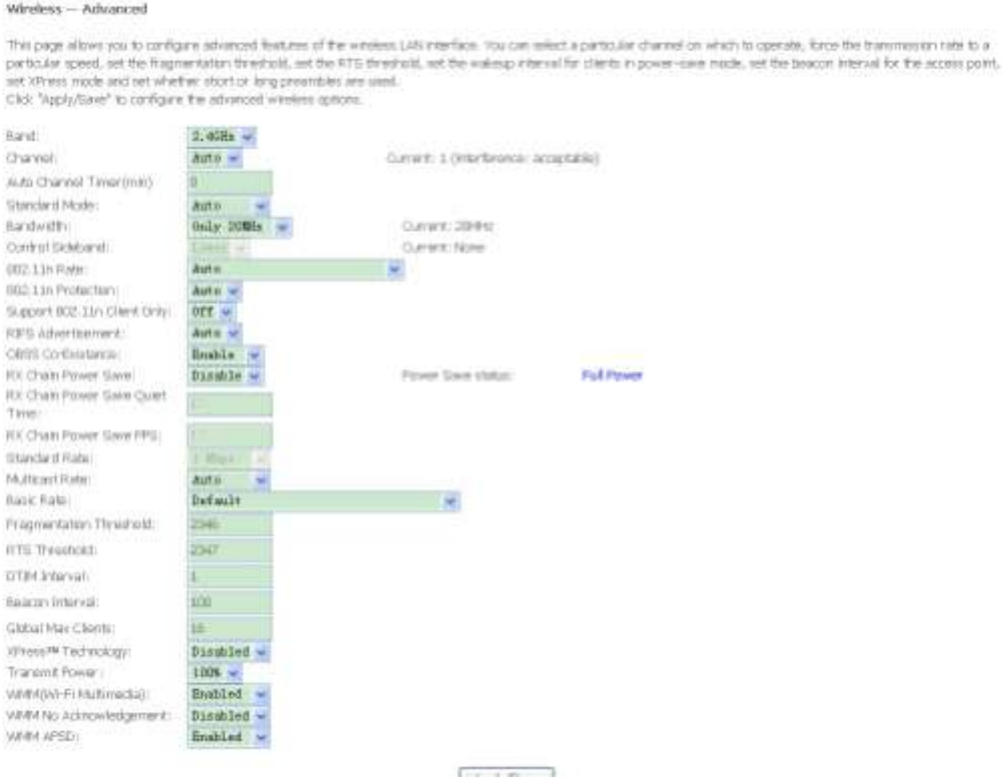
Wireless -- MAC Filter

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

MAC Address:

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.



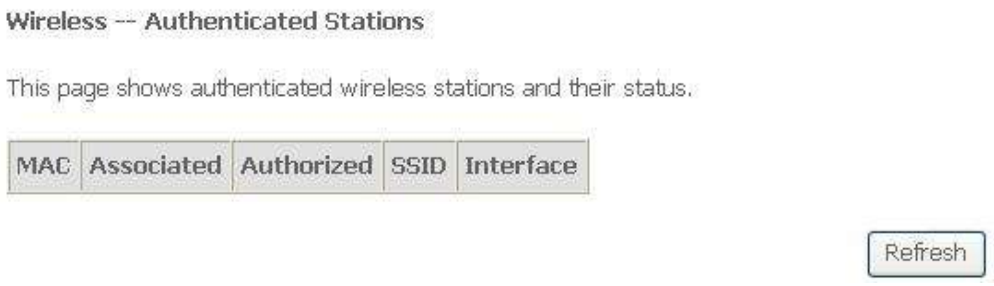
Wireless -- Advanced

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:	2.4GHz	
Channel:	Auto	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	0	
Standard Mode:	Auto	
Bandwidth:	Only 20MHz	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Auto	
OBSS Co-Existance:	Enable	
RX Chain Power Save:	Disable	Power Save status: Full Power
RX Chain Power Save Quiet Time:	[illegible]	
RX Chain Power Save PPS:	[illegible]	
Standard Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Station Info

