Proscend 140

ADSL2+/VDSL2 Router

User Manual

Version 0.01

Table of Contents

Chapter 1 Introduction

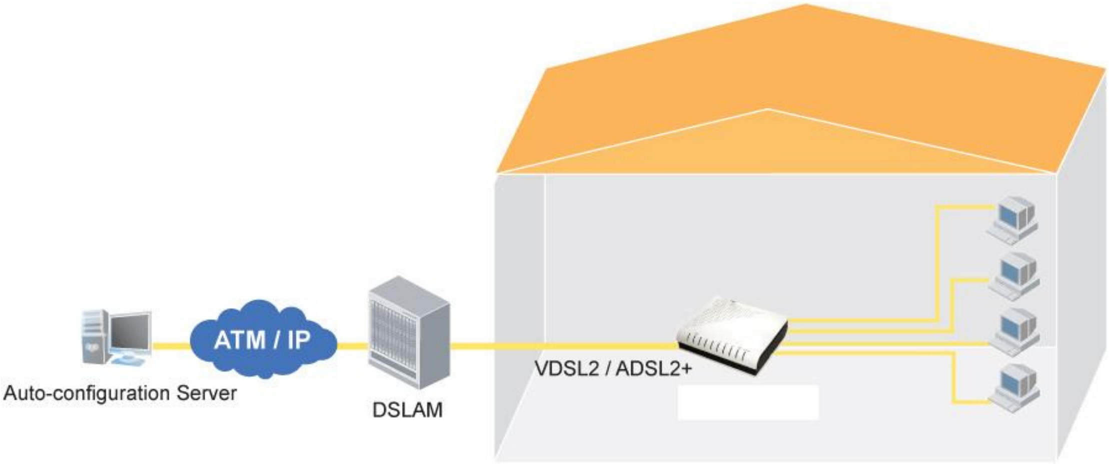
The Proscend 140 is a leading Multi-DSL router that can support both ADSL2+ and VDSL2. VDSL2 is a brand new standard and technology that is perfectly suitable for triple play (Video, Voice and Data) applications. Four 10/100 Base-T Ethernet ports and cost effective solution, designed to meet the needs of ISPs and carriers that intend to use one DSL device to cover end users in different loop range areas. Using only one DSL device creates savings for the TCO of ISP and carrier, while simultaneously providing valuable services without the need for upgrade.

1.1 Features

- Supports both ADSL2+ and VDSL2
- Support up to VDSL2 17a Profile
- UPnP
- IP/MAC address filtering
- Static route & RIP v1/v2 routing
- Dynamic IP assignment
- IP QoS
- NAT/PAT
- IGMP Proxy and fast leave
- DHCP Server/Relay/Client
- DNS Proxy
- Auto PVC configuration
- Per-VC packet level QoS
- Up to 16 VCs
- Embedded SNMP agent
- Web-based management
- RADIUS client
- Supports TR-069/TR-098/TR-111
- Configuration backup and restoration
- FTP/TFTP server
- Automatically switches to ADSL2+ /VDSL2 according to the port setting of DSLAM
- Supports remote administration, automatic firmware upgrade and configuration

1.2 Application

The following diagram depicts a typical application of the Proscend 140.



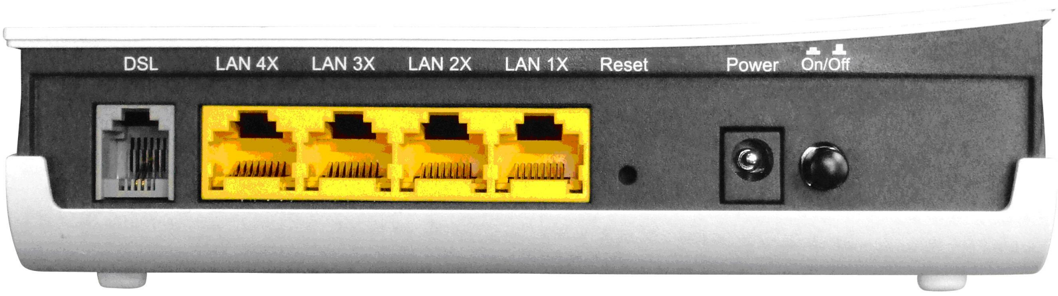
Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

REAR PANEL

The figure below shows the rear panel of the device.



Power ON

Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup.

Caution 1: If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, please contact technical support.

Caution 2: Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

Reset Button

- Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds. After the device has rebooted successfully, the front panel should display as expected.

NOTE: If pressed down for more than 20 seconds, the Proscend 140 will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

Ethernet (LAN) Ports

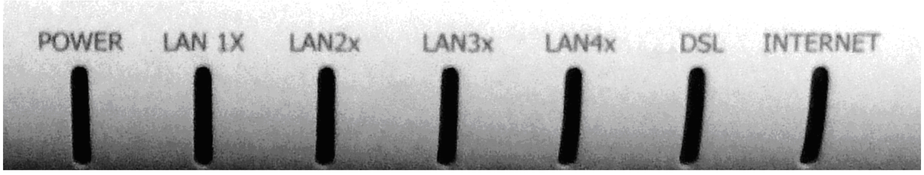
Use 10/100 BASE-T RJ-45 cables to connect up to four network devices. These ports are auto-sensing MDI/MDIX; so either straight-through or crossover cable can be used.

DSL Port

Connect the ADSL2+ or VDSL2 line to this port with a RJ-11 (telephone) cable.

2.2 LED Indicators

The front panel LED indicators are shown below and explained in the following table. This information can be used to check the status of the device and its connections.



LED	Color	Mode	Function
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.
LAN 1X~4X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over LAN.
DSL	Green	On	xDSL Link is established.
		Blink	fast: xDSL Link is training or data transmitting. slow: xDSL Link is not established.
INTERNET	Green	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an xDSL connection is still present.
		Off	Modem power off, modem in bridged mode or xDSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off.
		Blink	IP connected and IP Traffic is passing thru the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

3.1 Default Settings

The factory default settings of this device are summarized below.

- **LAN IP address: 192.168.1.1**
- **LAN subnet mask: 255.255.255.0**
- **Administrative access (username: root , password: 12345)**
- **User access (username: user, password: user)**
- **Remote (WAN) access (username: support, password: support)**

Technical Note

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

3.2 IP Configuration

DHCP MODE

When the Proscend 140 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

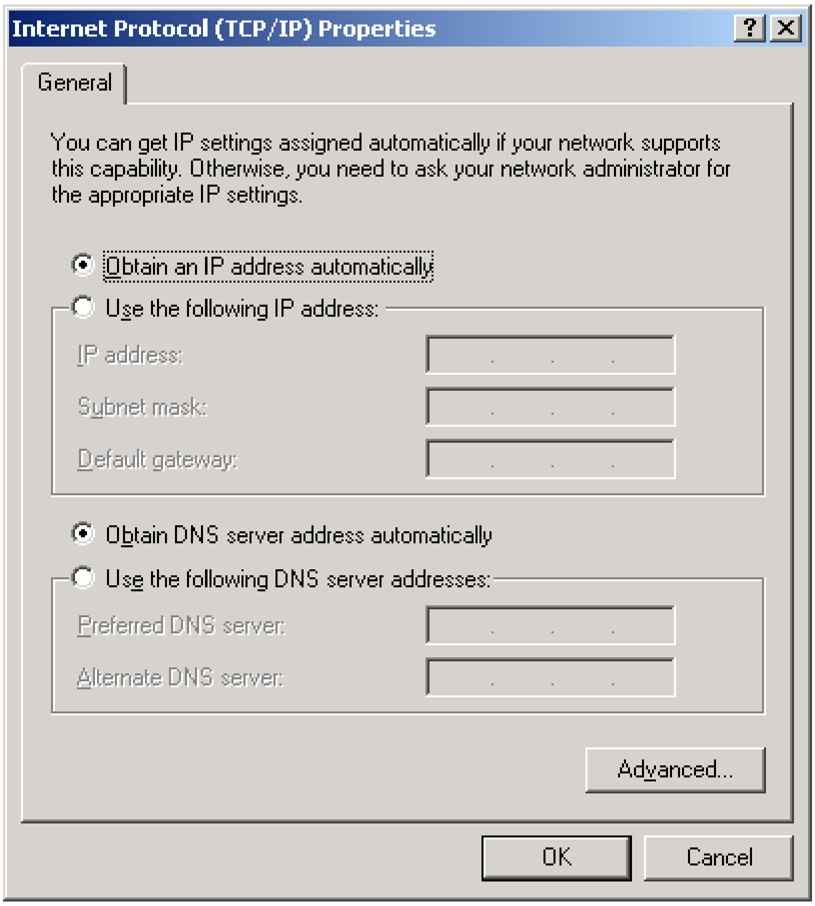
To obtain an IP address from the DCHP server, follow the steps provided below.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Select Obtain an IP address automatically as shown below.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

STEP 4: Click **OK** to submit these settings.

If you experience difficulty with DHCP mode, you can try static IP mode instead.

STATIC IP MODE

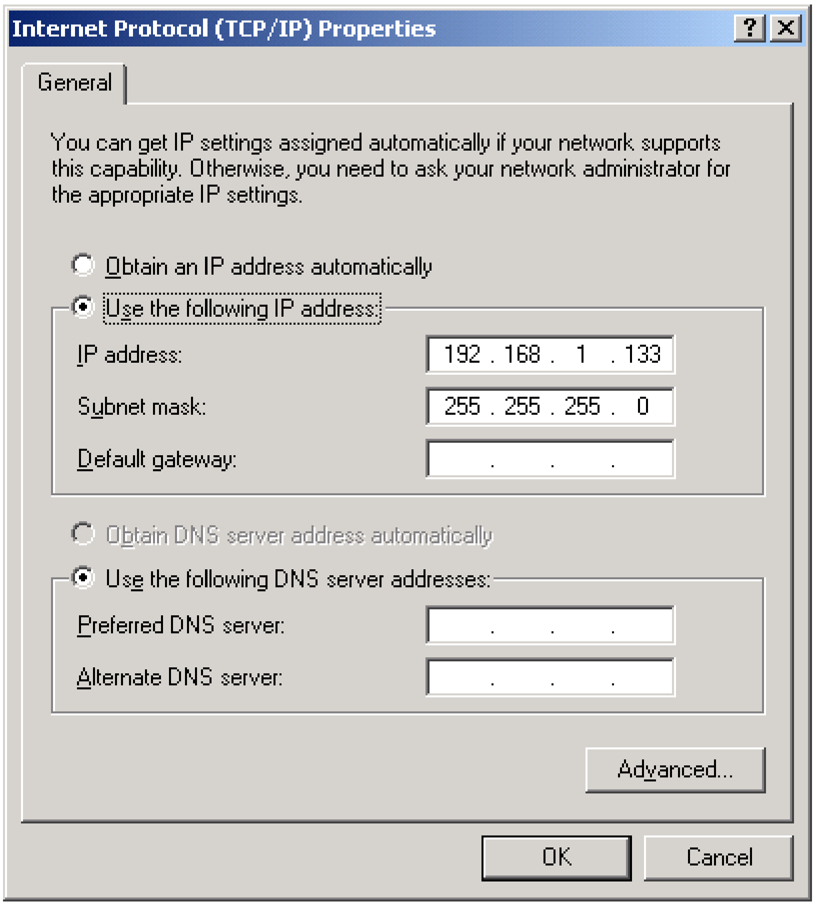
In static IP mode, you assign IP settings to your PC manually.
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 133

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Advanced...

OK Cancel

STEP 4: Click **OK** to submit these settings.

3.3 Login Procedure

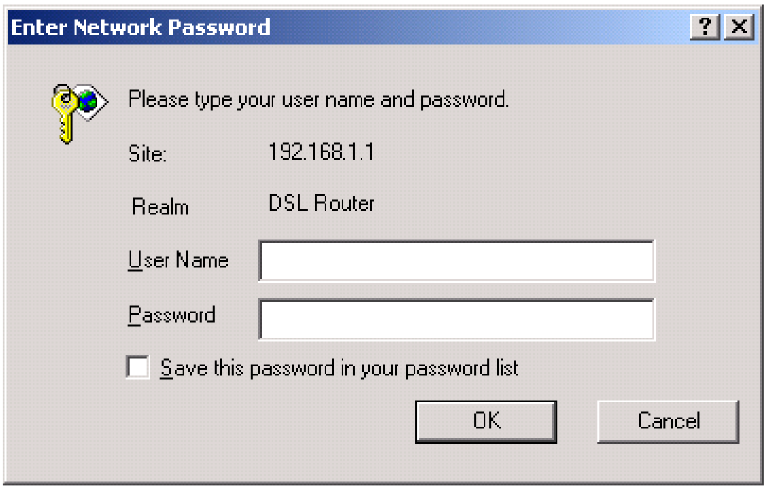
Perform the following steps to login to the web user interface.

NOTE: The default settings can be found in section 3.1.

STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Device Information screen and login with remote username and password.

STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm DSL Router

User Name

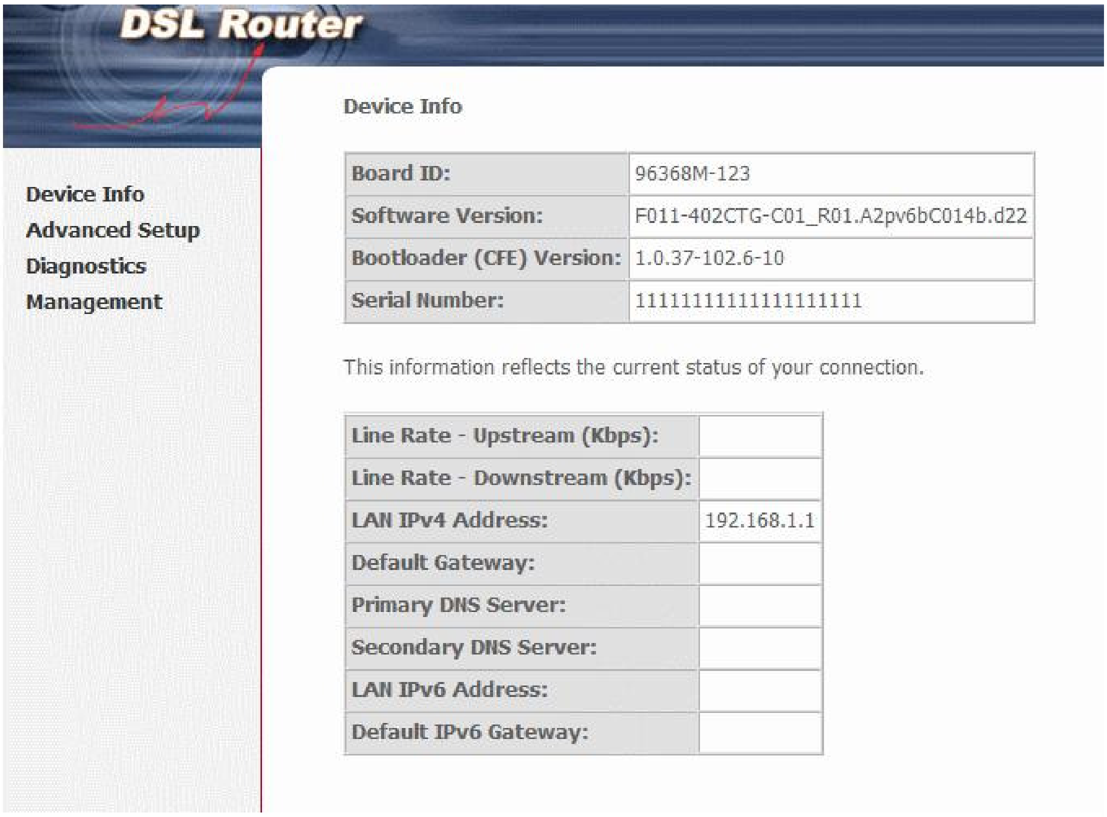
Password

□ Save this password in your password list

Click **OK** to continue.

NOTE: The login password can be changed later (see section 8.5.1).

STEP 3: After successfully logging in for the first time, you will reach this screen.



Device Info

Board ID:	96368M-123
Software Version:	F011-402CTG-C01_R01.A2pv6bC014b.d22
Bootloader (CFE) Version:	1.0.37-102.6-10
Serial Number:	1111111111111111111

This information reflects the current status of your connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	
Secondary DNS Server:	
LAN IPv6 Address:	
Default IPv6 Gateway:	

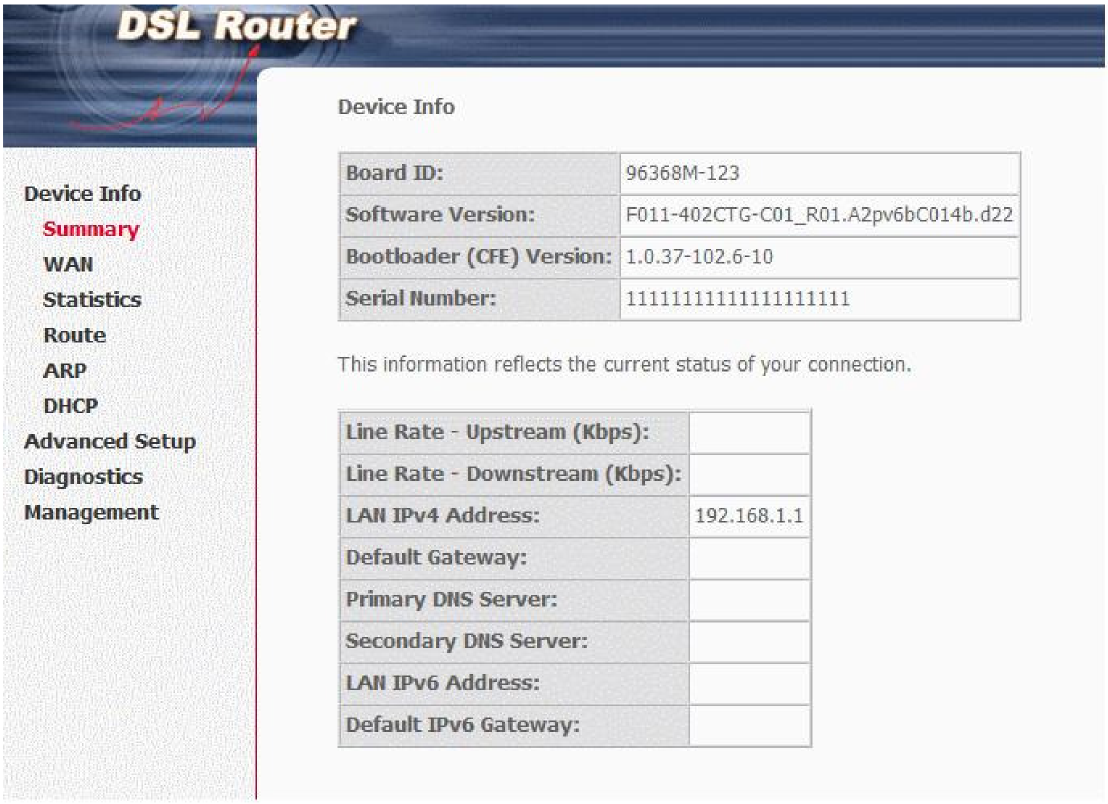
Chapter 4 Device Information

The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

NOTE:	The menu items shown are based upon the configured connection(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

The Device Info Summary screen displays at startup.



Device Info

Board ID:	96368M-123
Software Version:	F011-402CTG-C01_R01.A2pv6bC014b.d22
Bootloader (CFE) Version:	1.0.37-102.6-10
Serial Number:	11111111111111111111

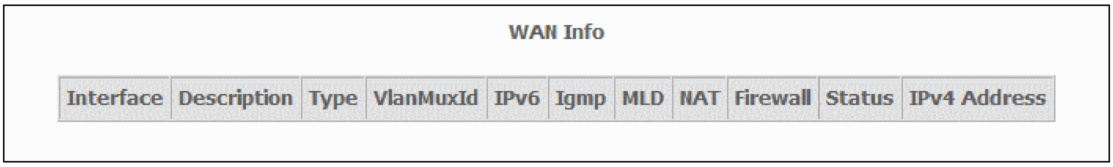
This information reflects the current status of your connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	
Secondary DNS Server:	
LAN IPv6 Address:	
Default IPv6 Gateway:	

This screen shows hardware, software, IP settings and other related information.

Chapter 5 WAN

Select WAN from the Device Info submenu to display any configured connections.



WAN Info

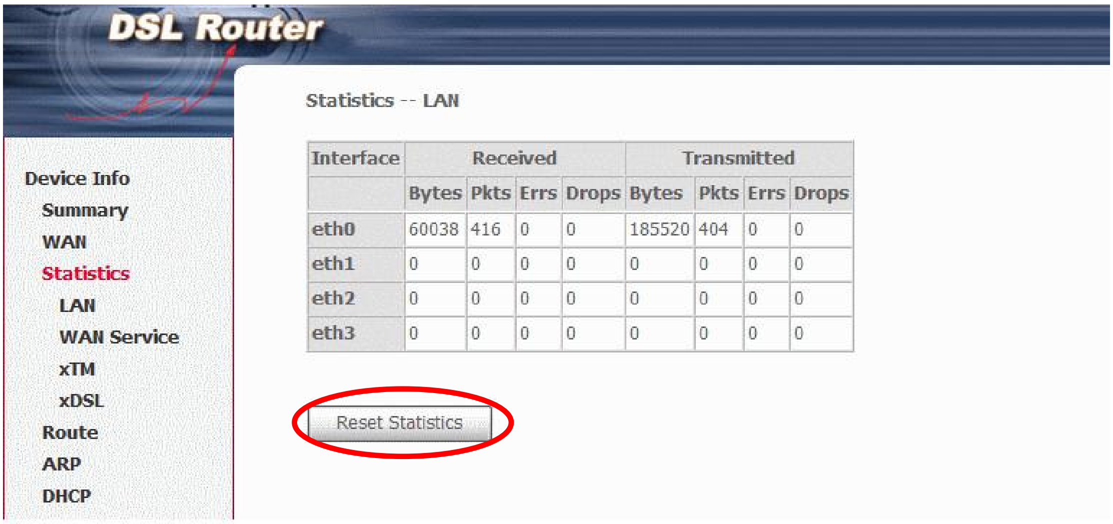
Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
IPv6	Shows WAN IPv6 address
IGMP	Shows Internet Group Management Protocol (IGMP) status
MLD	Shows Multicast Listener Discovery (MLD) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address

5.1 Statistics

This selection provides LAN, WAN, ATM/PTM and xDSL statistics.

NOTE: These screens are updated automatically every 15 seconds. Click **Reset Statistics** to perform a manual update.