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



Wireless -- Authenticated Stations

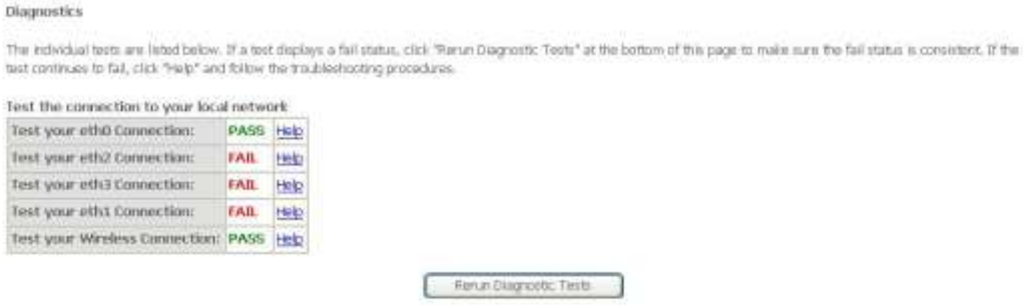
This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

Diagnostics

Your modem is capable of testing your DSL connection with access to **Diagnostics**.

This window is used to test connectivity of the Router.



Diagnostics

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 eth0 Connection:	PASS	Help
Test your eth2 Connection:	FAIL	Help
Test your eth3 Connection:	FAIL	Help
Test your eth1 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Management

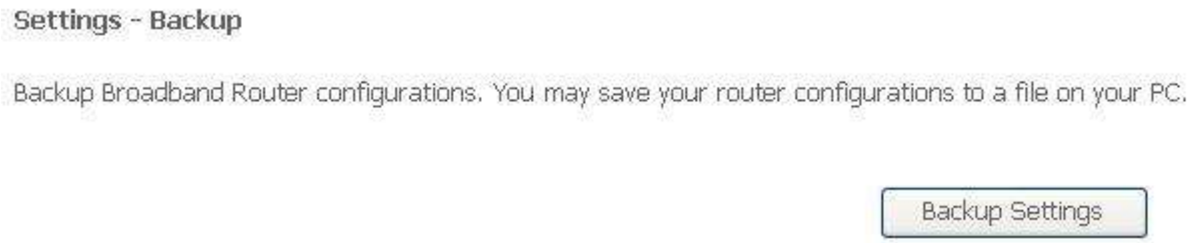
The Management directory features an array of options designed to help you get the most out of your Router.

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.

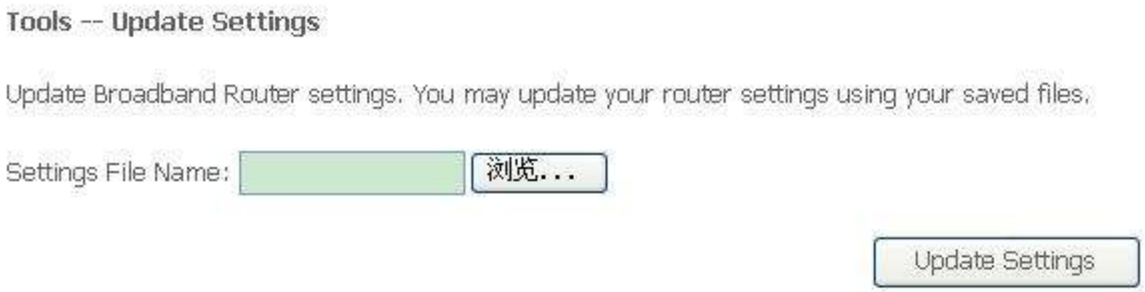


Settings - Backup

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 Settings** button to update your Router configurations with a file on your computer.

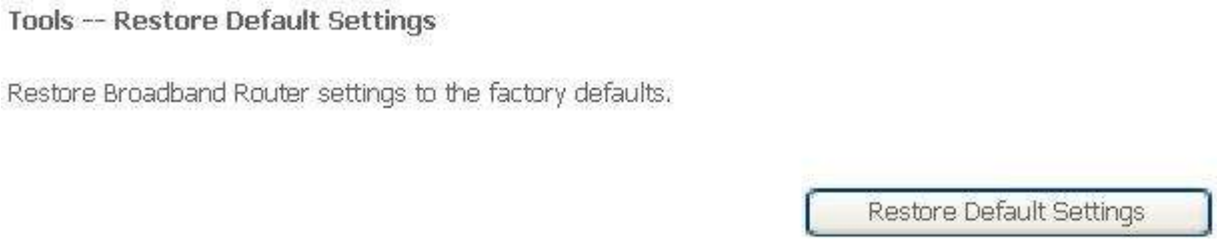


Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

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.

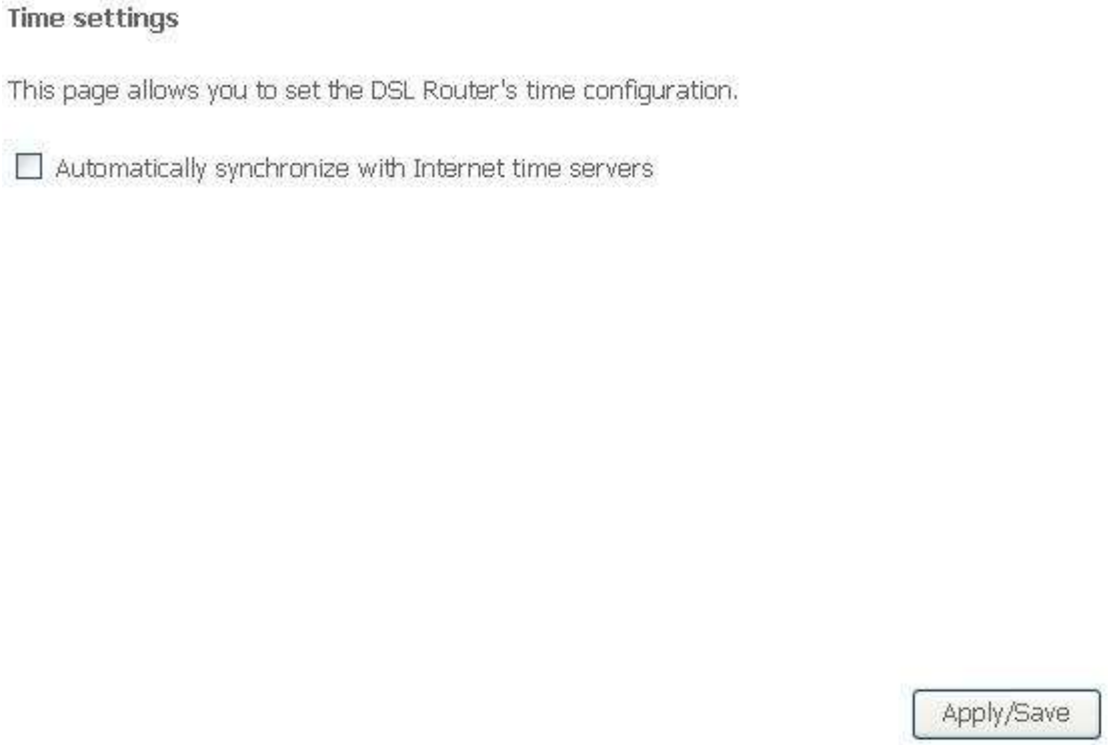


Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

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.

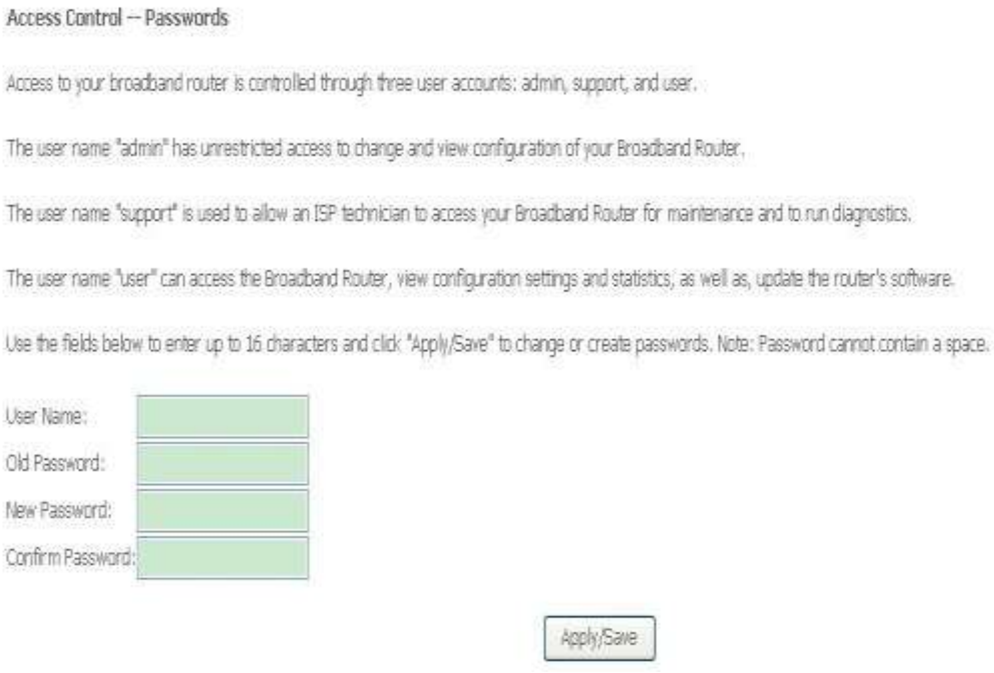
□ Automatically synchronize with Internet time servers