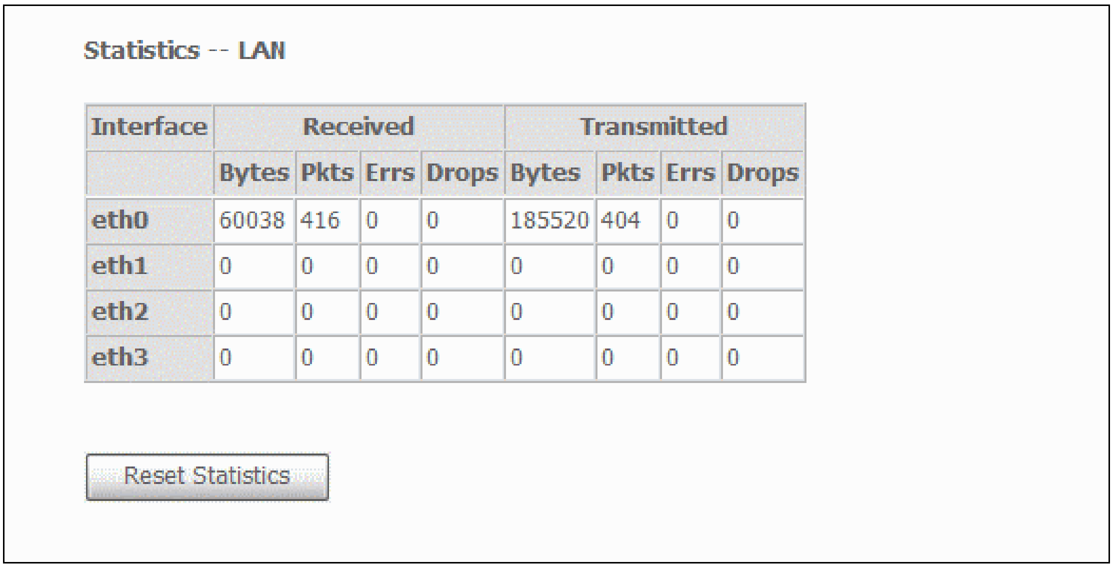


Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	60038	416	0	0	185520	404	0	0
eth1	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0

5.1.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



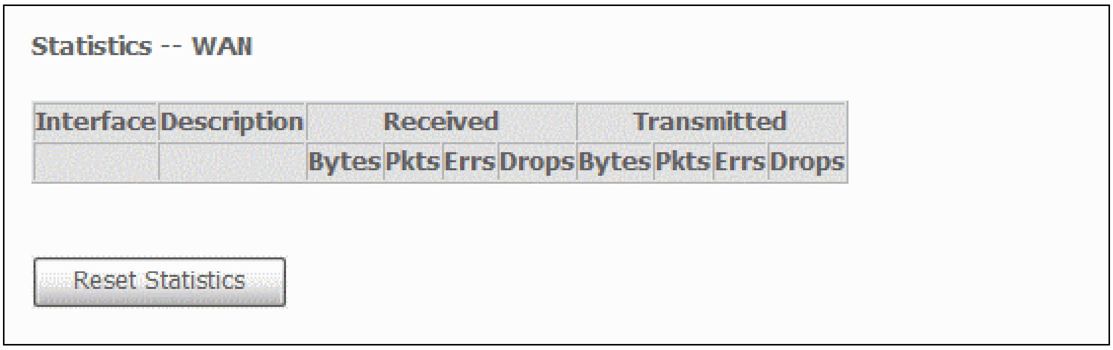
Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	60038	416	0	0	185520	404	0	0
eth1	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0

Heading	Description
Interface	LAN interface(s)
Received/Transmitted: - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

5.1.2 WAN Statistics

This screen shows data traffic statistics for each WAN interface.



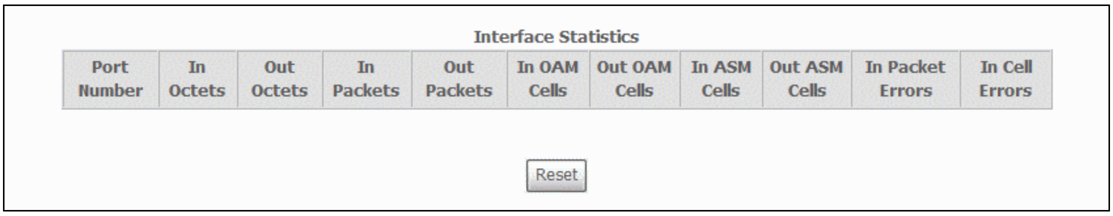
Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

Heading	Description
Interface	WAN interfaces
Description	WAN service label
Received/Transmitted - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

5.1.3 xTM Statistics

The following figure shows ATM/PTM statistics.



Interface Statistics

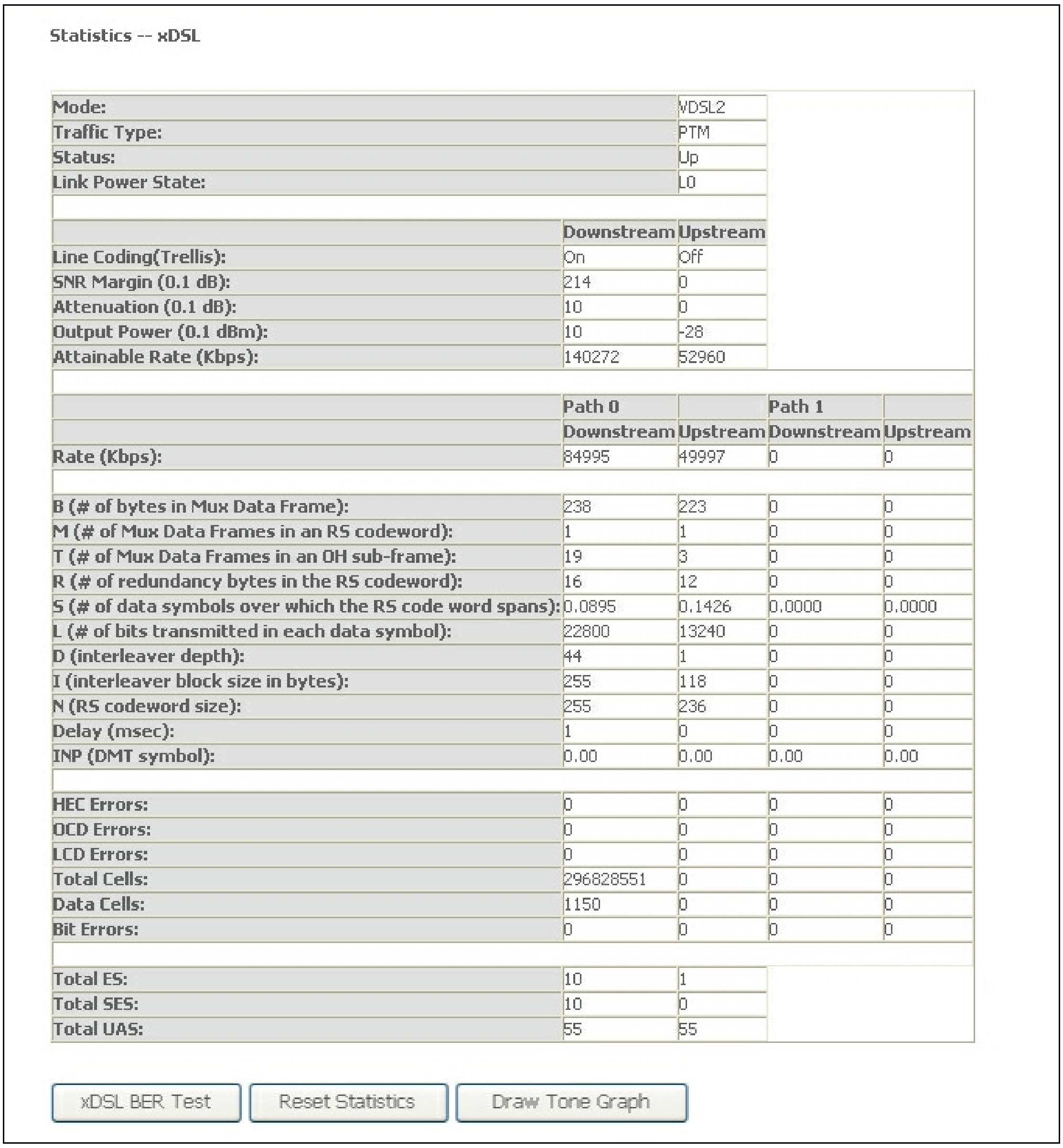
Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors

Heading	Description
Port Number	ATM PORT (0-3)
In Octets	Number of octets received over the interface
Out Octets	Number of octets transmitted over the interface
In Packets	Number of packets received over the interface
Out Packets	Number of packets transmitted over the interface
In OAM Cells	Number of OAM Cells received over the interface
Out OAM Cells	Number of OAM Cells transmitted over the interface
In ASM Cells	Number of ASM Cells received over the interface
Out ASM Cells	Number of ASM Cells transmitted over the interface
In Packet Errors	Number of packets in Error
In Cell Errors	Number of cells in Error.

5.1.4 xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type. The two examples below (VDSL & ADSL2+) show this variation.

VDSL



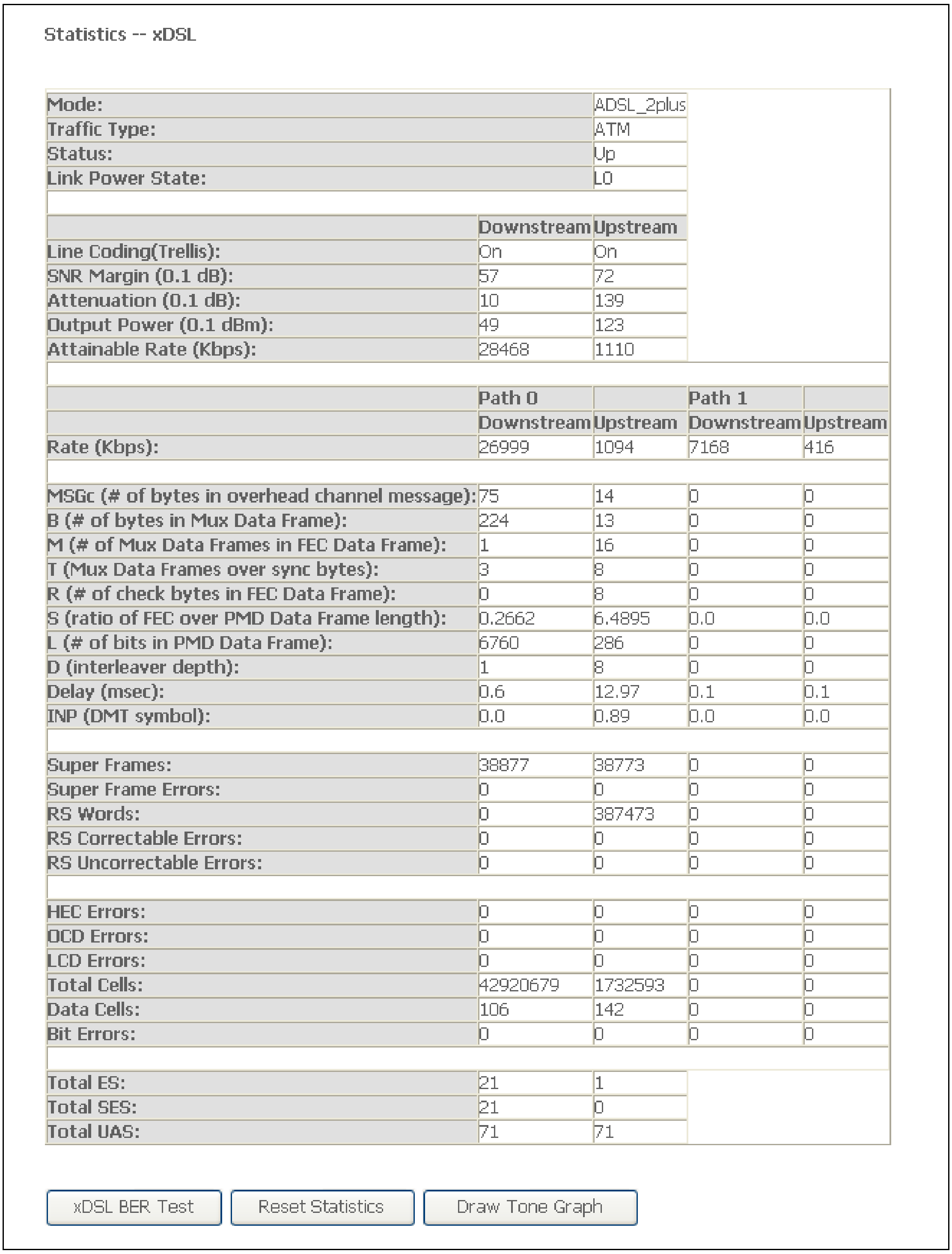
Statistics -- xDSL

Mode:	VDSL2
Traffic Type:	PTM
Status:	Up
Link Power State:	L0

	Downstream	Upstream
Line Coding(Trellis):	On	Off
SNR Margin (0.1 dB):	214	0
Attenuation (0.1 dB):	10	0
Output Power (0.1 dBm):	10	-28
Attainable Rate (Kbps):	140272	52960

	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	84995	49997	0	0
B (# of bytes in Mux Data Frame):	238	223	0	0
M (# of Mux Data Frames in an RS codeword):	1	1	0	0
T (# of Mux Data Frames in an OH sub-frame):	19	3	0	0
R (# of redundancy bytes in the RS codeword):	16	12	0	0
S (# of data symbols over which the RS code word spans):	0.0895	0.1426	0.0000	0.0000
L (# of bits transmitted in each data symbol):	22800	13240	0	0
D (interleaver depth):	44	1	0	0
I (interleaver block size in bytes):	255	118	0	0
N (RS codeword size):	255	236	0	0
Delay (msec):	1	0	0	0
INP (DMT symbol):	0.00	0.00	0.00	0.00
HEC Errors:	0	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	296828551	0	0	0
Data Cells:	1150	0	0	0
Bit Errors:	0	0	0	0
Total ES:	10	1		
Total SES:	10	0		
Total UAS:	55	55		

ADSL



Statistics -- xDSL

Mode:		ADSL_2plus		
Traffic Type:		ATM		
Status:		Up		
Link Power State:		L0		
	Downstream	Upstream		
Line Coding(Trellis):	On	On		
SNR Margin (0.1 dB):	57	72		
Attenuation (0.1 dB):	10	139		
Output Power (0.1 dBm):	49	123		
Attainable Rate (Kbps):	28468	1110		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	26999	1094	7168	416
MSGc (# of bytes in overhead channel message):	75	14	0	0
B (# of bytes in Mux Data Frame):	224	13	0	0
M (# of Mux Data Frames in FEC Data Frame):	1	16	0	0
T (Mux Data Frames over sync bytes):	3	8	0	0
R (# of check bytes in FEC Data Frame):	0	8	0	0
S (ratio of FEC over PMD Data Frame length):	0.2662	6.4895	0.0	0.0
L (# of bits in PMD Data Frame):	6760	286	0	0
D (interleaver depth):	1	8	0	0
Delay (msec):	0.6	12.97	0.1	0.1
INP (DMT symbol):	0.0	0.89	0.0	0.0
Super Frames:	38877	38773	0	0
Super Frame Errors:	0	0	0	0
RS Words:	0	387473	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	0	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	42920679	1732593	0	0
Data Cells:	106	142	0	0
Bit Errors:	0	0	0	0
Total ES:	21	1		
Total SES:	21	0		
Total UAS:	71	71		

Click the **Reset Statistics** button to refresh this screen.

Field	**Description**
Mode	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+
Traffic Type	Channel type Interleave or Fast
Status	Lists the status of the DSL link

Field	Description
Link Power State	Link output power state.

Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin
Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rates downstream/upstream

In VDSL mode, the following section is inserted.

B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in a RS codeword
T	Number of Mux Data Frames in an OH sub-frame
R	Number of redundancy bytes in the RS codeword
S	Number of data symbols the RS codeword spans
L	Number of bits transmitted in each data symbol
D	The interleaver depth
I	The interleaver block size in bytes
N	RS codeword size
Delay	The delay in milliseconds (msec)
INP	DMT symbol

In ADSL2+ mode, the following section is inserted.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Mux Data Frames over sync bytes

R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)
INP	DMT symbol

In G.DMT mode, the following section is inserted.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

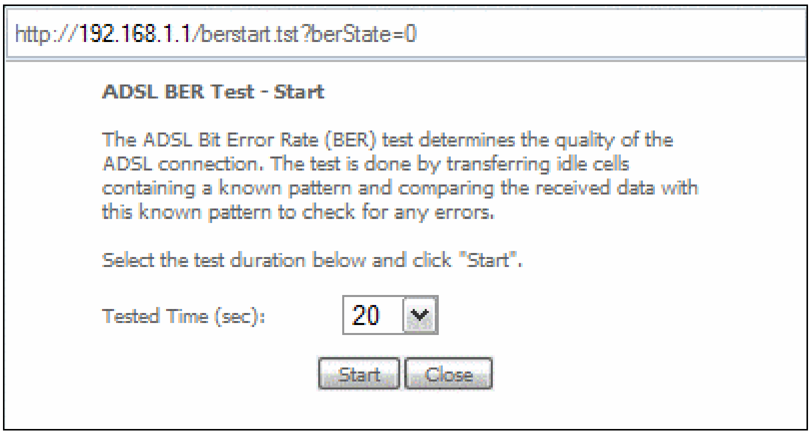
Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of Out-of-Cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

xDSL BER TEST

Click **xDSL BER Test** on the xDSL Statistics screen to test the Bit Error Rate (BER). A small pop-up window will open after the button is pressed, as shown below.



http://192.168.1.1/berstart.tst?berState=0

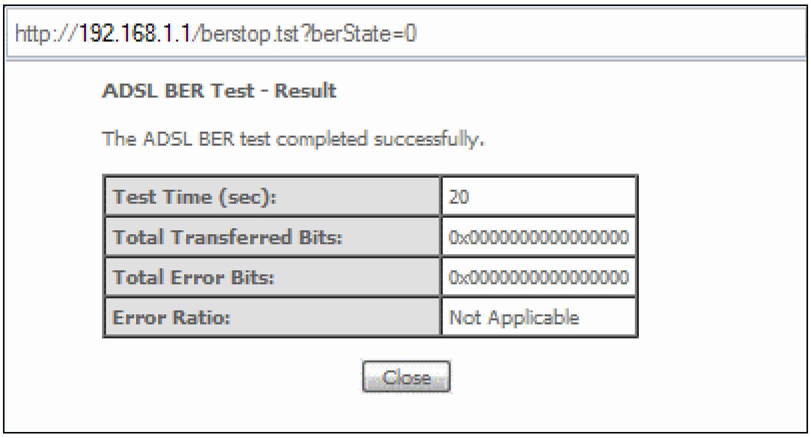
ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): 20

Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



http://192.168.1.1/berstop.tst?berState=0

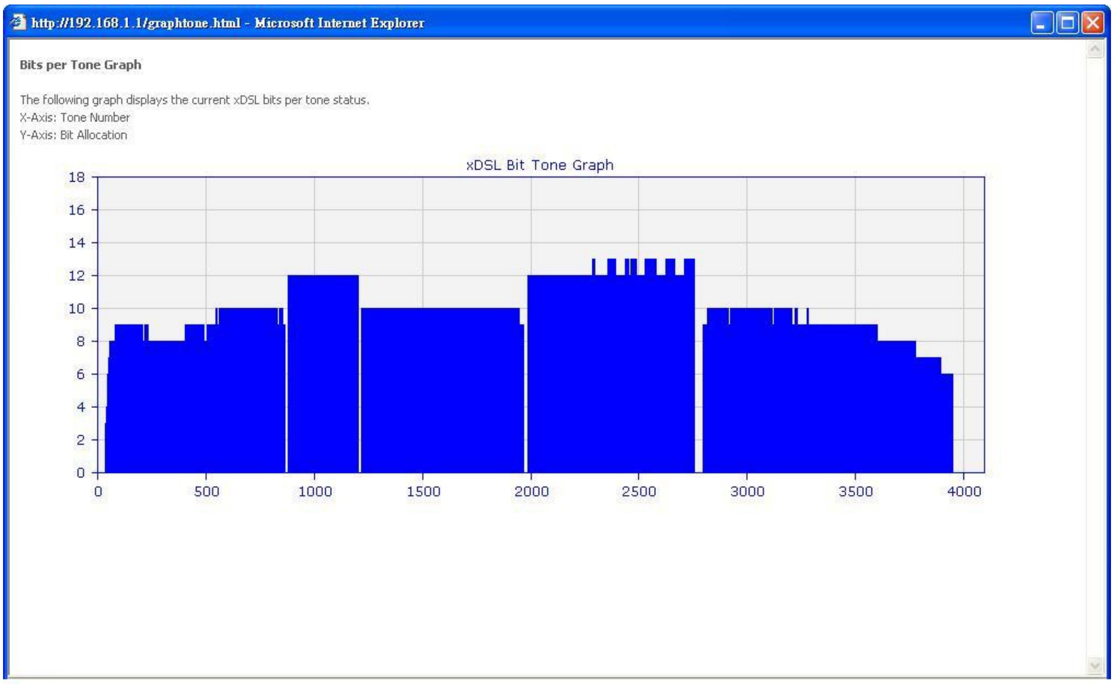
ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x0000000000000000
Total Error Bits:	0x0000000000000000
Error Ratio:	Not Applicable

xDSL TONE GRAPH

Click **Draw Tone Graph** on the xDSL Statistics screen and a pop-up window will display the xDSL bits per tone status, as shown below.



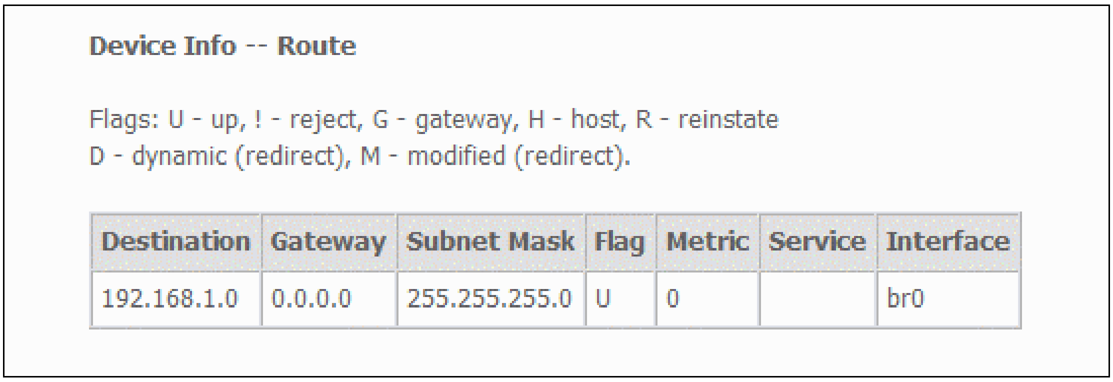
http://192.168.1.1/graphtone.html - Microsoft Internet Explorer

Bits per Tone Graph

The following graph displays the current xDSL bits per tone status.
X-Axis: Tone Number
Y-Axis: Bit Allocation

5.2 Route

Choose **Route** to display the routes that the Proscend 140 has found.



Device Info -- Route

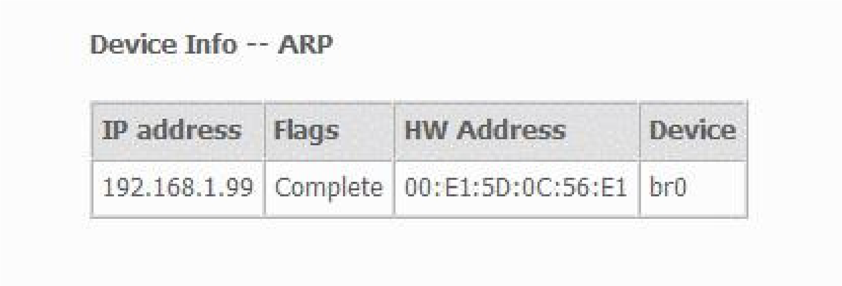
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Field	Description
Destination	Destination network or destination host
Gateway	Next hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

5.3 ARP

Click **ARP** to display the ARP information.



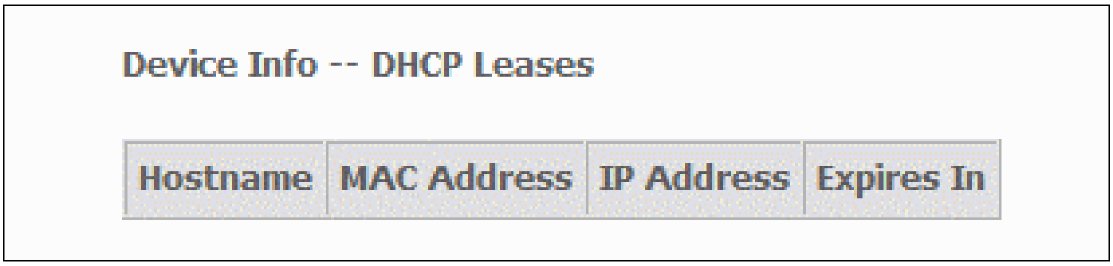
Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.99	Complete	00:E1:5D:0C:56:E1	br0

Field	Description
IP address	Shows IP address of host pc
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

5.4 DHCP

Click **DHCP** to display all DHCP Leases.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

Chapter 6 Advanced Setup

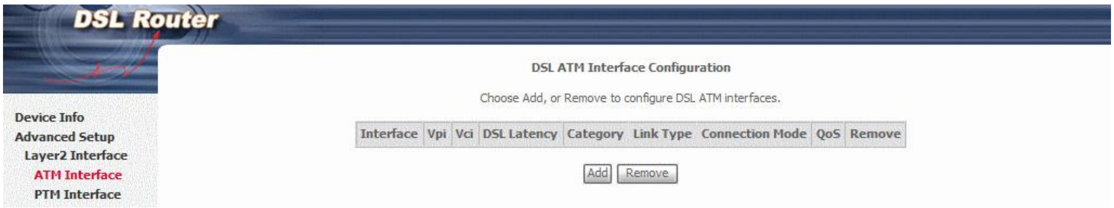
This chapter explains the following screens:

6.1 Layer 2 Interface

The ATM and PTM interface screens are described here.