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:

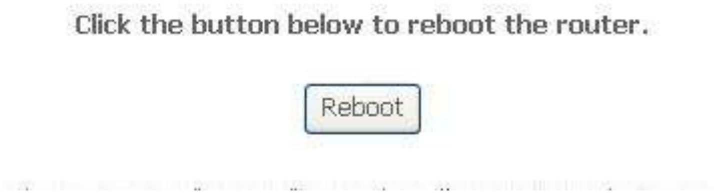
New Password:

Confirm Password:

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.

Troubleshooting

This chapter provides solutions to problems that might occur during the installation and operation of the DSL-STV504. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

1. How do I configure my DSL-STV504 Router without the CD-ROM?

- Connect your PC to the Router using an Ethernet cable.
- Open a web browser and enter the address http://192.168.1.1
- 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:

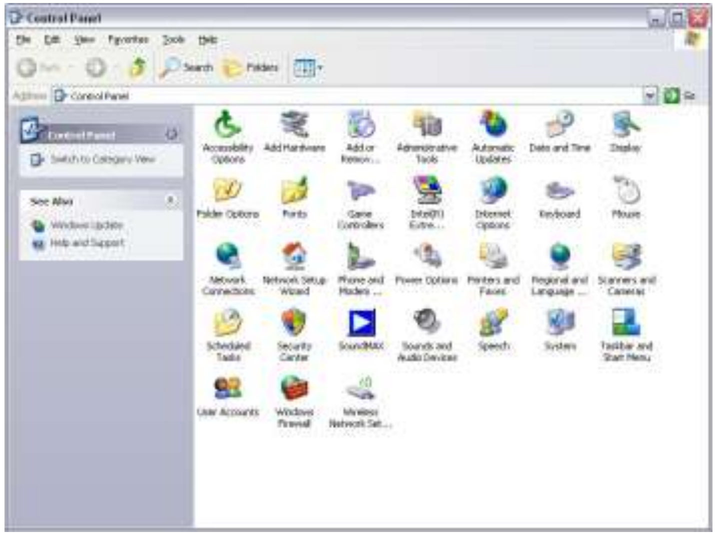
- Follow the directions in Question 2 to reset the Router.
- Check that all the cables are firmly connected at both ends.
- Check the LEDs on the front of the Router. The Power indicator should be on, the Status indicator should flash, and the DSL and LAN indicators should be on as well.
- Please ensure 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.

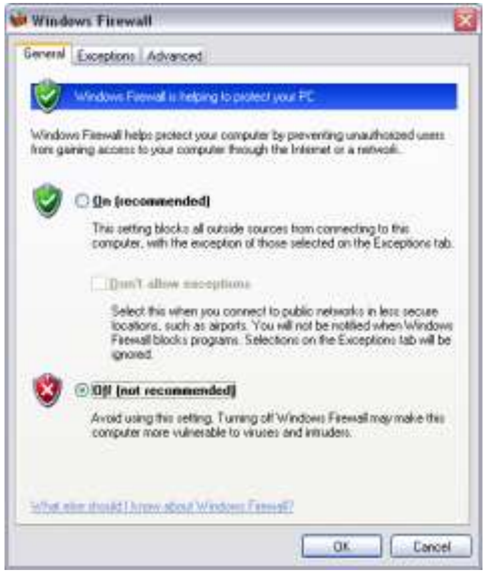
4. Why can’t I get an Internet connection?

For ADSL 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**.




Windows Firewall

General | Exceptions | Advanced

Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

● Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

OK | Cancel

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、

FCC Information

FCC Caution

・ Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

・ This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

・ For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

・ This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter..

This device must not be co-located or operating in conjunction with any other antenna or transmitter

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Federal Communications Commission (FCC) Requirements, Part 15

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

---Reorient or relocate the receiving antenna.
---Increase the separation between the equipment and receiver.
---Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
---Consult the dealer or an experienced radio/TV technician for help.

Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

MPE Statement (Safety Information)

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only.
Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

Safety Information

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

Please use the factory recommended power supply.