6.1.1 ATM Interface

Add or remove ATM interface connections here.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove

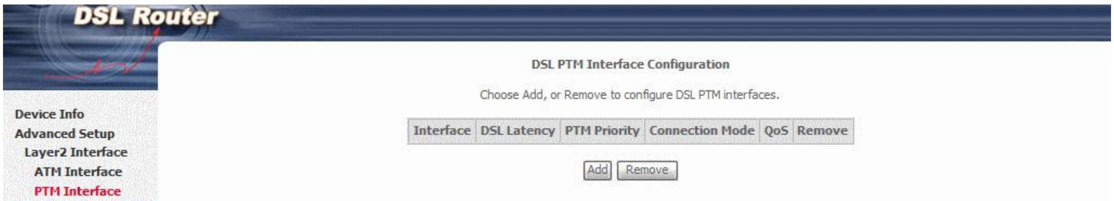
Click **Add** to create a new ATM interface (see Appendix E).

NOTE: Up to 8 ATM interfaces can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click **Remove**.

6.1.2 PTM Interface

Add or remove PTM interface connections here.



DSL PTM Interface Configuration

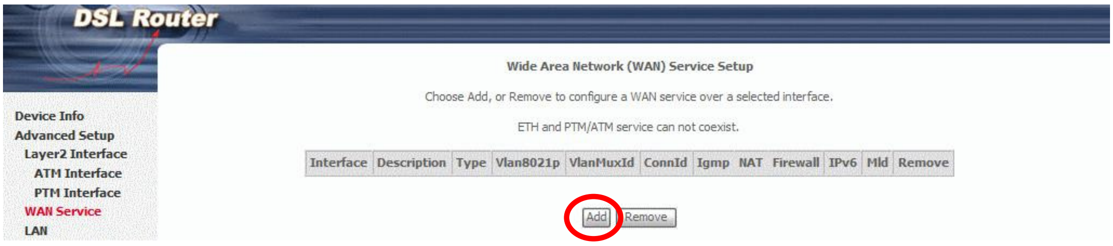
Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Connection Mode	QoS	Remove

Click **Add** to create a new connection (see Appendix E). To remove a connection, select its Remove column radio button and click **Remove**.

6.2 WAN

This screen allows for the configuration of WAN interfaces.



Wide Area Network (WAN) Service Setup

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

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Mld	Remove

Click the **Add** button to create a new connection (see Appendix E for details).

NOTE: In Default Mode, up to 8 WAN connections can be configured; while VLAN Mux and MSC Connection Modes support up to 16 WAN connections.

To remove a connection, select its Remove column radio button and click **Remove.**

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
ConnId	Connection ID
IGMP	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows the WAN IPv6 address
MLD	Shows Multicast Listener Discovery (MLD) status
Remove	Select interfaces to remove

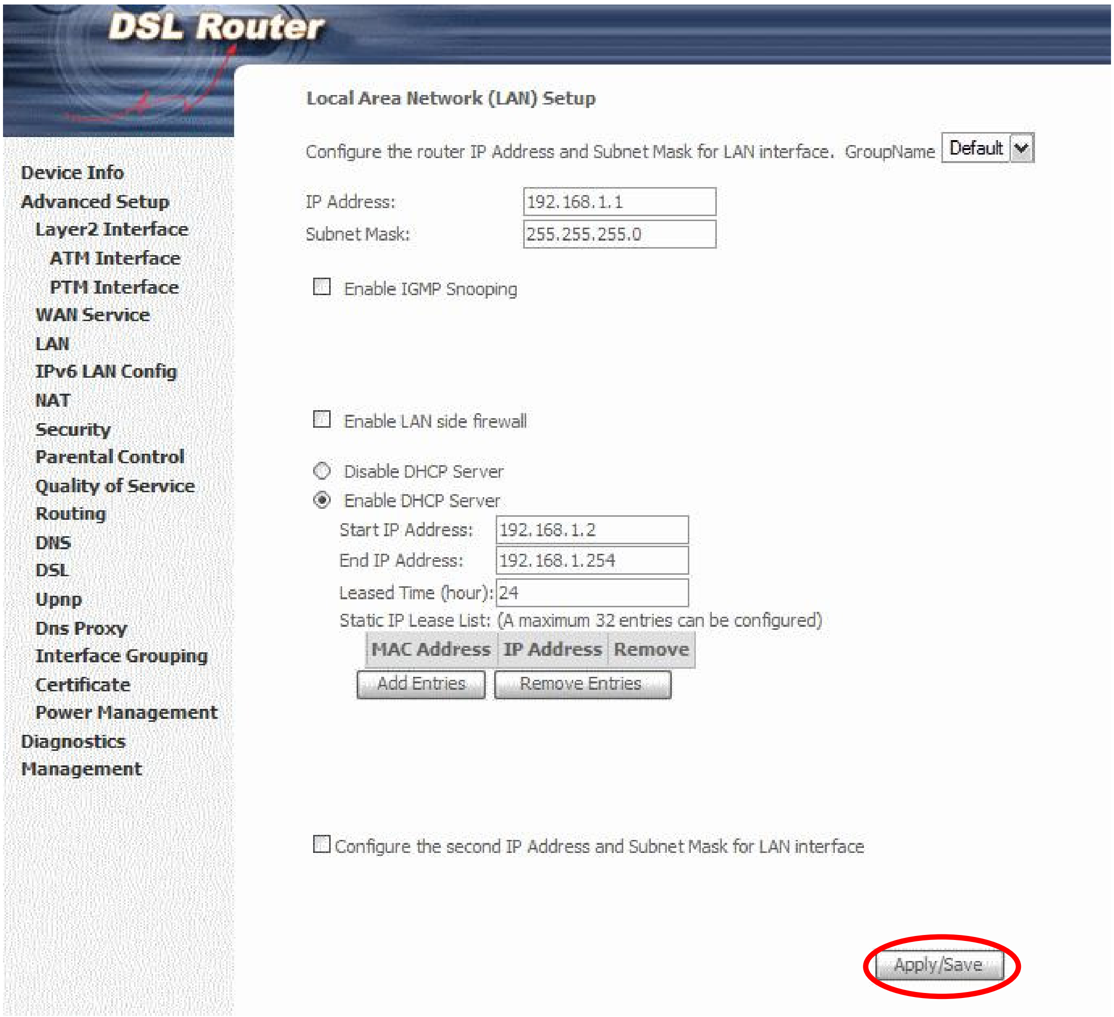
To remove a connection, select its Remove column radio button and click **Remove.**

To **Add** a new WAN connection, click the **Add** button and follow the instructions.

NOTE: Up to 16 PVC profiles can be configured and saved in flash memory.

6.3 LAN

Configure the LAN interface settings and then click **Apply/Save**.



Local Area Network (LAN) Setup

Configure the 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

□ 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): 24

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

MAC Address	IP Address	Remove

□ Configure the second IP Address and Subnet Mask for LAN interface

Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable IGMP Snooping: Enable by ticking the checkbox ☑.

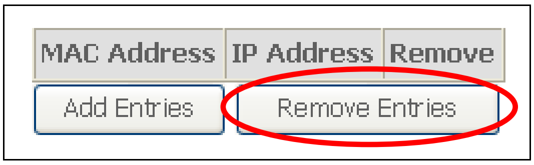
Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

Enable LAN side firewall: Enable by ticking the checkbox ☑.

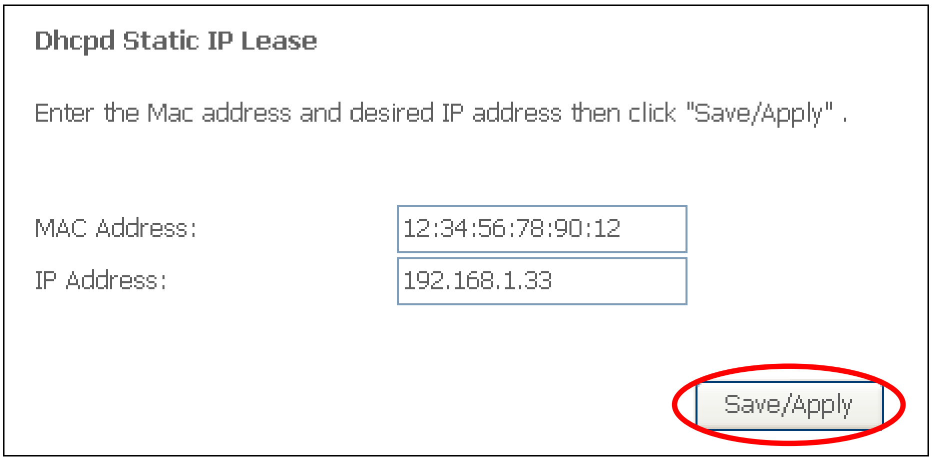
DHCP Server: To enable DHCP, select **Enable DHCP server** and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

Static IP Lease List: A maximum of 32 entries can be configured.



MAC Address	IP Address	Remove

To add an entry, enter MAC address and Static IP and then click **Save/Apply**.



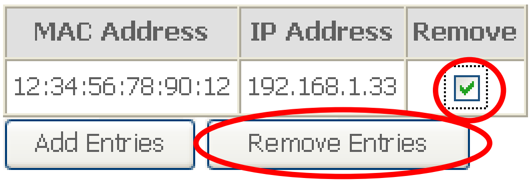
Dhcpd Static IP Lease

Enter the Mac address and desired IP address then click "Save/Apply" .

MAC Address: 12:34:56:78:90:12

IP Address: 192.168.1.33

To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.

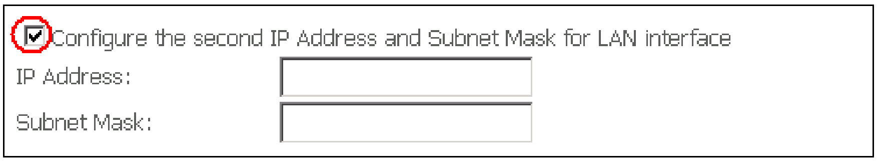


MAC Address	IP Address	Remove
12:34:56:78:90:12	192.168.1.33	☑

DHCP Server Relay: Enable with checkbox ☑ and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. *This option is hidden if NAT is enabled or when the router is configured with only one Bridge PVC.*

2ND LAN INTERFACE

To configure a secondary IP address, tick the checkbox ☑ .



☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

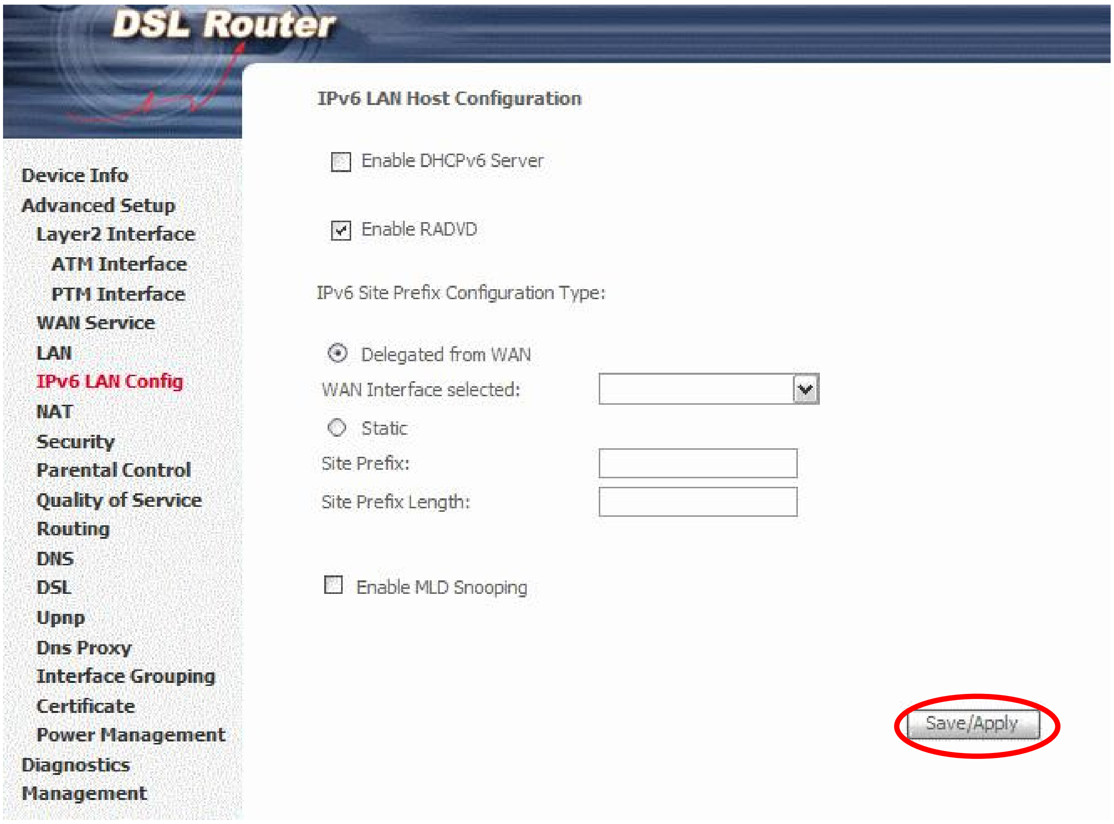
Subnet Mask:

IP Address: Enter the secondary IP address for the LAN port.

Subnet Mask: Enter the secondary subnet mask for the LAN port.

6.4 IPv6 LAN Host

Configure the IPv6 LAN Host options (see below) and then click **Save/Apply**.



IPv6 LAN Host Configuration

☐ Enable DHCPv6 Server

☑ Enable RADVD

IPv6 Site Prefix Configuration Type:

● Delegated from WAN

WAN Interface selected:

○ Static

Site Prefix:

Site Prefix Length:

☐ Enable MLD Snooping

DHCPv6 Server: To enable DHCP for IPv6, select the **Enable DHCPv6 server** checkbox ☑. This setting enables the router to assign IP settings to every IPv6-capable LAN device (IPv6 clients).

RADVD: Select the checkbox ☑ to enable the **R**outer **ADV**ertisement **D**aemon. This provides information that IPv6 clients can use for auto configuration according to the Neighbour Discovery for IPv6 protocol (RFC2461).

IPv6 Site Prefix

This setting can be delegated from a WAN Interface or assigned statically.

Enable MLD Snooping: Enable by ticking the checkbox ☑.

Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if snooping is enabled.

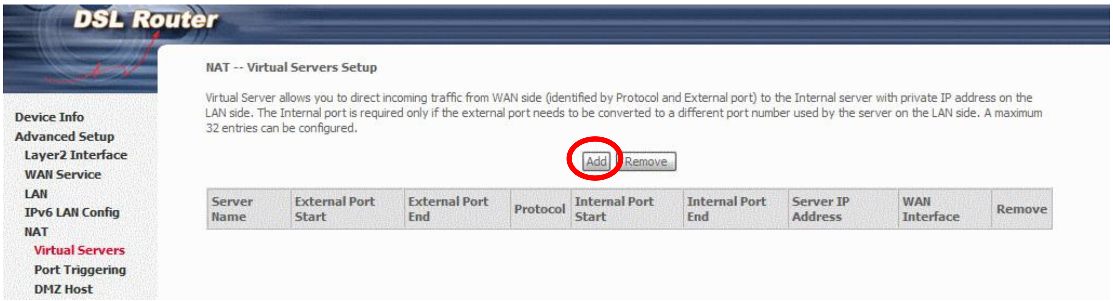
Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

6.5 NAT

To display this option, NAT must be enabled in at least one PVC shown on the Advanced Setup - WAN screen. *NAT is not an available option in Bridge mode*.

6.5.1 Virtual Servers

Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the Internal server with private IP addresses 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 of 32 entries can be configured.

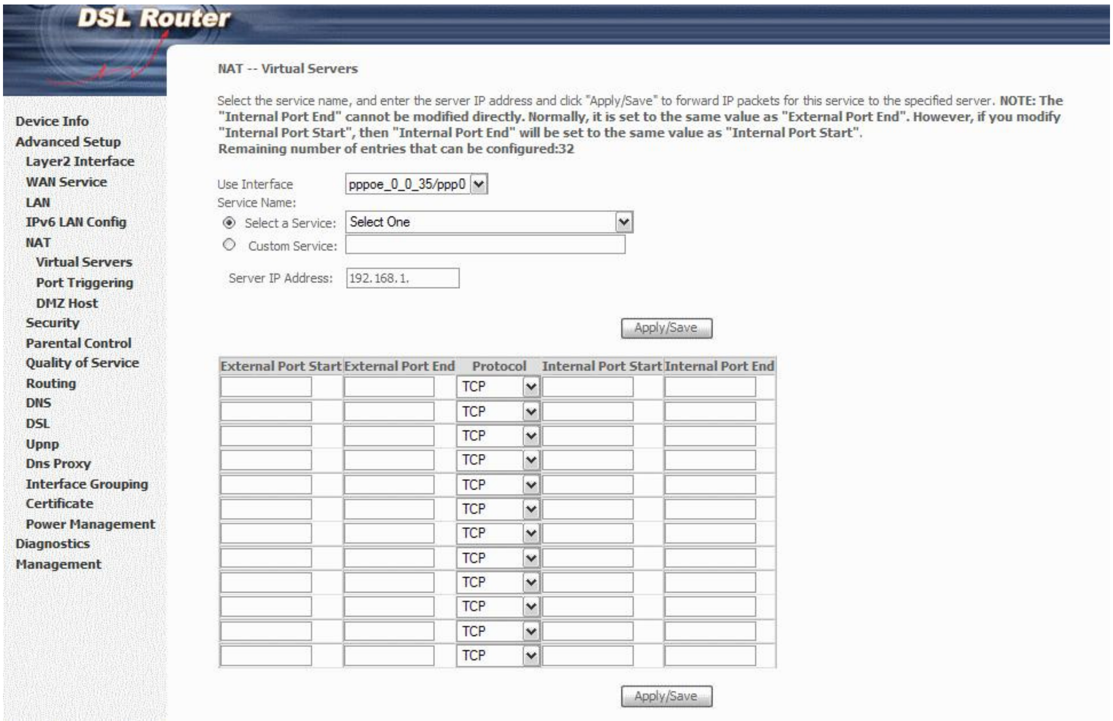


NAT -- Virtual Servers Setup

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

To add a Virtual Server, click **Add**. The following will be displayed.



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: pppoe_0_0_35/ppp0
Service Name:
● Select a Service: Select One
○ Custom Service:
Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

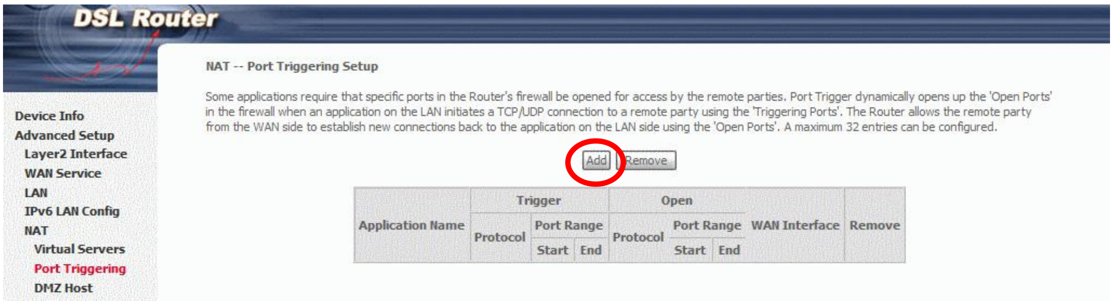
Consult the table below for field and header descriptions.

Field/Header	**Description**
Use Interface	Select a WAN interface from the drop-down box.
Select a Service **Or** Custom Service	User should select the service from the list. **Or** User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured

Field/Header	Description
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

6.5.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port Triggers dynamically '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.

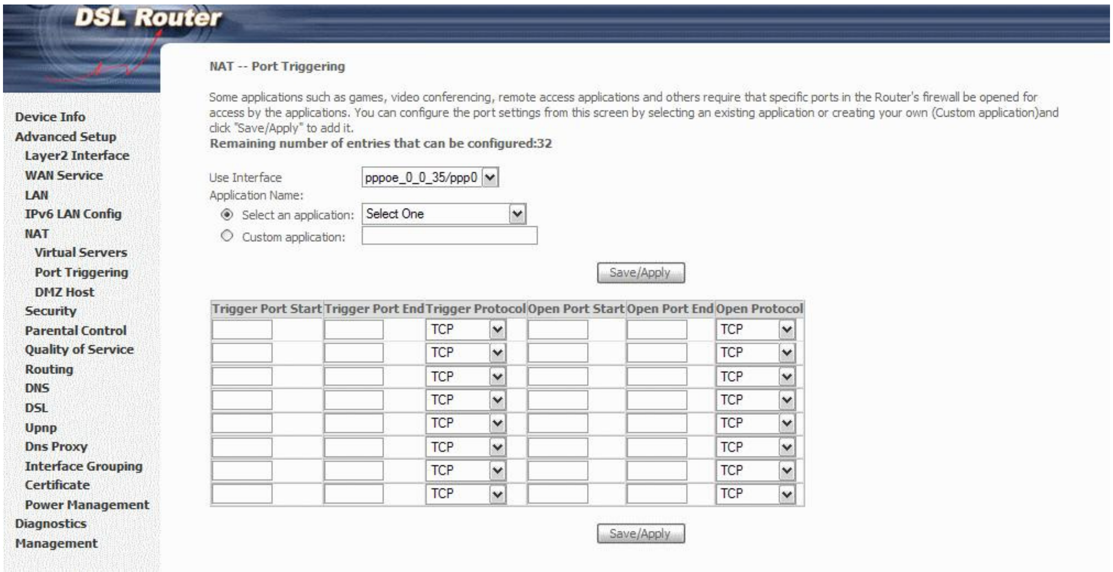


NAT -- Port Triggering Setup

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		

To add a Trigger Port, click **Add**. The following will be displayed.



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: pppoe_0_0_35/ppp0

Application Name:

● Select an application: Select One

○ Custom application:

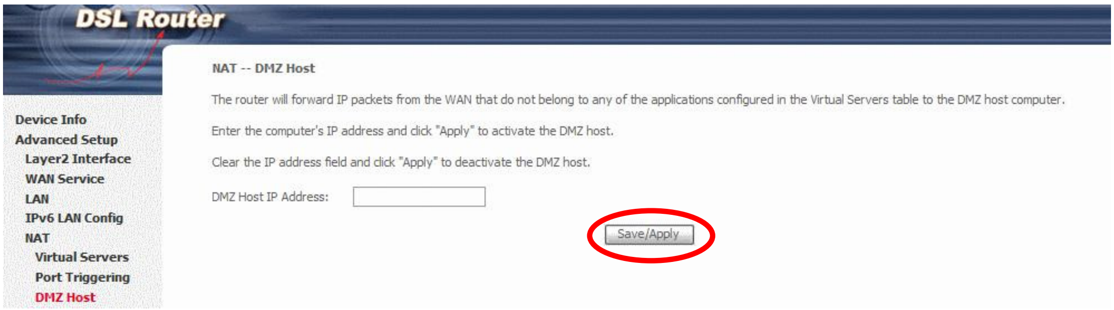
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Consult the table below for field and header descriptions.

Field/Header	**Description**
Use Interface	Select a WAN interface from the drop-down box.
Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP, or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP, or UDP.

6.5.3 DMZ Host

The DSL 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.



NAT -- DMZ Host

The 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:

To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.
To **Deactivate** the DMZ host, clear the IP address field and click **Save/Apply**.

6.6 Security

To display this function, you must enable the firewall feature in WAN Setup.
For detailed descriptions, with examples, please consult Appendix A.

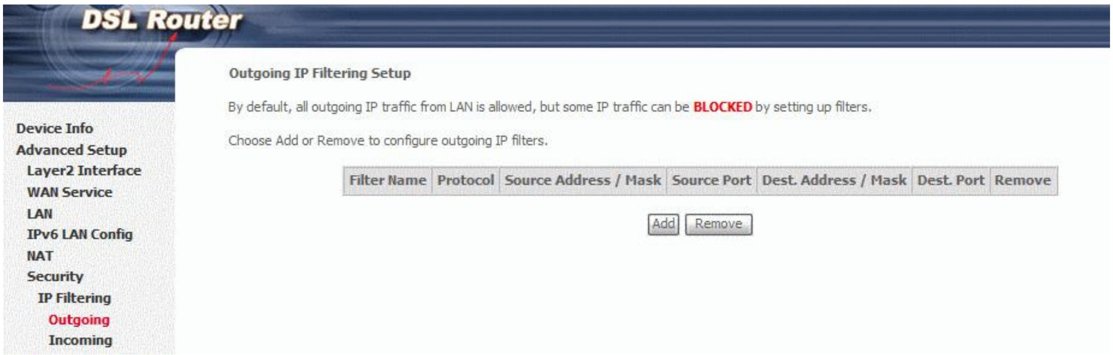
6.6.1 IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

NOTE: This function is not available when in bridge mode. Instead, MAC Filtering performs a similar function.

OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.



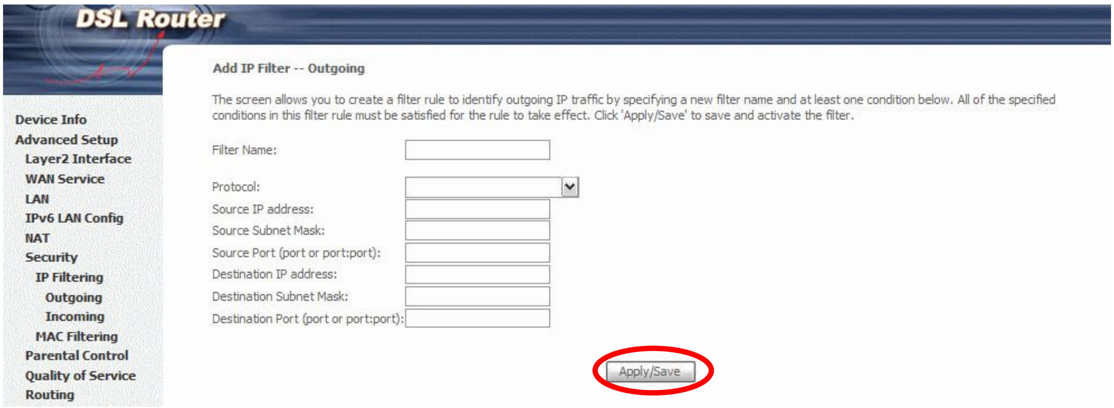
Outgoing IP Filtering Setup

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	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filter (to block some outgoing IP traffic), click the **Add** button.
On the following screen, enter your filter criteria and then click **Apply/Save**.



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:

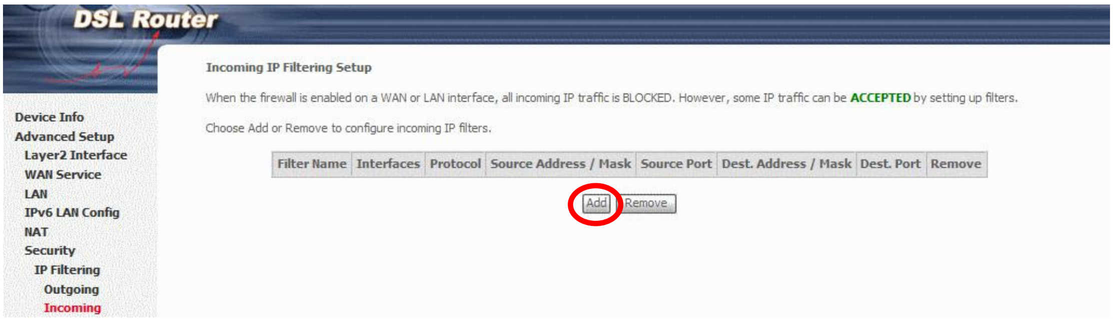
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination Port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.



Incoming IP Filtering Setup

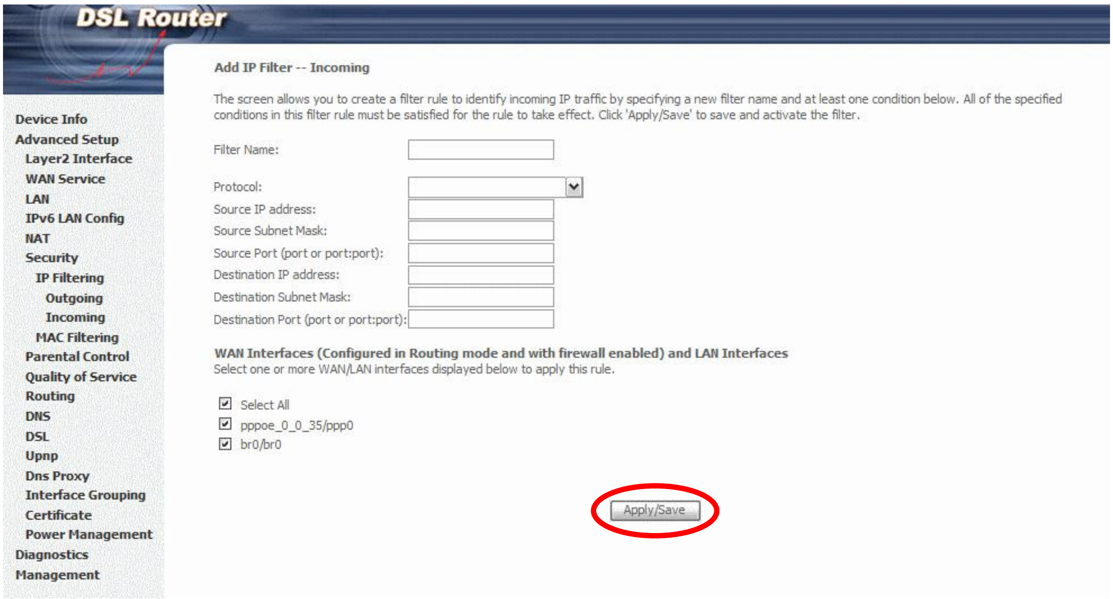
When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.



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:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

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
☑ pppoe_0_0_35/ppp0
☑ br0/br0

Consult the table below for field descriptions.

Field	**Description**
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination Port (port or port:port)	Enter destination port number or range.

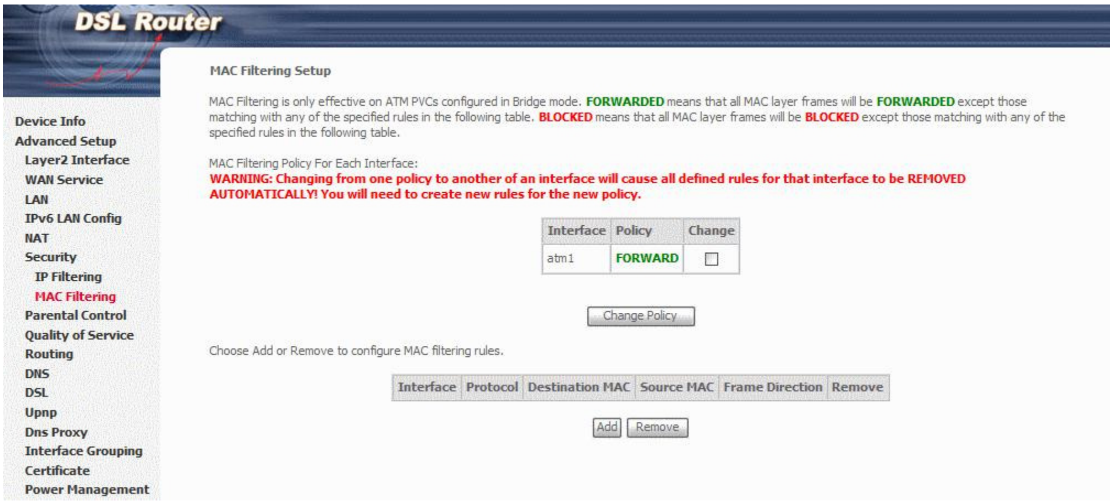
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

6.6.2 MAC Filtering

NOTE: This option is only available in bridge mode. Other modes use IP Filtering to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the Proscend 140 can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the MAC filter rules. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the MAC filter rules. The default MAC Filtering Global policy is **FORWARDED**. It can be changed by clicking the **Change Policy** button.



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.

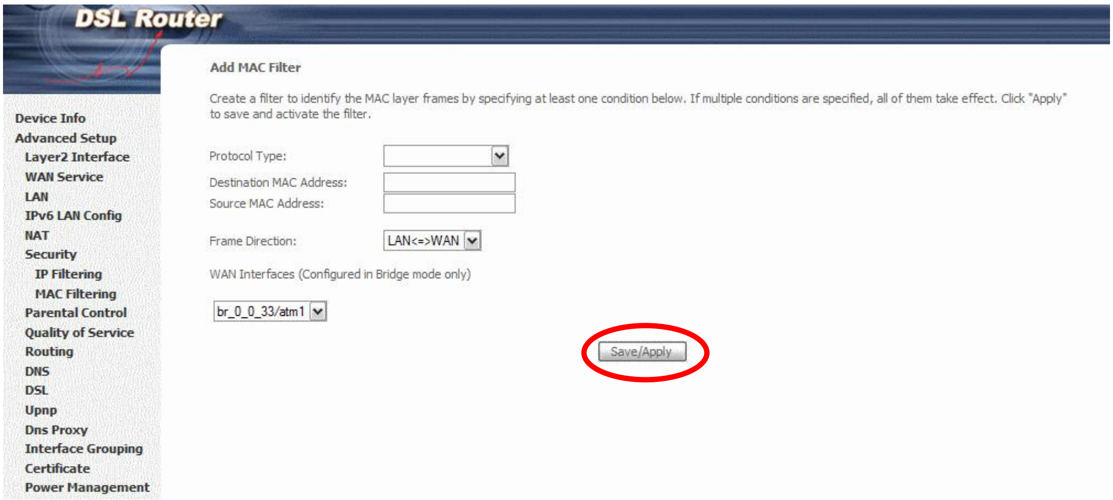
MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm1	FORWARD	□

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save/Apply** to save and activate the filter rule.



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: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_0_0_33/atm1

Consult the table below for detailed field descriptions.

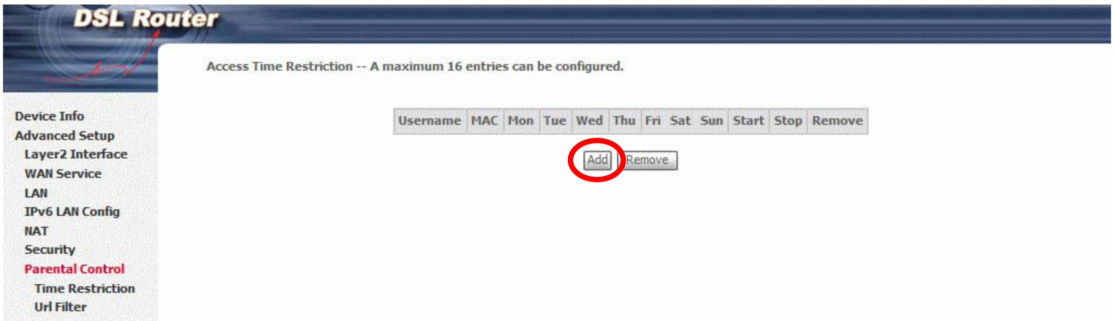
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface.

6.7 Parental Control

This selection provides WAN access control functionality.

6.7.1 Time Restriction

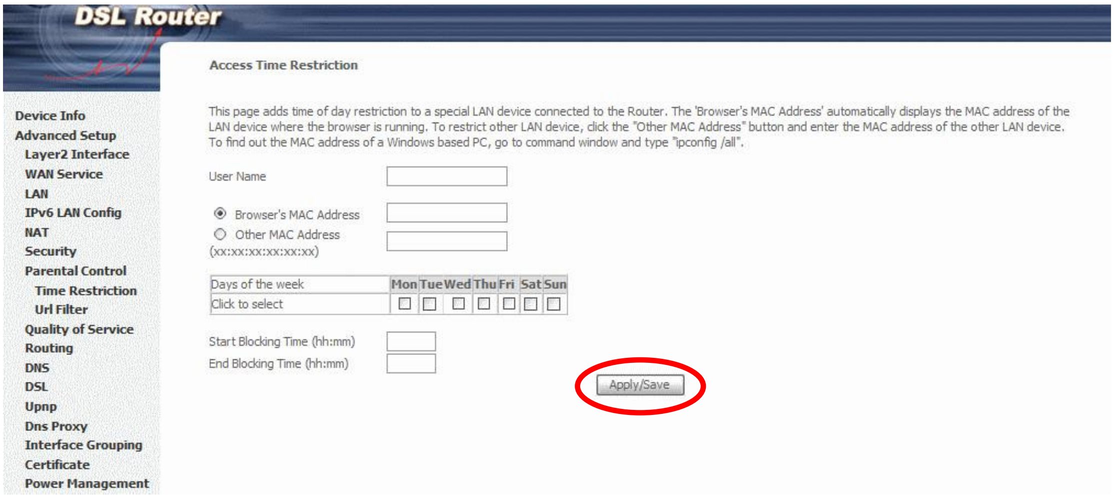
This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.4, so that the scheduled times match your local time.



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

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

Click **Add** to display the following screen.



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)

See below for field descriptions. Click **Apply/Save** to add a time restriction.

User Name: A user-defined label for this restriction.

Browser's MAC Address: MAC address of the PC running the browser.

Other MAC Address: MAC address of another LAN device.

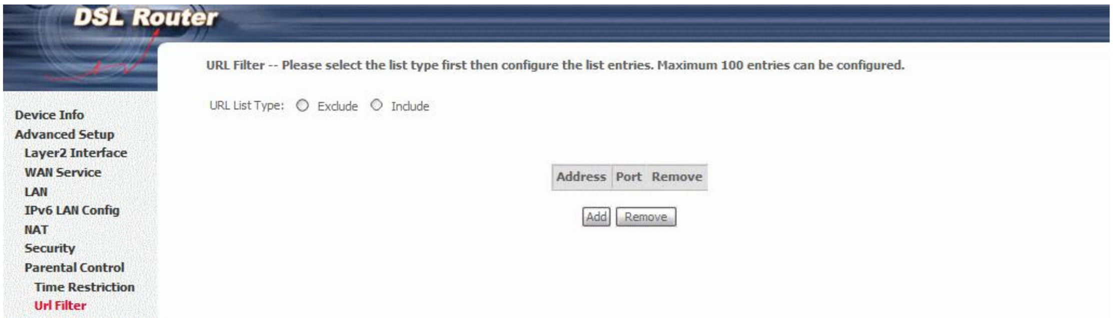
Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

End Blocking Time: The time the restrictions end.

6.7.2 URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL address and port number.

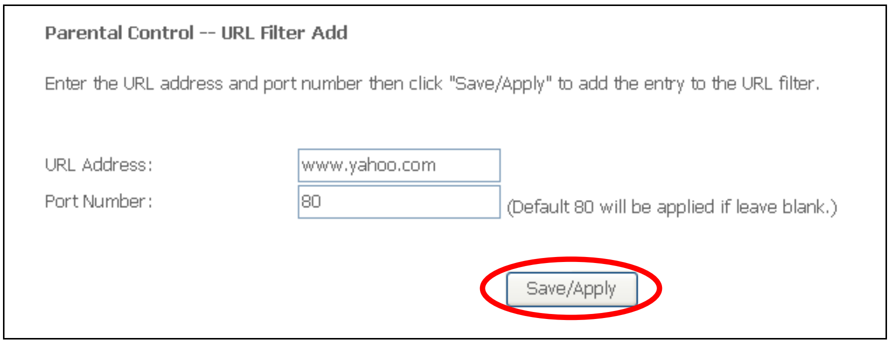


URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ○ Exclude ○ Include

Address	Port	Remove

Click **Add** to display the following screen.



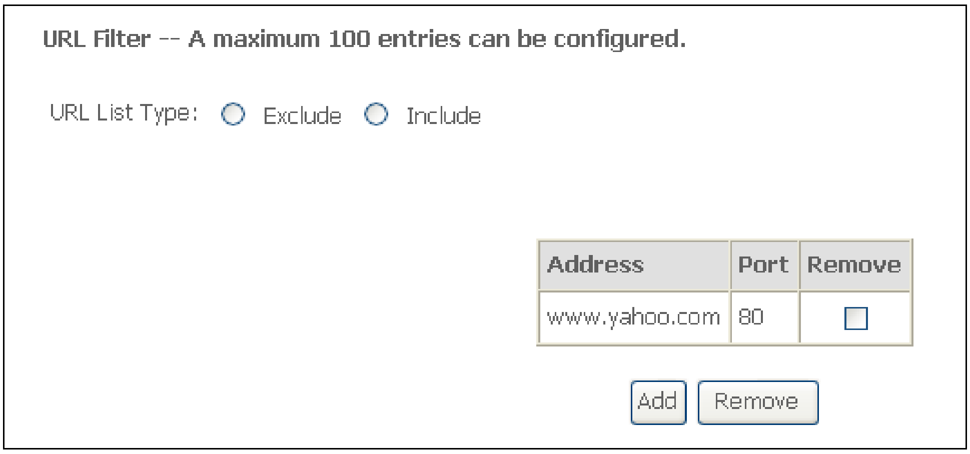
Parental Control -- URL Filter Add

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

URL Address: www.yahoo.com

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

Enter the URL address and port number then click **Save/Apply** to add the entry to the URL filter. URL Addresses begin with "www", as shown in this example.



URL Filter -- A maximum 100 entries can be configured.

URL List Type: ○ Exclude ○ Include

Address	Port	Remove
www.yahoo.com	80	□

A maximum of 100 entries can be added to the URL Filter list.

Tick the **Exclude** radio button to deny access to the websites listed.

Tick the **Include** radio button to restrict access to only those listed websites.

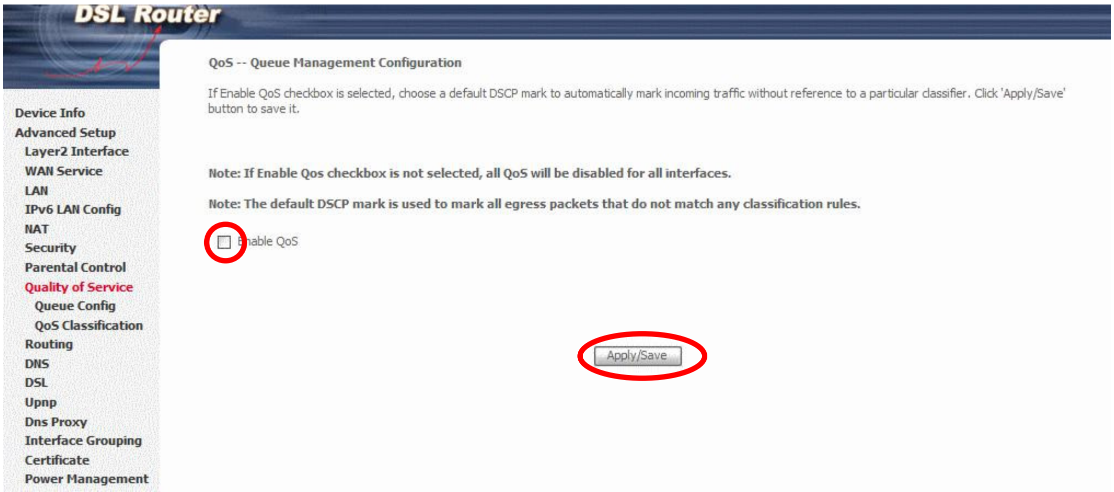
6.8 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option. (see Appendix E for detailed PVC setup instructions).

6.8.1 Queue Management Configuration

To Enable QoS tick the checkbox ☑ and select a Default DSCP Mark.

Click **Apply/Save** to activate QoS.



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

Apply/Save

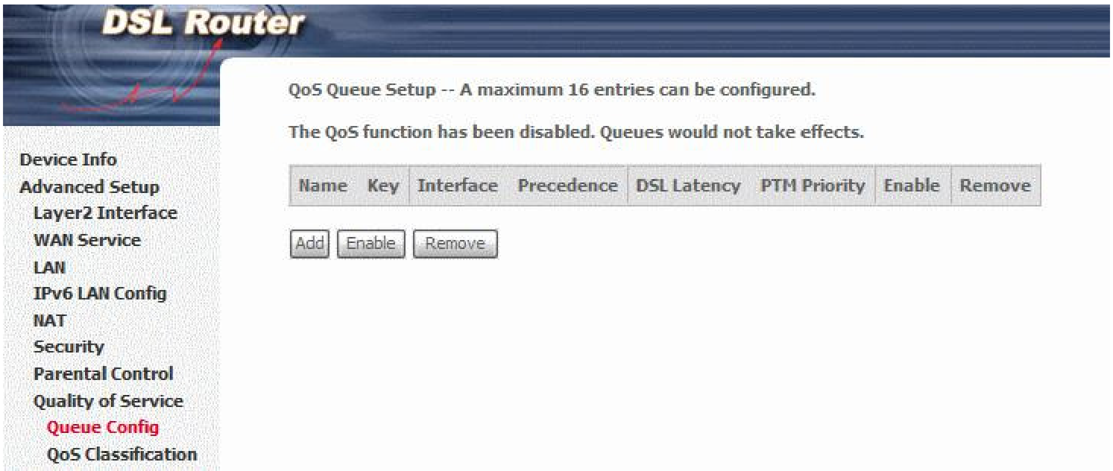
QoS and **DSCP Mark** are defined as follows:

Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

6.8.2 Queue Configuration

This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button. Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.

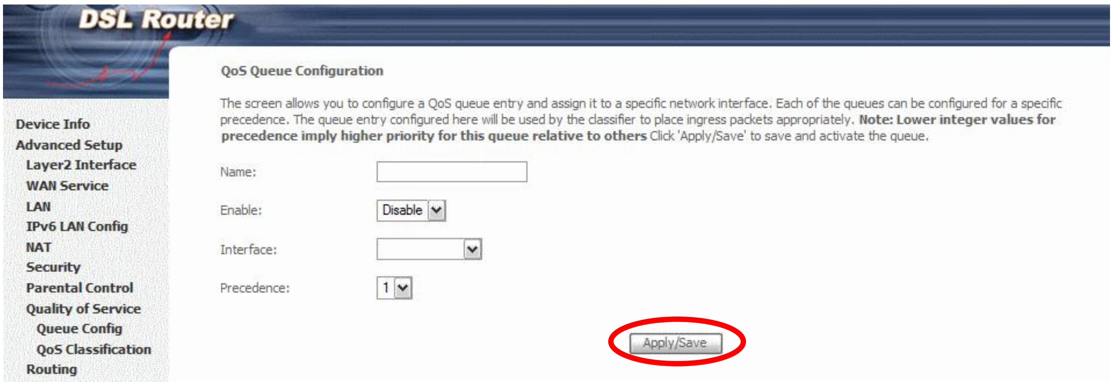


QoS Queue Setup -- A maximum 16 entries can be configured.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove

Click **Enable** to activate the QoS Queue. Click **Add** to display the following screen.



QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Apply/Save' to save and activate the queue.

Name:

Enable: Disable

Interface:

Precedence: 1

Name: Identifier for this Queue entry.

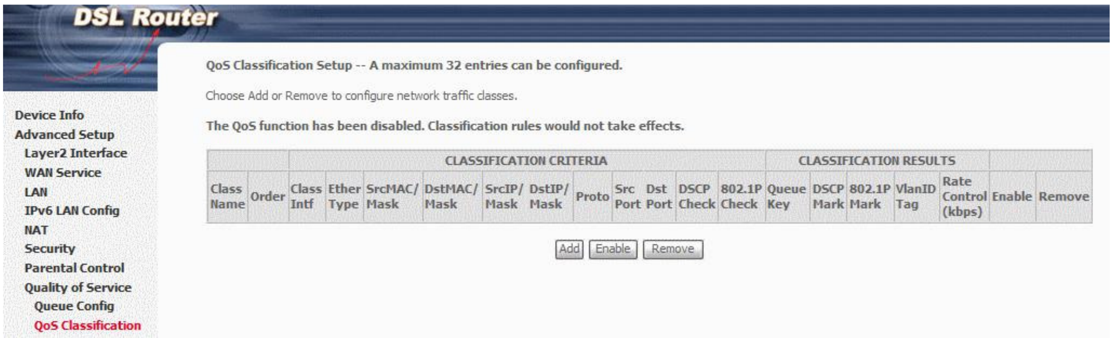
Enable: Enable/Disable the Queue entry.

Interface: Assign the entry to a specific network interface (QoS enabled).

Precedence: Configure precedence for the Queue entry. Lower integer values for precedence imply higher priority for this entry relative to others.

6.8.3 QoS Classification

The network traffic classes are listed in the following table.



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

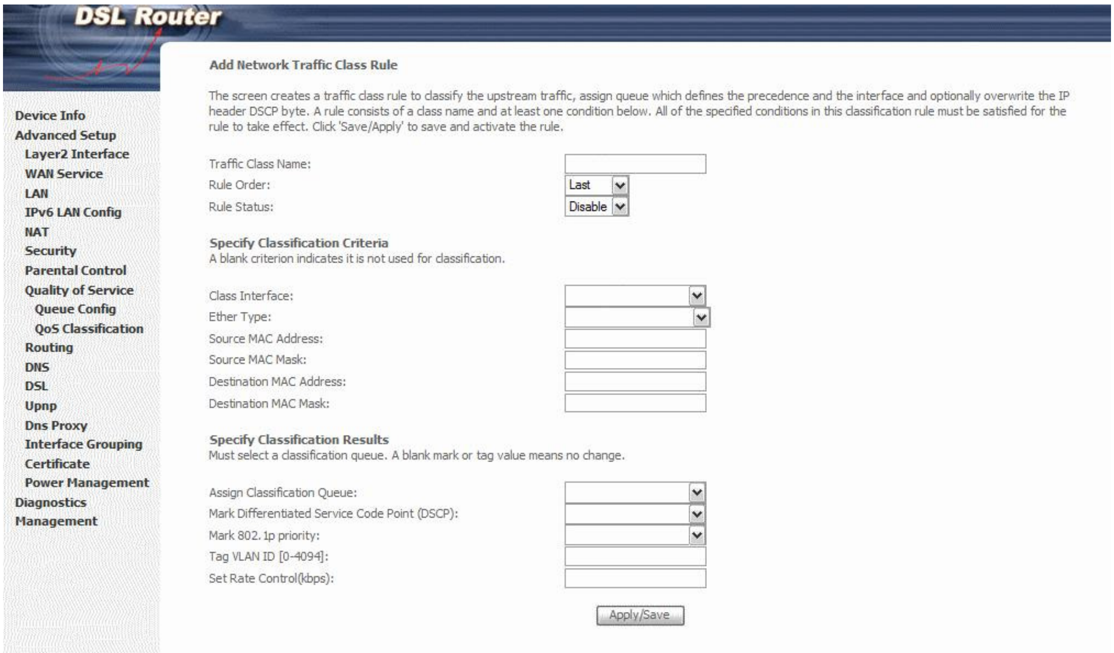
Choose Add or Remove to configure network traffic classes.

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/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove

Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one logical condition. All the conditions specified in the rule must be satisfied for it to take effect.



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which 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 below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' 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:
Ether Type:
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:
Mark Differentiated Service Code Point (DSCP):
Mark 802.1p priority:
Tag VLAN ID [0-4094]:
Set Rate Control(kbps):

Field	**Description**
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-3)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
Assign Classification Queue	The queue configurations are presented in this format: "Interfacename&Prece P&Queue Q" where P and Q are the Precedence and Queue Key values for the corresponding Interface as listed on the Queue Config screen.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. Lower values have higher priority.
Tag VLAN ID	Enter a 802.1Q VLAN ID tag [2-4094]
Set Rate Control	The data transmission rate limit in kbps.

6.9 Routing

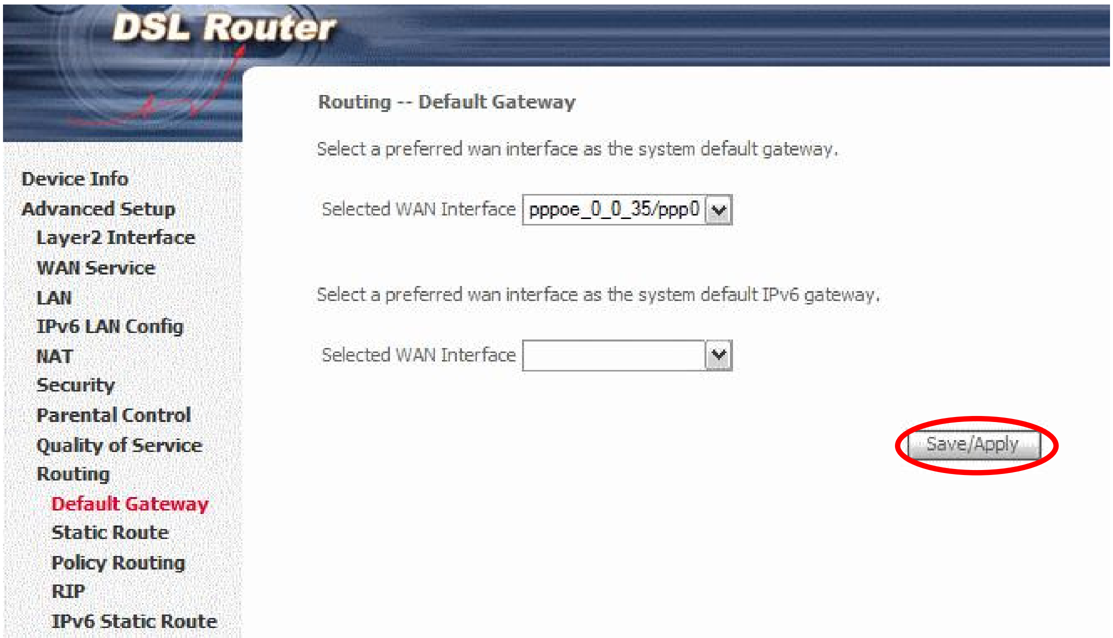
The following routing functions are accessed from this menu:

Default Gateway, Static Route, Policy Routing, RIP and **IPv6 Static Route**.

NOTE: In bridge mode, the **RIP** menu option is hidden while the other menu options are shown but ineffective.

6.9.1 Default Gateway

Select WAN Interfaces as default gateways and then click **Save/Apply**.



Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoe_0_0_35/ppp0

Select a preferred wan interface as the system default IPv6 gateway.

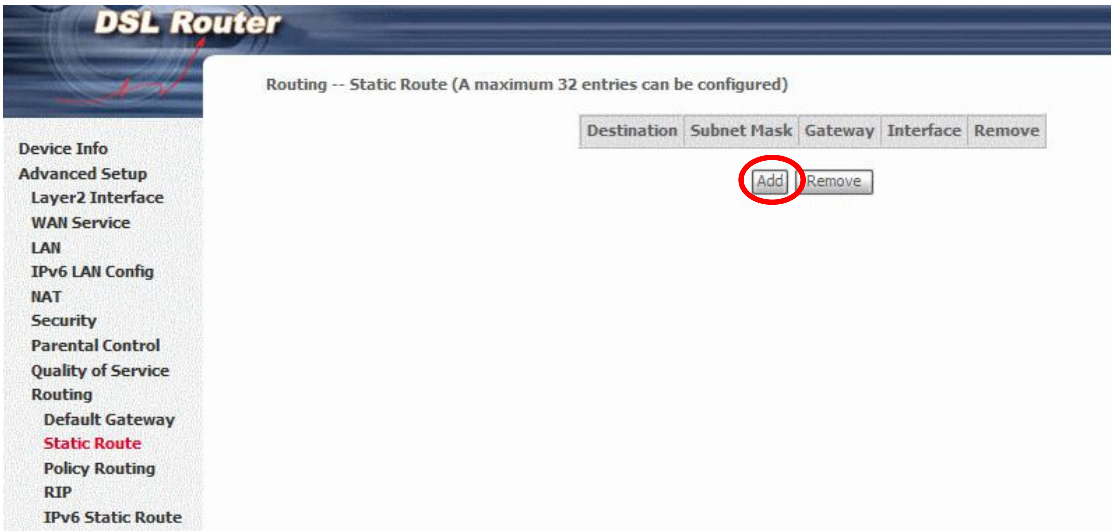
Selected WAN Interface

NOTE: After enabling the Automatic Assigned Default Gateway, the device must be rebooted to activate the assigned default gateway.

6.9.2 Static Route

This option allows for the configuration of static routes by destination IP.

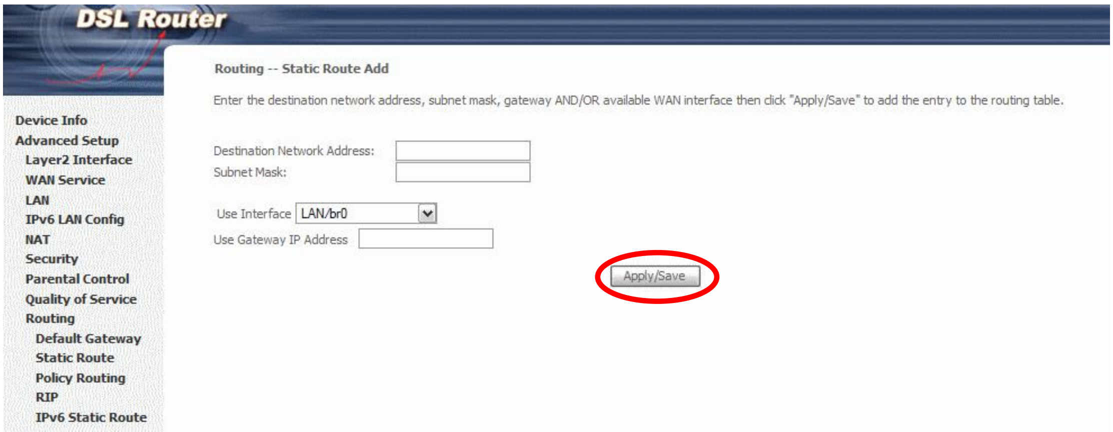
Click **Add** to create a static route or click **Remove** to delete a static route.



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

Destination	Subnet Mask	Gateway	Interface	Remove

After clicking **Add** the following screen will display.



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.

Destination Network Address:

Subnet Mask:

Use Interface LAN/br0

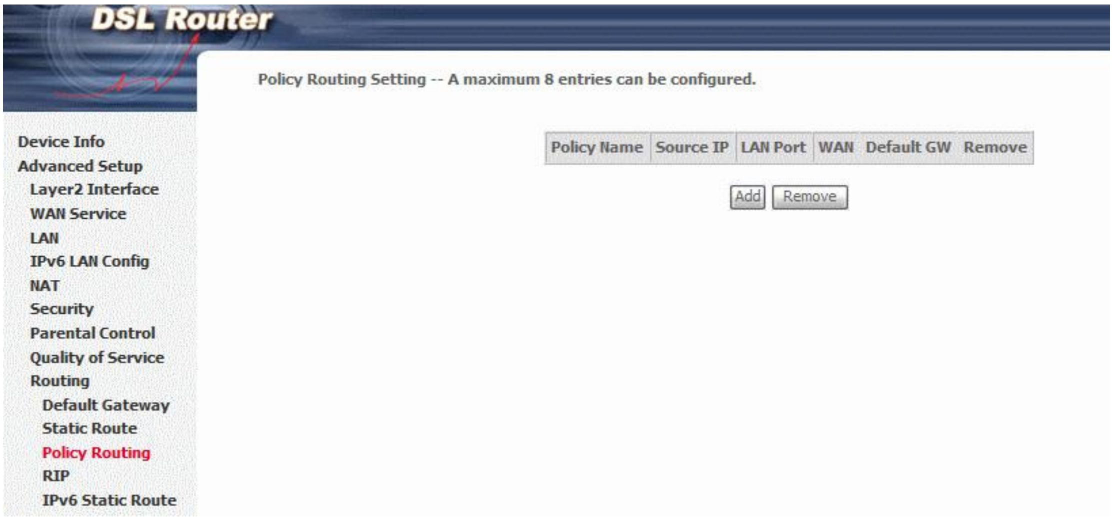
Use Gateway IP Address

Enter Destination Network Address, Subnet Mask, Gateway IP Address, and/or WAN Interface before clicking **Apply/Save** to add an entry to the routing table.

6.9.3 Policy Routing

This option allows for the configuration of static routes by policy.

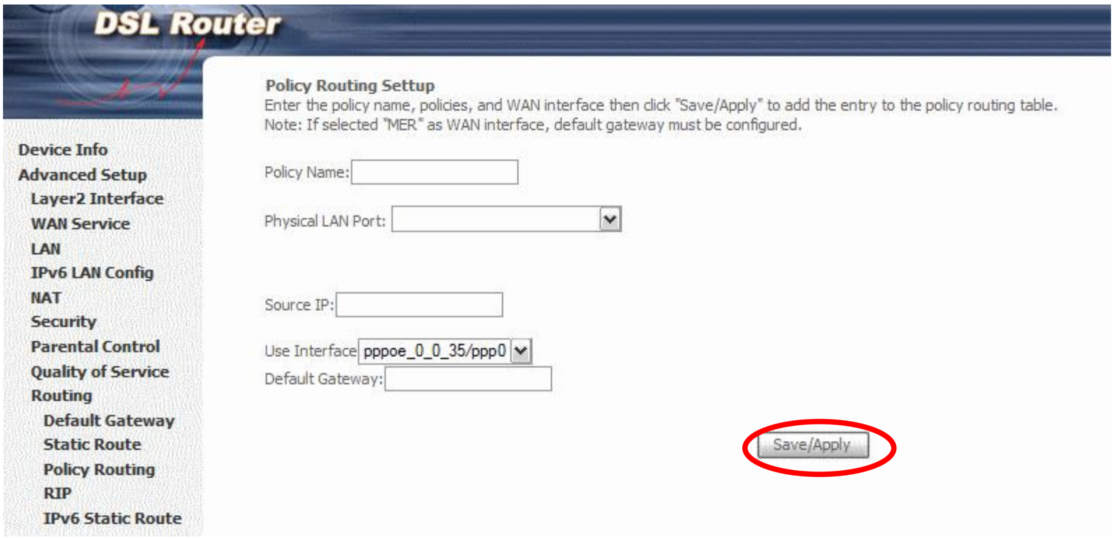
Click **Add** to create a routing policy or **Remove** to delete one.



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

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

On the following screen, complete the form and click **Save/Apply** to create a policy.



Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.

Note: If selected "MER" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

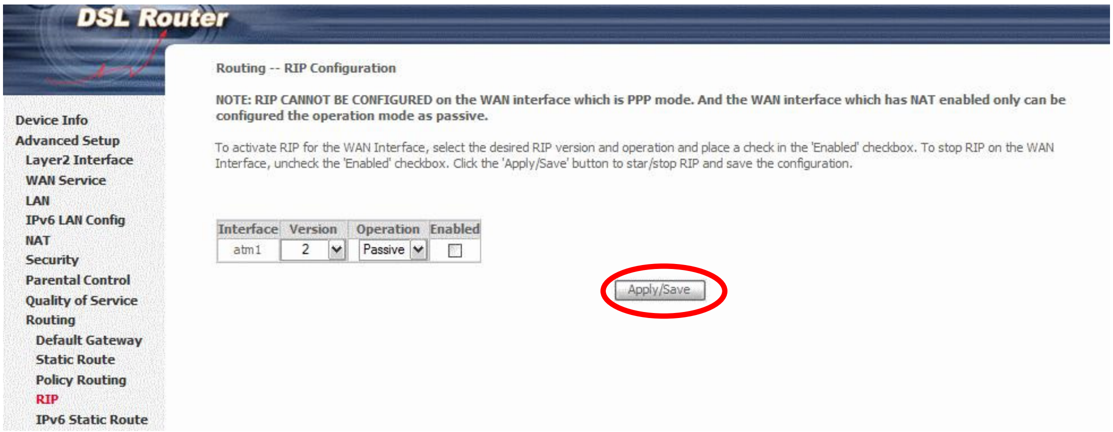
Source IP:

Use Interface pppoe_0_0_35/ppp0

Default Gateway:

6.9.4 RIP

To activate RIP, configure the RIP version/operation mode and select the **Enabled** checkbox ☑ for at least one WAN interface before clicking **Save/Apply**.



Routing -- RIP Configuration

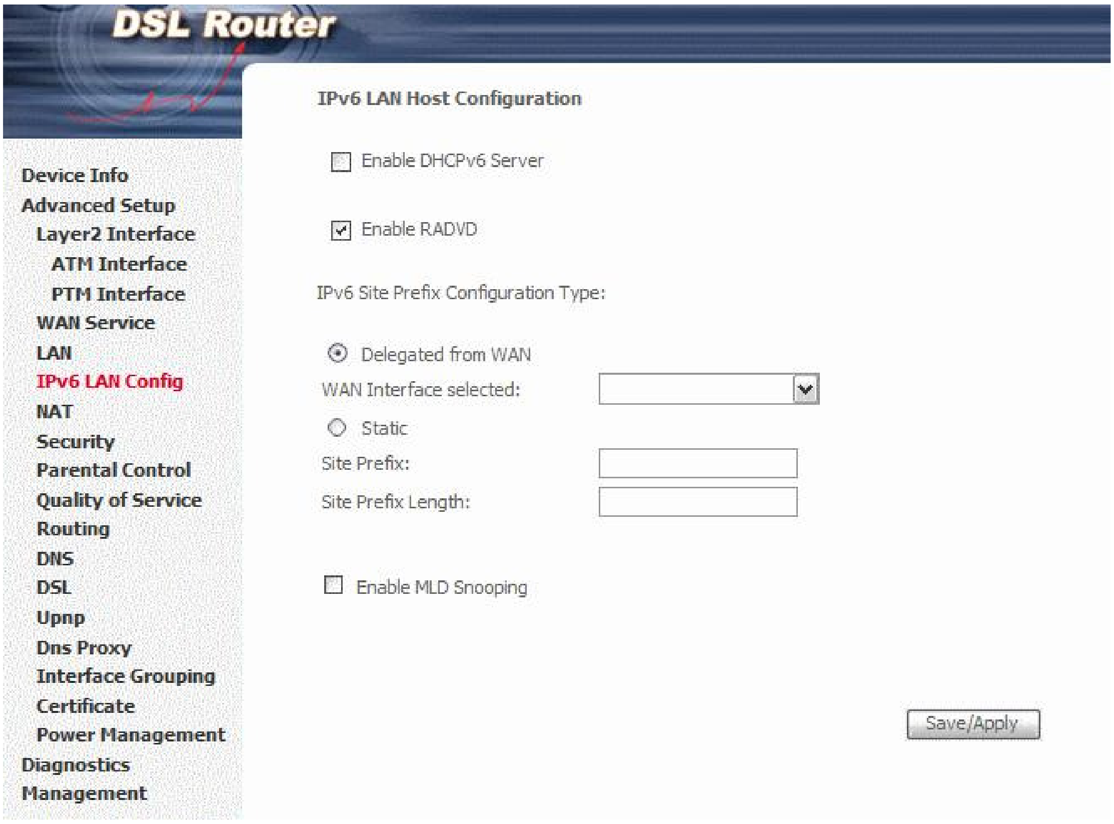
NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive.

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
atm1	2	Passive	□

6.9.5 IPv6 Static Route

This option allows for the configuration of static routes by destination IP. Click **Add** to create a static route or click **Remove** to delete a static route.



IPv6 LAN Host Configuration

□ Enable DHCPv6 Server

☑ Enable RADVD

IPv6 Site Prefix Configuration Type:

● Delegated from WAN

WAN Interface selected:

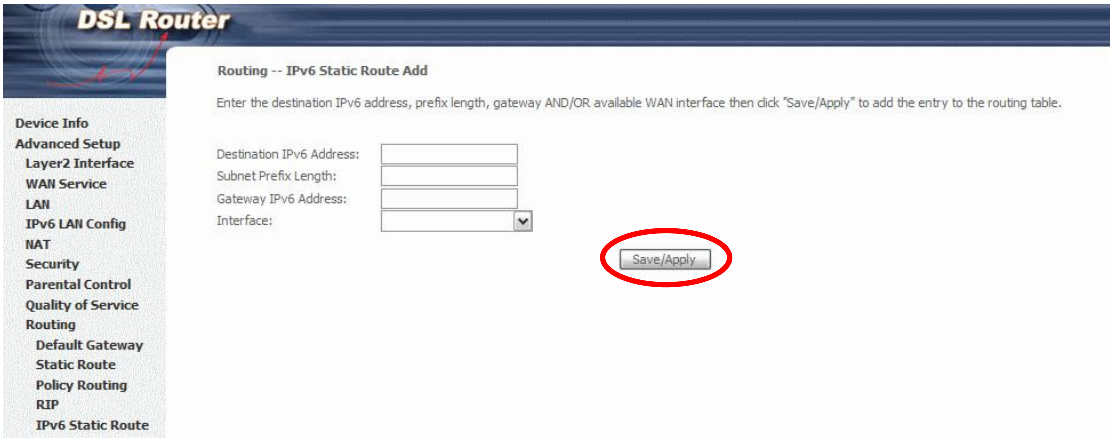
○ Static

Site Prefix:

Site Prefix Length:

□ Enable MLD Snooping

After clicking **Add** the following screen will display.



Routing -- IPv6 Static Route Add

Enter the destination IPv6 address, prefix length, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination IPv6 Address:

Subnet Prefix Length:

Gateway IPv6 Address:

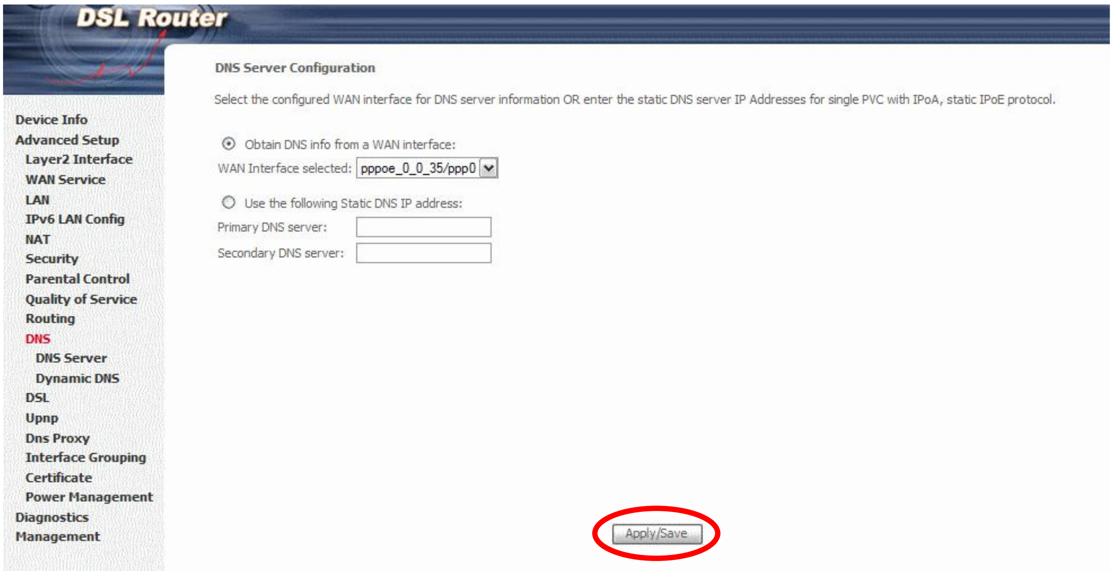
Interface:

Enter Destination IPv6 Address, Subnet Prefix Length, Gateway IPv6 Address, and/or Interface before clicking **Save/Apply** to add a routing entry.

6.10 DNS

6.10.1 DNS Server

To obtain DNS information from a WAN interface, select the first radio button and then choose a WAN interface from the drop-down box. For Static DNS, select the second radio button and enter the IP Address of the primary (and secondary) DNS server(s). Click **Apply/Save** to save the new configuration.



DNS Server Configuration

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static IPoE protocol.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoe_0_0_35/ppp0

○ Use the following Static DNS IP address:

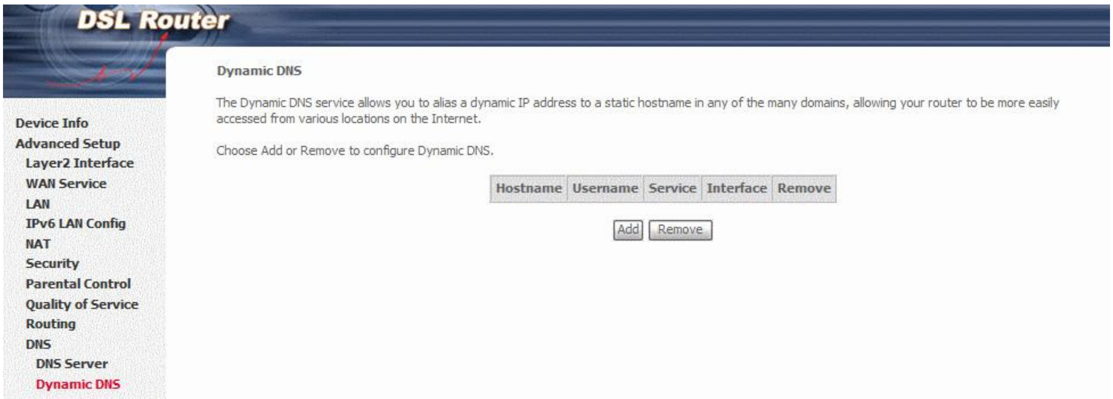
Primary DNS server:

Secondary DNS server:

NOTE: You must reboot the router to make the new configuration effective.

6.10.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the Proscend 140 to be more easily accessed from various locations on the Internet.



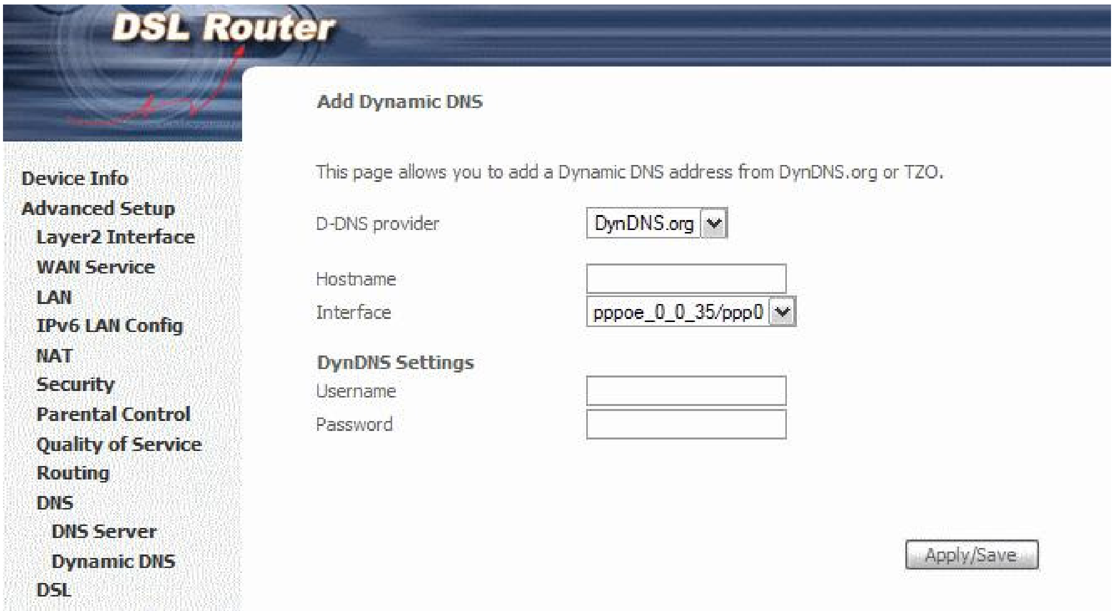
Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your 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

To add a dynamic DNS service, click **Add**. The following screen will display.



Add Dynamic DNS

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

D-DNS provider: DynDNS.org

Hostname:

Interface: pppoe_0_0_35/ppp0

DynDNS Settings

Username:

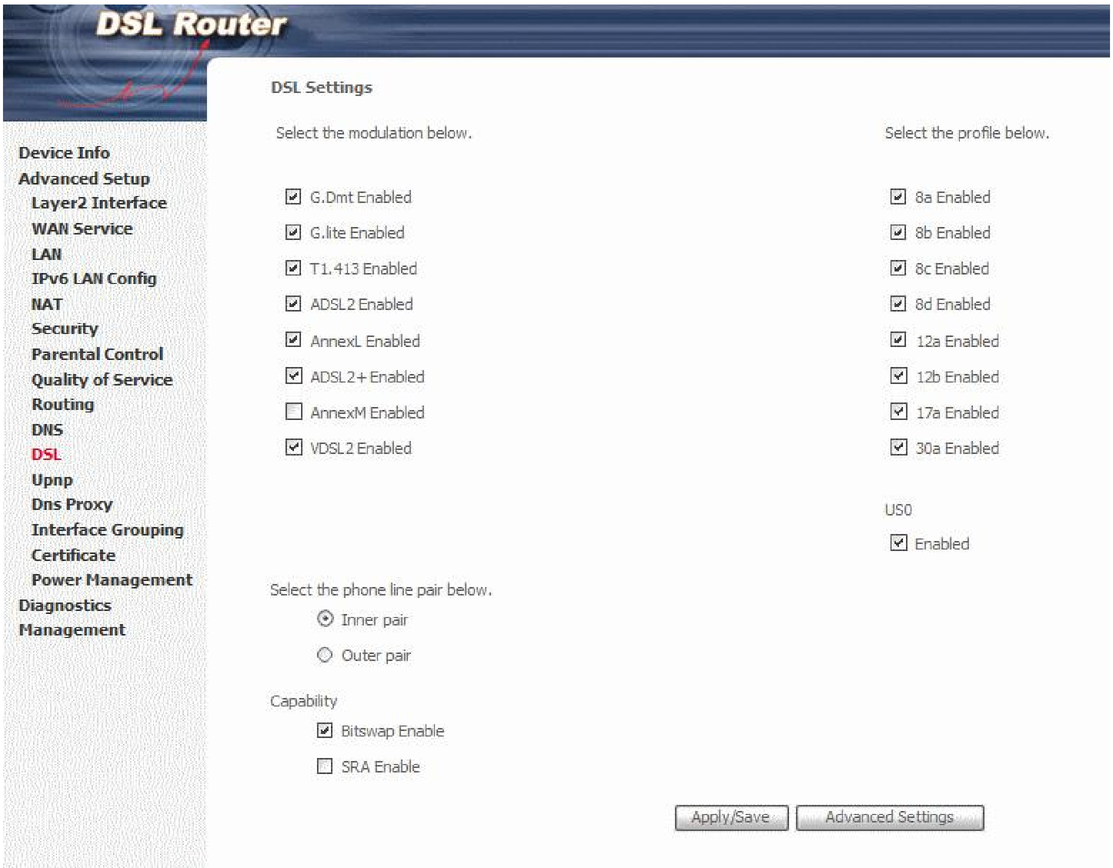
Password:

Consult the table below for field descriptions.

Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

6.11 DSL

The DSL Settings screen allows for the selection of DSL modulation modes. For optimum performance, the modes selected should match those of your ISP.



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

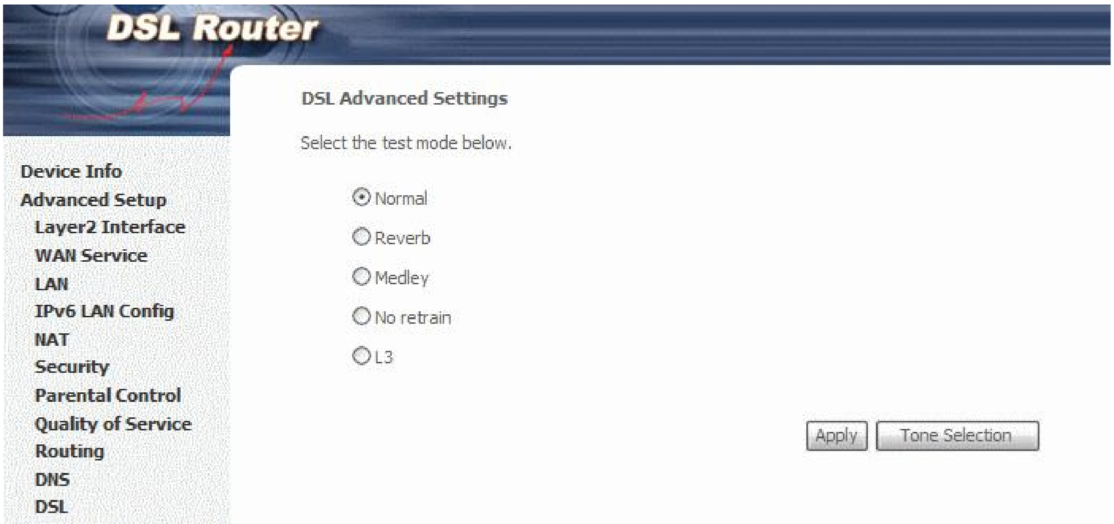
☑ Bitswap Enable
□ SRA Enable

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
G.Dmt	Downstream: 12 Mbps Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates
ADSL2+	Downstream: 24 Mbps Upstream: 1.0 Mbps
AnnexM	Downstream: 24 Mbps Upstream: 3.5 Mbps
VDSL2	Downstream: 100 Mbps Upstream: 60 Mbps
Options	**Description**

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)
Profile Selection	8a-d, 12a-b, 17a, 30a, US0

Advanced DSL Settings

Click **Advanced Settings** to reveal additional options. On the following screen you can select a test mode or modify tones by clicking **Tone Selection**. Click **Apply** to implement these settings and return to the previous screen.

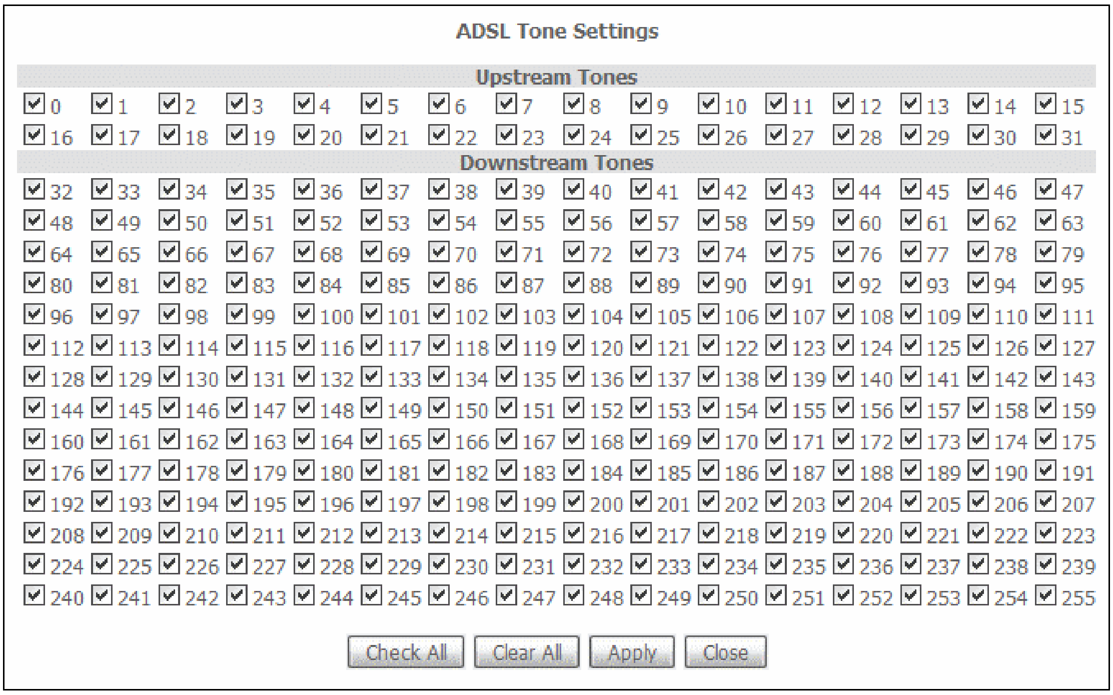


DSL Advanced Settings

Select the test mode below.

● Normal
○ Reverb
○ Medley
○ No retrain
○ L3

On this screen you select the tones you want activated, then click **Apply** and **Close**.



ADSL Tone Settings

Upstream Tones

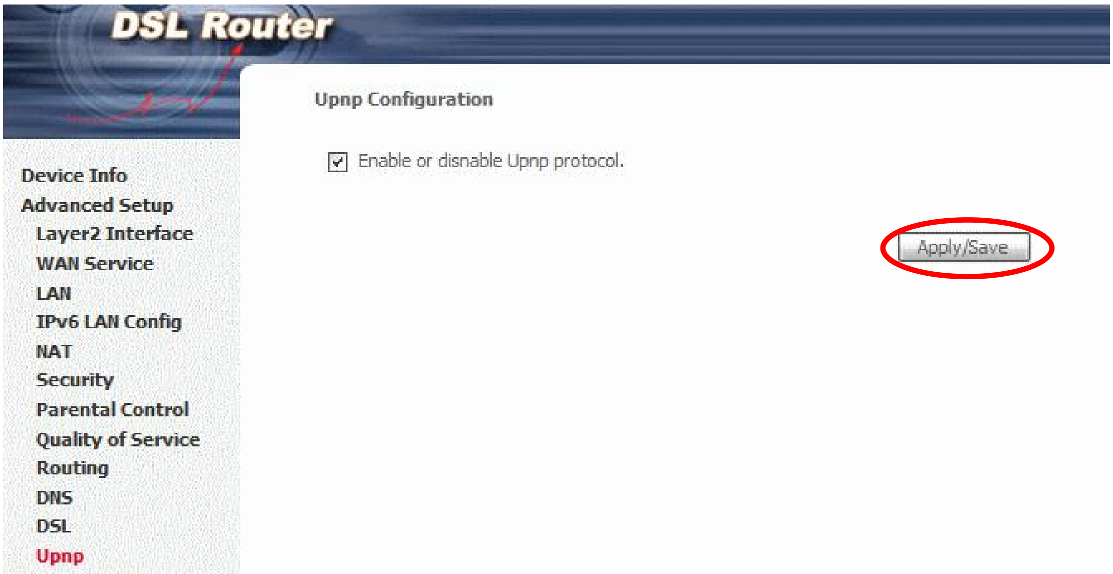
☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15
☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31

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

6.12 UPnP

Select the checkbox ☑ provided and click **Apply/Save** to enable UPnP protocol.

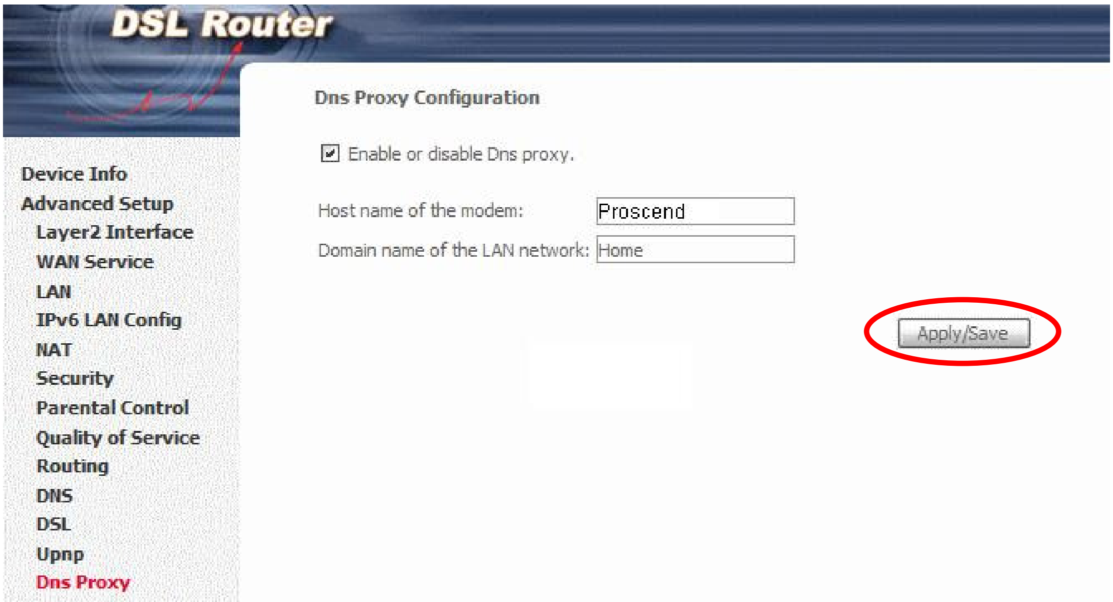


Upnp Configuration

☑ Enable or disnable Upnp protocol.

6.13 DNS Proxy

To enable DNS Proxy, select the corresponding checkbox ☑ and then enter Host and Domain names, as the example shown below. Click **Apply/Save** to continue.



Dns Proxy Configuration

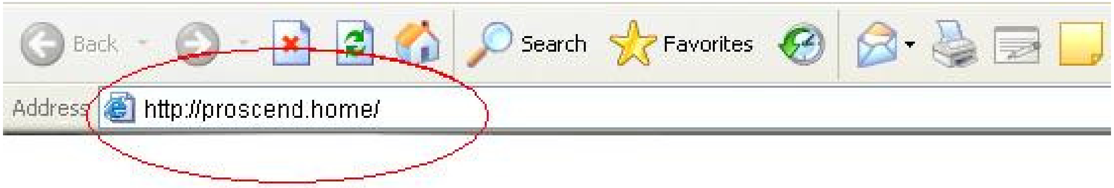
☑ Enable or disable Dns proxy.

Host name of the modem: Proscend

Domain name of the LAN network: Home

See below for further details.

The Host Name and Domain Name are combined to form a unique label that is mapped to the router IP address. This can be used to access the WUI with a local name rather than by using the router IP address. The figure below shows an example of this. In the browser address bar (circled in red) the prefix "http://" is added to the local name "proscend.home" [Host.Domain] for WUI access.

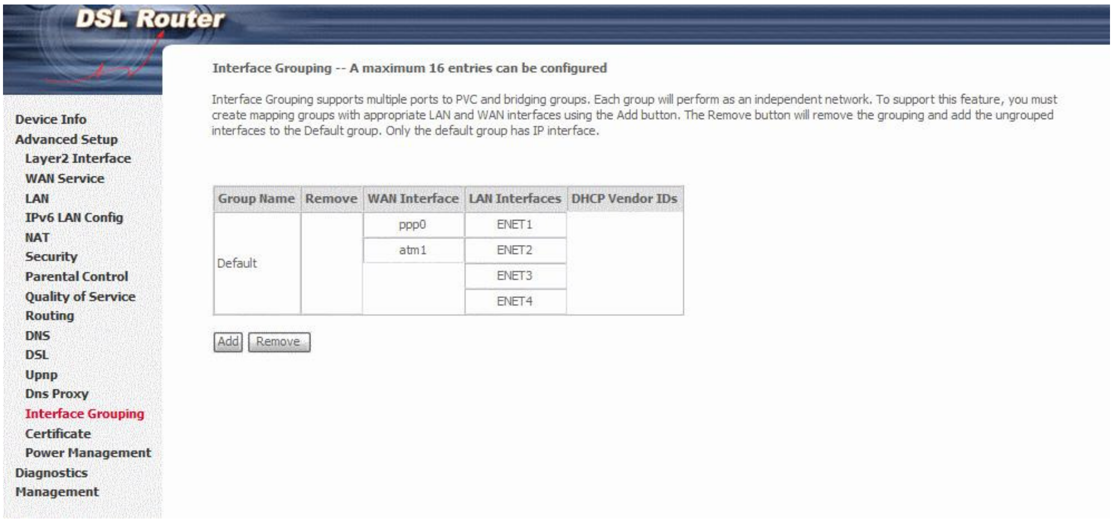


http://proscend.home/

6.14 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.

The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

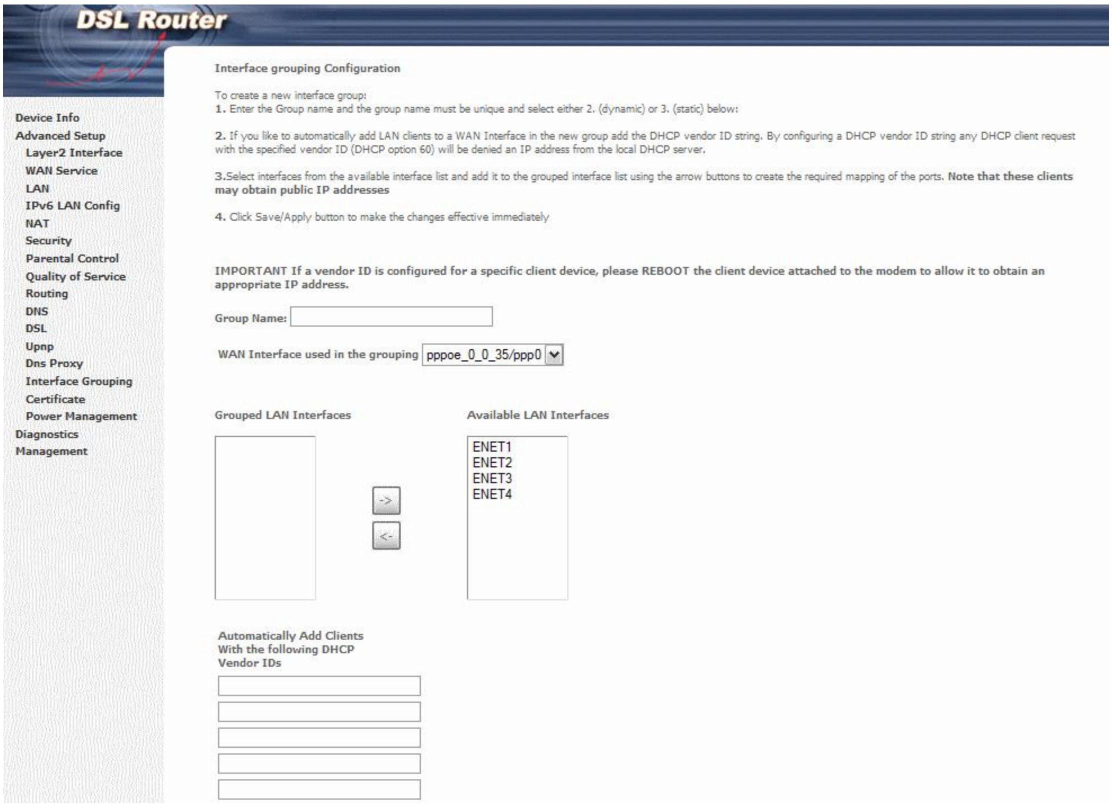


Interface Grouping -- A maximum 16 entries can be configured

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		ppp0	ENET1	
		atm1	ENET2	
			ENET3	
			ENET4	

To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown here.



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 Save/Apply 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:

WAN Interface used in the grouping: pppoe_0_0_35/ppp0

Grouped LAN Interfaces

Available LAN Interfaces: ENET1, ENET2, ENET3, ENET4

Automatically Add Clients With the following DHCP Vendor IDs

Automatically Add Clients With the Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Interface Grouping is enabled.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, and ENET4.

The Interface Grouping configuration will be:

1. Default: ENET1, ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

If the onboard DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

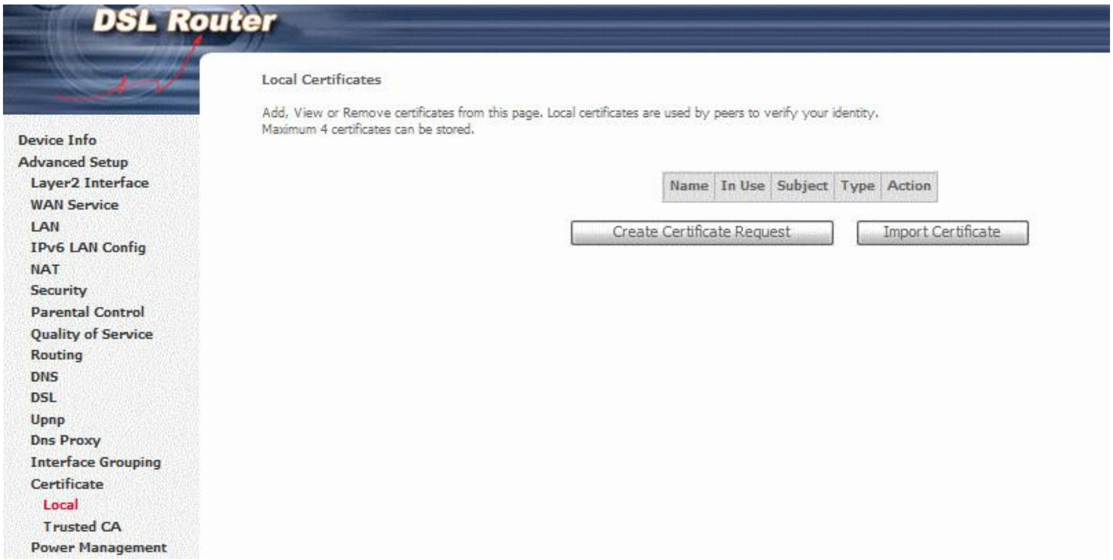
If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, nas_0_38, and ENET1.

6.15 Certificate

A certificate is a public key, attached with its owner’s information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures.   There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

6.15.1 Local



Local Certificates

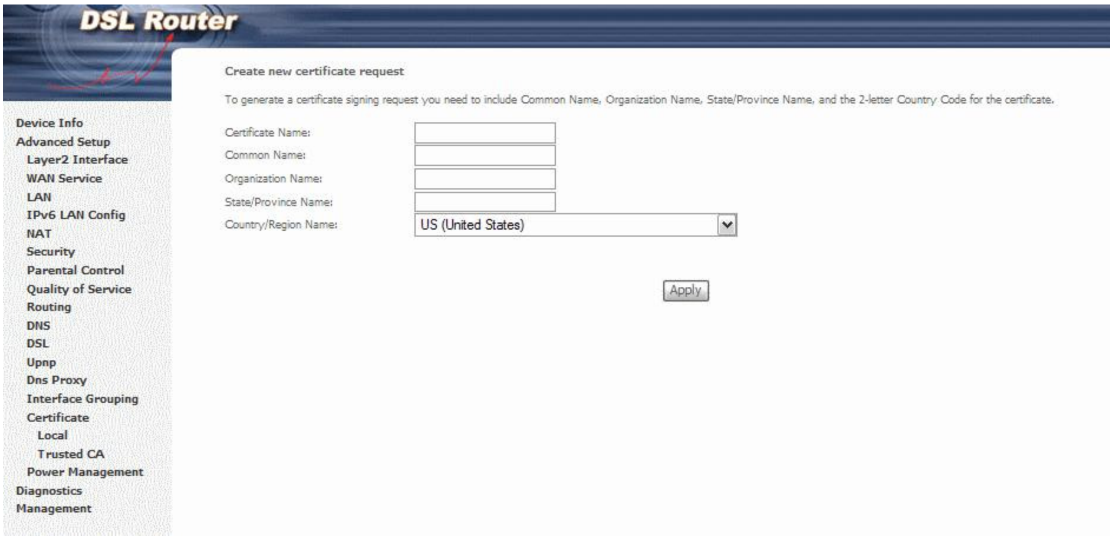
Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.



Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

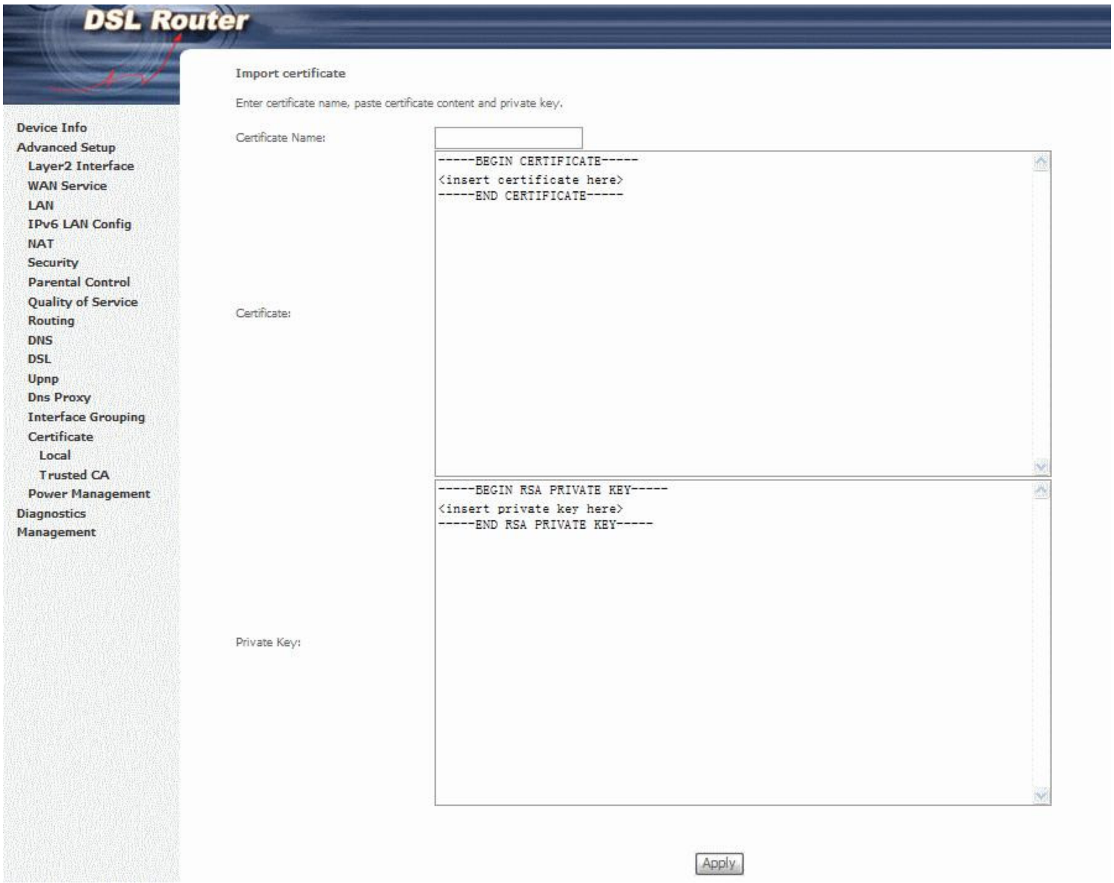
Country/Region Name: US (United States)

The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

IMPORT CERTIFICATE

Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.



Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

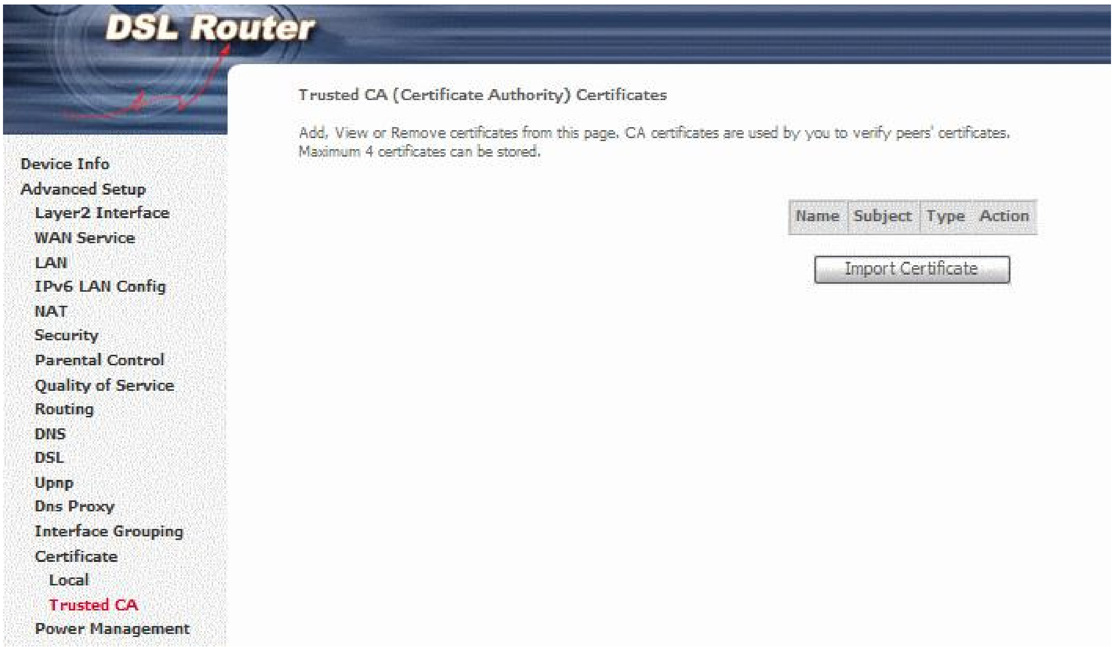
Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

Enter a certificate name and click **Apply** to import the local certificate.

6.15.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.

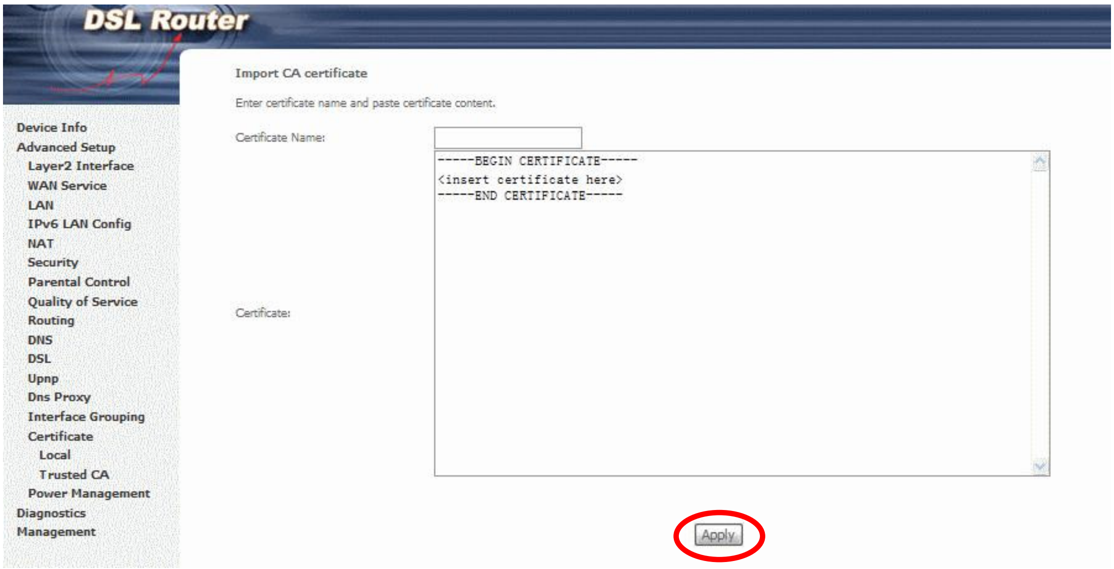


Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Name	Subject	Type	Action

Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

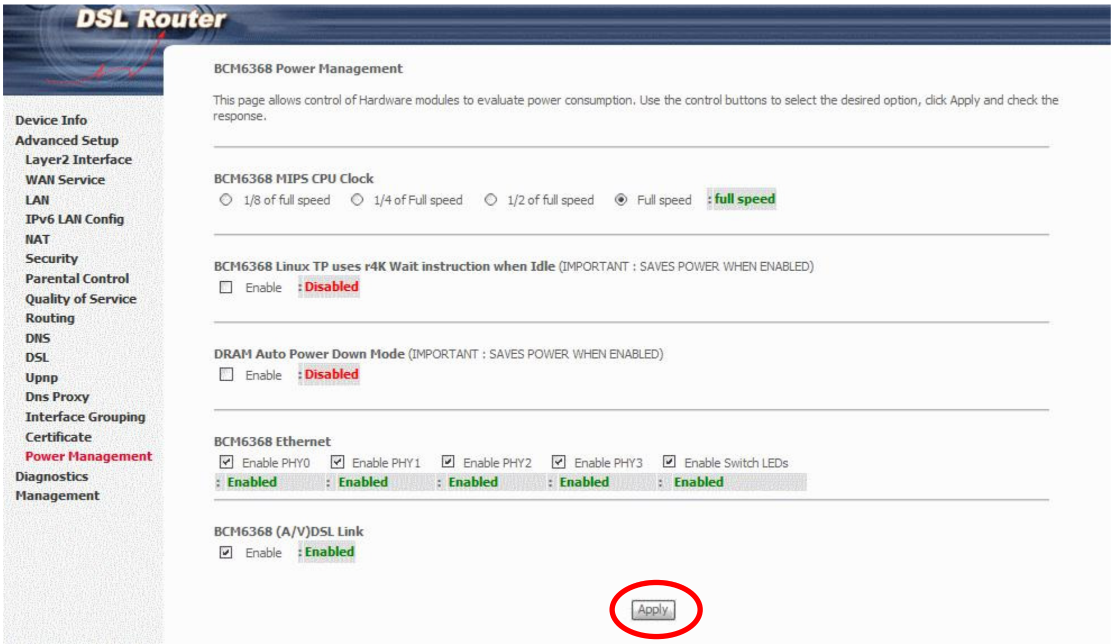
Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Enter a certificate name and click **Apply** to import the CA certificate.

6.16 Power Management

This screen allows for control of hardware modules to evaluate power consumption. Use the buttons to select the desired option, click **Apply** and check the response.



BCM6368 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 response.

BCM6368 MIPS CPU Clock
○ 1/8 of full speed ○ 1/4 of Full speed ○ 1/2 of full speed ● Full speed : full speed

BCM6368 Linux TP uses r4K Wait instruction when Idle (IMPORTANT : SAVES POWER WHEN ENABLED)
□ Enable : Disabled

DRAM Auto Power Down Mode (IMPORTANT : SAVES POWER WHEN ENABLED)
□ Enable : Disabled

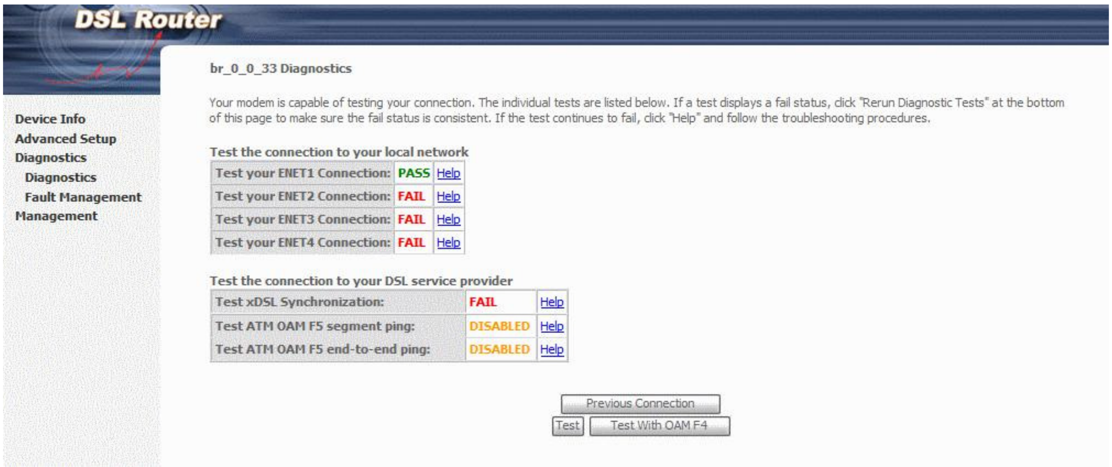
BCM6368 Ethernet

☑ Enable PHY0	☑ Enable PHY1	☑ Enable PHY2	☑ Enable PHY3	☑ Enable Switch LEDs
: Enabled	: Enabled	: Enabled	: Enabled	: Enabled

BCM6368 (A/V)DSL Link
☑ Enable : Enabled

Chapter 7 Diagnostics

The first Diagnostics screen is a dashboard that shows overall connection status. If a test displays a fail status, click the button to retest and confirm the error. If a test continues to fail, click Help and follow the troubleshooting procedures.



br_0_0_33 Diagnostics

Your modem is capable of testing your 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.

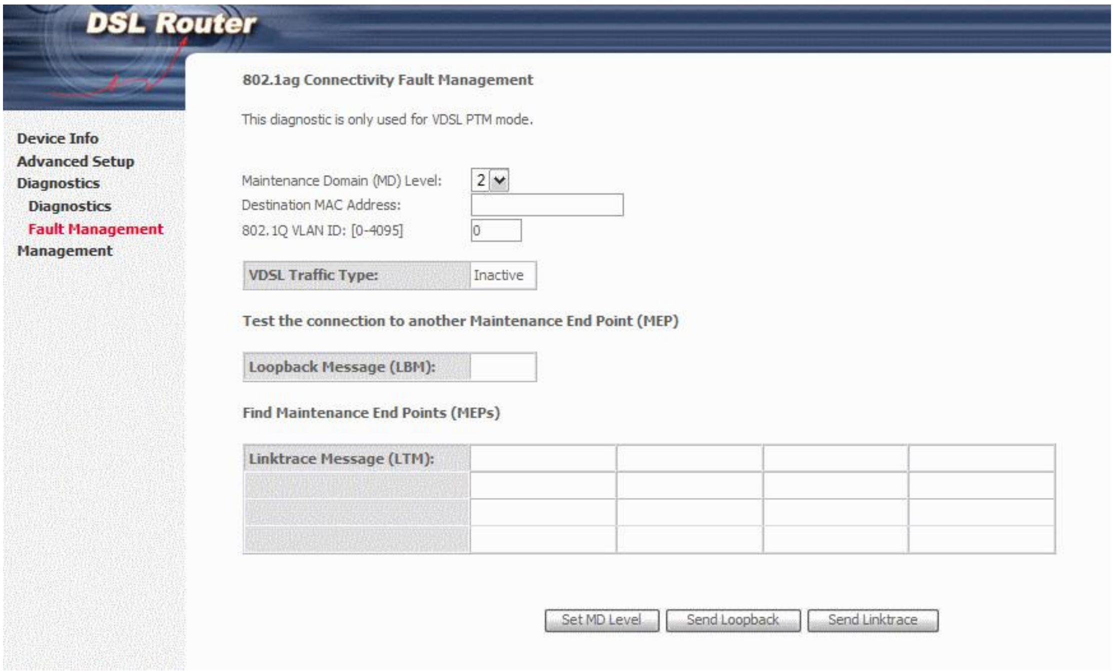
Test the connection to your local network

Test your ENET1 Connection:	PASS	Help
Test your ENET2 Connection:	FAIL	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	FAIL	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

The second Diagnostics screen (Fault Management) is used for VDSL diagnostics.



802.1ag Connectivity Fault Management

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level: 2

Destination MAC Address:

802.1Q VLAN ID: [0-4095] 0

VDSL Traffic Type:	Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):	

Find Maintenance End Points (MEPs)

Linktrace Message (LTM):				

Chapter 8 Management

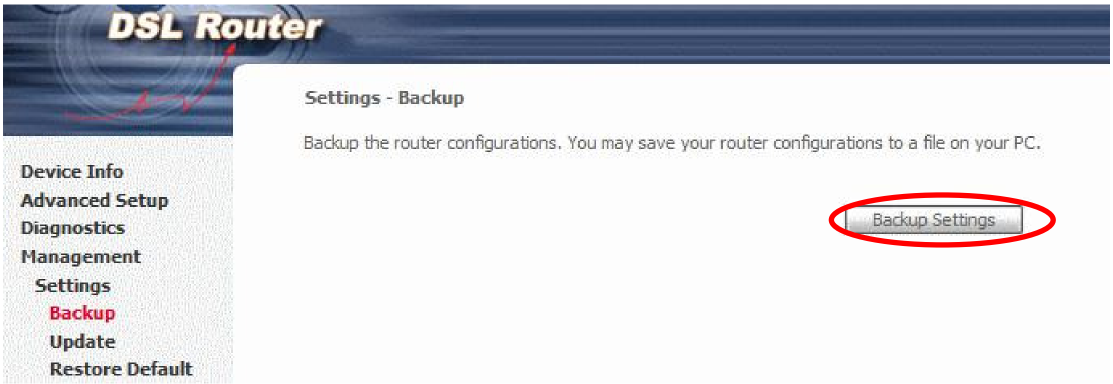
The Management menu has the following maintenance functions and processes:

8.1 Settings

This includes Backup Settings, Update Settings, and Restore Default screens.

8.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for the backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.



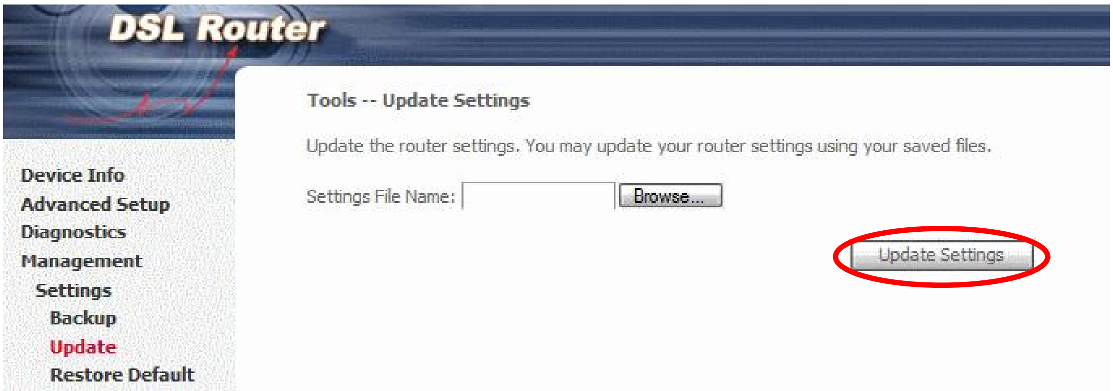
Settings - Backup

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

8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**.

Enter the file name (including folder path) in the **Settings File Name** box, or press **Browse...** to search for the file, then click **Update Settings** to recover settings.



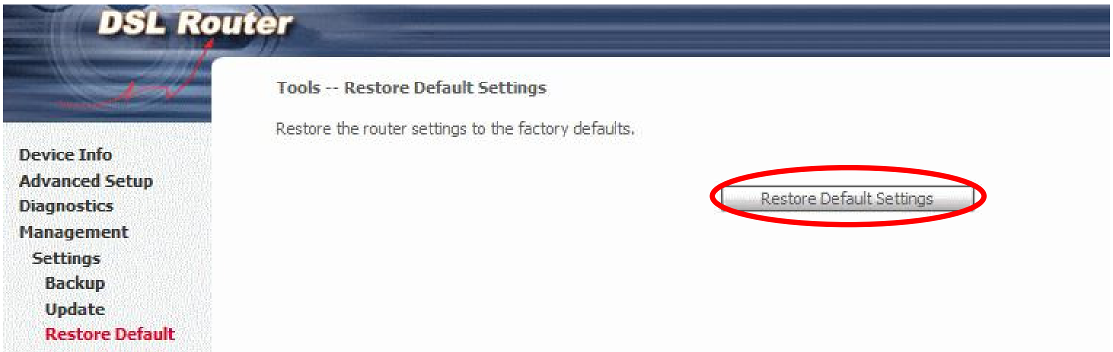
Tools -- Update Settings

Update the router settings. You may update your router settings using your saved files.

Settings File Name:

8.1.3 Restore Default

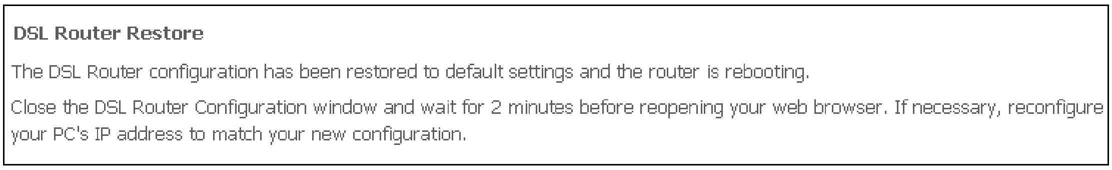
Click **Restore Default Settings** to restore factory default settings.



Tools -- Restore Default Settings

Restore the router settings to the factory defaults.

After **Restore Default Settings** is clicked, the following screen appears.



DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

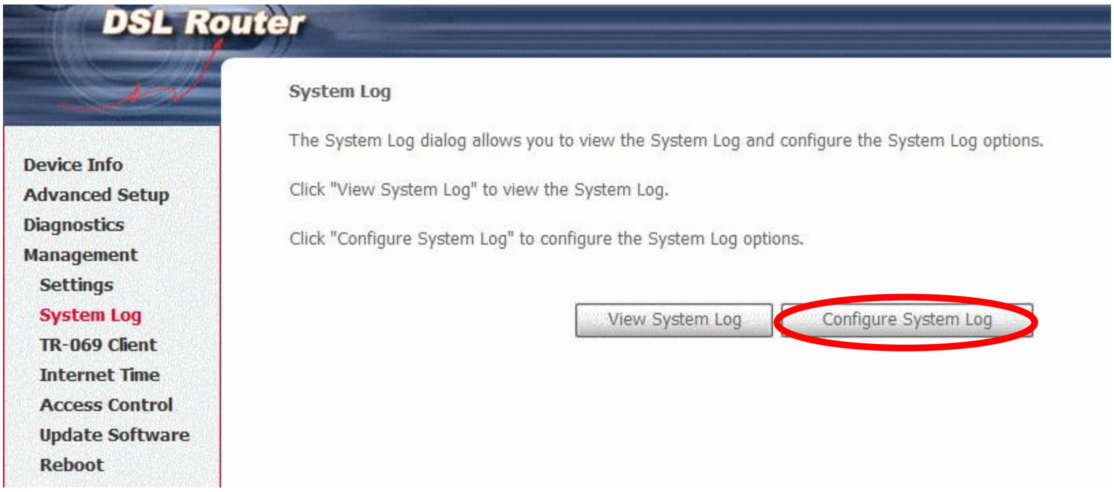
NOTE: This entry has the same effect as the **Reset** button. The Proscend 140 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

8.2 System Log

This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

STEP 1: Click **Configure System Log**.



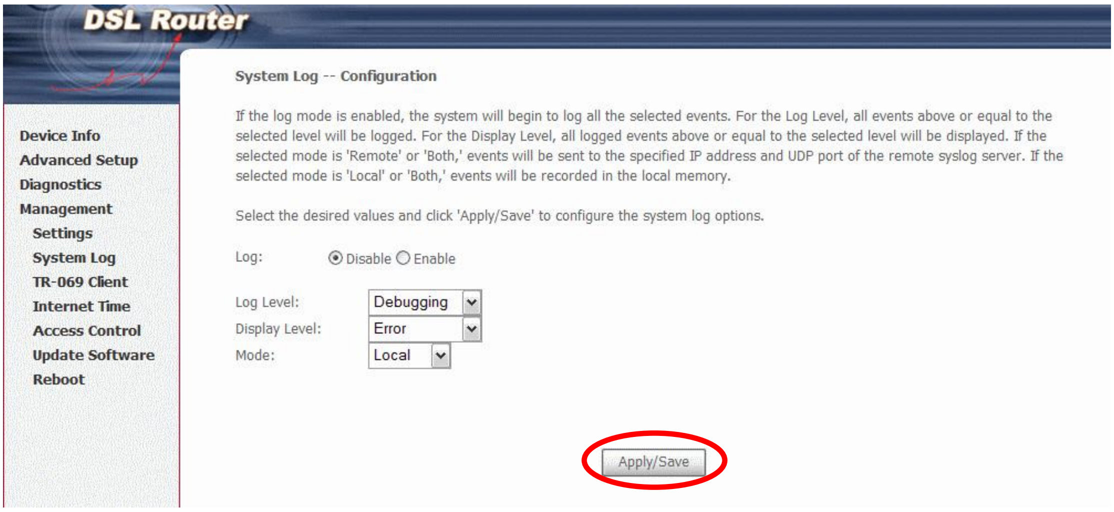
System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

STEP 2: Select desired options and click **Apply/Save**.



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

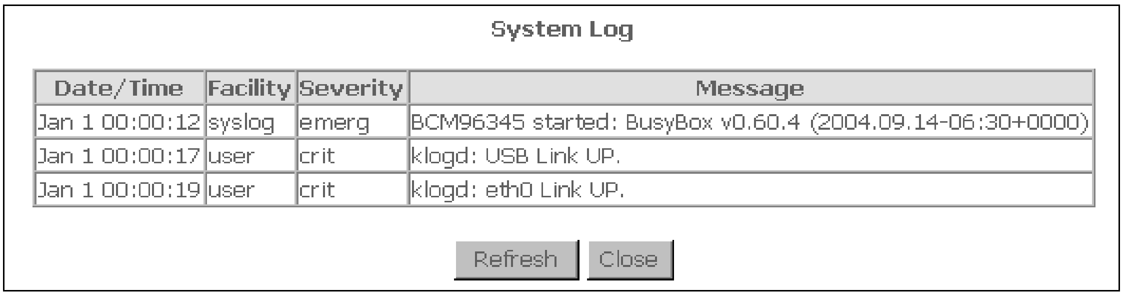
Log: ● Disable ○ Enable

Log Level: Debugging
Display Level: Error
Mode: Local

Consult the table below for detailed descriptions of each system log option.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the **Enable** radio button and then click **Apply/Save**.
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the device's SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both modes is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

STEP 3: Click **View System Log**. The results are displayed as follows.

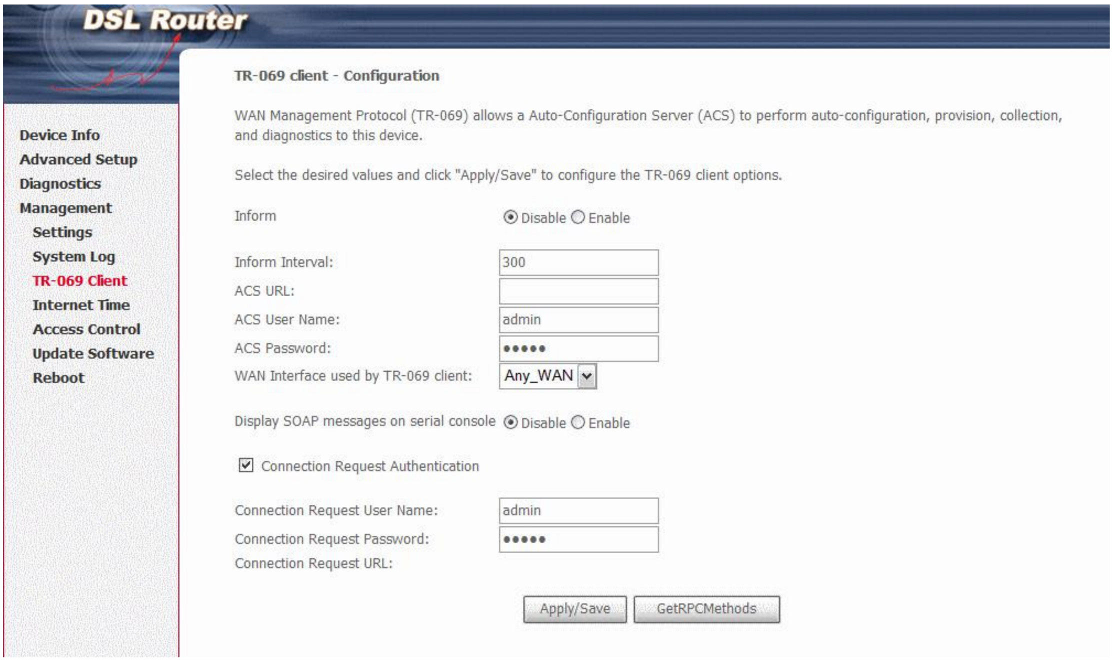


System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:12	syslog	emerg	BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0000)
Jan 1 00:00:17	user	crit	klogd: USB Link UP.
Jan 1 00:00:19	user	crit	klogd: eth0 Link UP.

8.3 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.



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: 300

ACS URL:

ACS User Name: admin

ACS Password: •••••

WAN Interface used by TR-069 client: Any_WAN

Display SOAP messages on serial console ● Disable ○ Enable

☑ Connection Request Authentication

Connection Request User Name: admin

Connection Request Password: •••••

Connection Request URL:

The table below is provided for ease of reference.

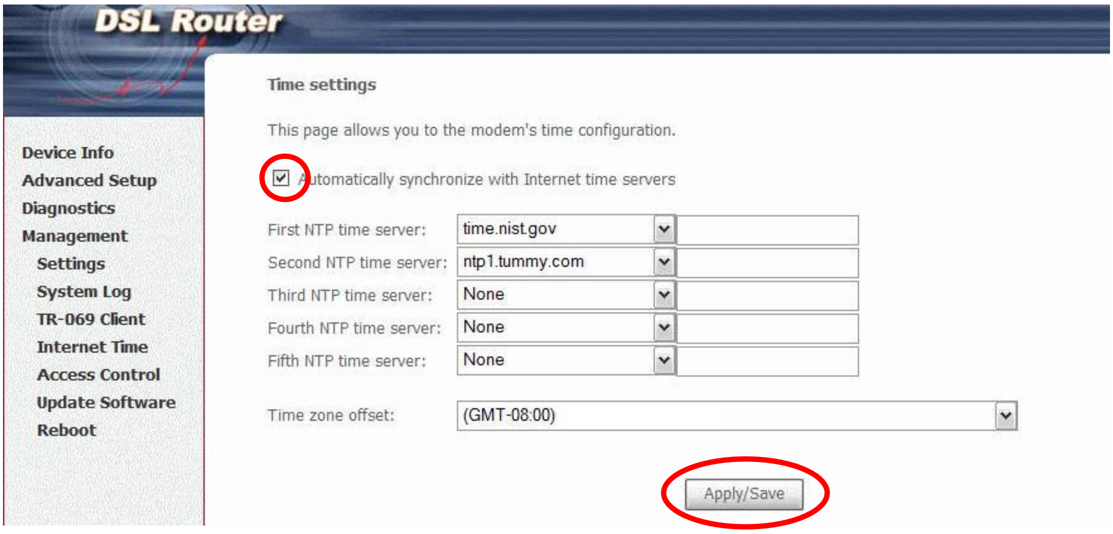
Option	**Description**
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.

Option	Description
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Display SOAP messages on serial console	Enable/Disable SOAP messages on serial console. This option is used for advanced troubleshooting of the device.
Connection Request	
Authorization	Tick the checkbox ☑ to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to Proscend 140.

The **Get RPC Methods** button forces the CPE to establish an immediate connection to the ACS. This may be used to discover the set of methods supported by the ACS or CPE. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods.

8.4 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox ☑, choose your preferred time server(s), select the correct time zone offset, and click **Save/Apply**.



Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server:	time.nist.gov
Second NTP time server:	ntp1.tummy.com
Third NTP time server:	None
Fourth NTP time server:	None
Fifth NTP time server:	None
Time zone offset:	(GMT-08:00)

NOTE: Internet Time must be activated to use Parental Control.
In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

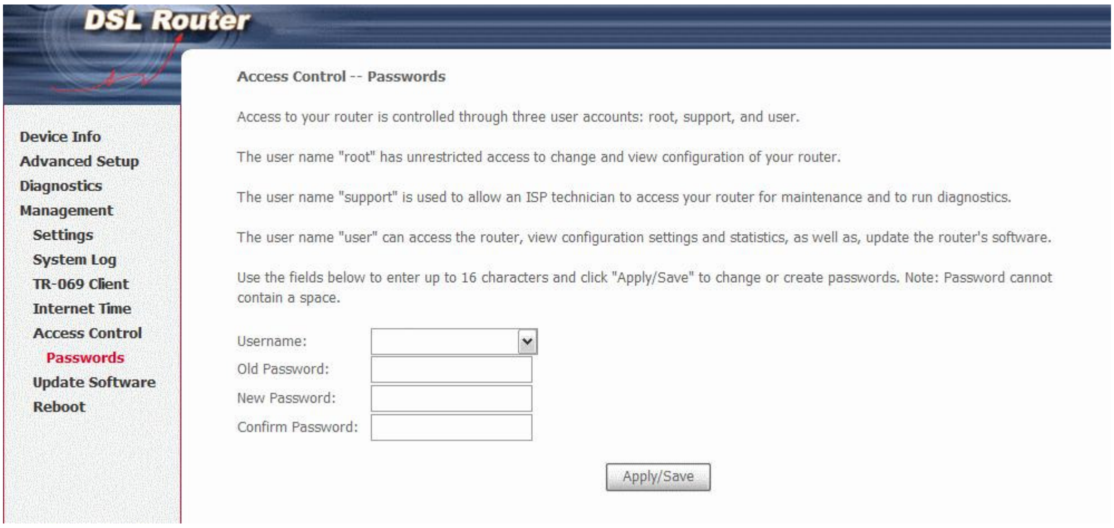
8.5 Access Control

8.5.1 Passwords

This screen is used to configure the user account access passwords for the device. Access to the Proscend 140 is controlled through the following three user accounts:

- **root** - unrestricted access to change and view the configuration.
- **support** - used for remote maintenance and diagnostics of the router
- **user** - can view configuration settings & statistics and update firmware.

Use the fields below to change password settings. Click **Save/Apply** to continue.



Access Control -- Passwords

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

The user name "root" has unrestricted access to change and view configuration of your router.

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

The user name "user" can access the 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.

Username:

Old Password:

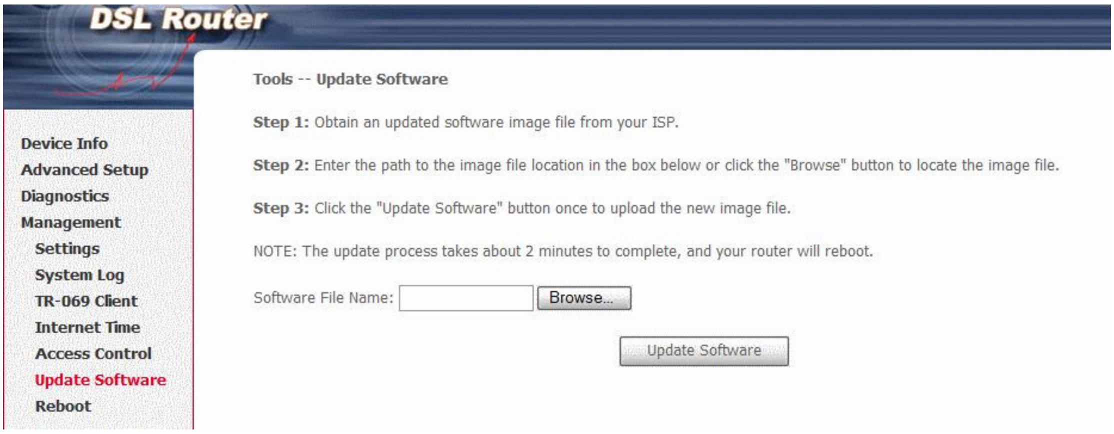
New Password:

Confirm Password:

NOTE: Passwords can be up to 16 characters in length.

8.6 Update Software

This option allows for firmware upgrades from a locally stored file.



Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your router will reboot.

Software File Name:

STEP 1: Obtain an updated software image file from your ISP.

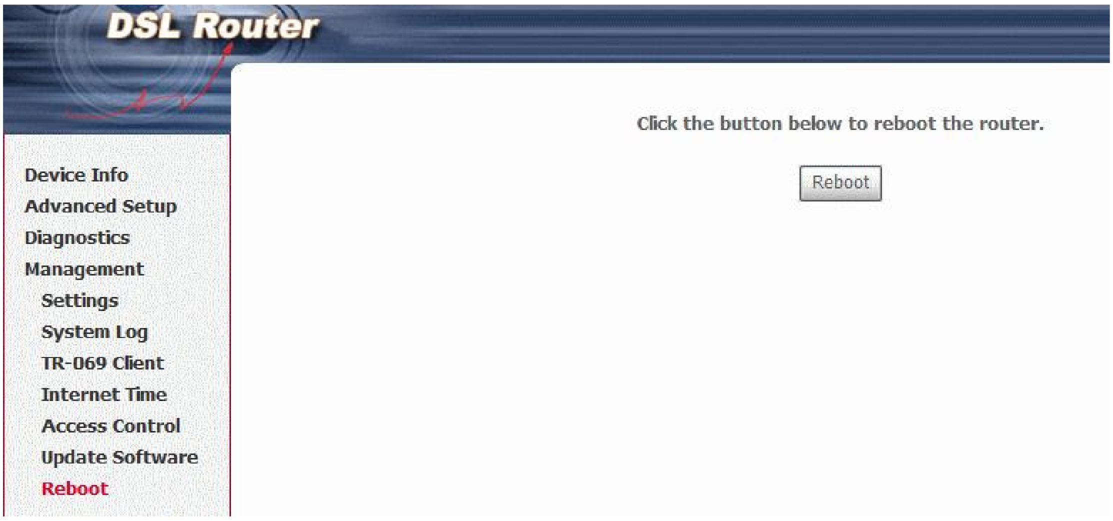
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 3: Click the **Update Software** button once to upload and install the file.

NOTE: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the Device Information screen with the firmware version installed, to confirm the installation was successful.

8.7 Reboot

To save the current configuration and reboot the router, click **Save/Reboot**.



Click the button below to reboot the router.

NOTE: You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

Appendix A - Firewall

STATEFUL PACKET INSPECTION

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

DENIAL OF SERVICE ATTACK

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER

These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER

Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

Example 1:	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source IP address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Dest. IP Address	: NA
	Dest. Subnet Mask	: NA
	Dest. Port	: NA

This filter will Drop all TCP packets coming from the LAN with IP Address/Subnet Mask of 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:	Filter Name	: Out_Filter2
	Protocol	: UDP
	Source IP Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0

Source Port	: 5060:6060
Dest. IP Address	: 172.16.13.4
Dest. Subnet Mask	: 255.255.255.0
Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from the LAN with IP Address / Subnet Mask of 192.168.1.45/24 and a source port range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port range of 6060 to 7070.

INCOMING IP FILTER

Helps in setting rules to Allow or Deny packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, specific packet types coming from the WAN can be Accepted.

Example 1:	Filter Name	: In_Filter1
	Protocol	: TCP
	Policy	: Allow
	Source IP Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 80
	Dest. IP Address	: NA
	Dest. Subnet Mask	: NA
	Dest. Port	: NA
	Selected WAN interface	: br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:	Filter Name	: In_Filter2
	Protocol	: UDP
	Policy	: Allow
	Source IP Address	: 210.168.219.45
	Source Subnet Mask	: 255.255.0.0
	Source Port	: 5060:6060
	Dest. IP Address	: 192.168.1.45
	Dest. Sub. Mask	: 255.255.255.0
	Dest. Port	: 6060:7070
	Selected WAN interface	: br0

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in Bridge mode. After a Bridge mode connection is created, navigate to Advanced Setup → Security → MAC Filtering in the WUI.

Example 1:	Global Policy	: Forwarded
	Protocol Type	: PPPoE
	Dest. MAC Address	: 00:12:34:56:78:90
	Source MAC Address	: NA
	Src. Interface	: eth1
	Dest. Interface	: eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:	Global Policy	: Blocked
	Protocol Type	: PPPoE
	Dest. MAC Address	: 00:12:34:56:78:90
	Source MAC Address	: 00:34:12:78:90:56
	Src. Interface	: eth1
	Dest. Interface	: eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. All other frames on this interface are dropped.

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the Proscend 140, as per chosen days of the week and the chosen times.

Example:	User Name	: FilterJohn
	Browser's MAC Address	: 00:29:46:78:63:21
	Days of the Week	: Mon, Wed, Fri

Start Blocking Time	: 14:00
End Blocking Time	: 18:00

With this rule, a LAN device with MAC Address of 00:29:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix B - Pin Assignments

ETHERNET Ports (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix C - Specifications

Hardware Interface

RJ-11 X 1 for ADSL2+/VDSL2, RJ-45 X 4 for LAN (10/100 Base-T), Reset Button X 1, Power Switch X 1

WAN Interface

ADSL2+ ....Downstream : 24 Mbps   Upstream : 1.3 Mbps
ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, AnnexM

VDSL2 ....Downstream : 100 Mbps   Upstream : 60 Mbps
ITU-T G.993.2 (supporting profile 8a, 8b, 8c, 8d, 12a, 12b, 17a)

LAN Interface

Standard......................IEEE 802.3, IEEE 802.3u
10/100 BaseT ....Auto-sense
MDI/MDIX support ....Yes

ATM Attributes

RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE);
RFC 2364 (PPPoA); RFC 1577 (IPoA)

PVCs 16
AAL type AAL5
ATM service class ....UBR/CBR/VBR
ATM UNI support...........UNI 3.1/4.0
OAM F4/F5 ....Yes

Management

Compliant with TR-069/TR-098/TR-104/TR-111 remote management protocols, Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP / TFTP / FTP server

Bridge Functions

Transparent bridging and learning ....IEEE 802.1d
VLAN support ....Yes
Spanning Tree Algorithm ....Yes
IGMP Snooping ....Yes

Routing Functions

Static route, RIP v1/v2, NAT/PAT, DMZ, DHCP Server/Relay/Client, DNS Proxy, ARP, IGMP Proxy

Security Functions

Authentication protocol : PAP, CHAP

TCP/IP/Port filtering rules, Port Triggering/Forwarding, Packet and MAC address filtering, Access Control, DoS Protection, SSH, VPN Pass through

QoS .... L3 policy-based QoS, IP QoS, ToS

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box

Power Supply ....Input: 100 - 240 Vac
Output: 12 Vdc / 1.5 A

Environment Condition

Operating temperature ....0 ~ 50 degrees Celsius

Relative humidity ....5 ~ 95% (non-condensing)

Dimensions ....205 mm (W) x 48 mm (H) x 145 mm (D)

Kit Weight

(1*Proscend 140, 1* RJ-11 cable, 1* RJ-45 cable, 1* Power Adapter, 1* CD-ROM) = 0.7 kg

NOTE: Specifications are subject to change without notice

Appendix D - SSH Client

Unlike Microsoft Windows, Linux OS has a ssh client included. For Windows users, there is a public domain one called "putty" that can be downloaded from here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the ssh client you must first enable SSH access for the LAN or WAN from the Management → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

For WAN access, type: ssh -l support *WAN IP address*

To access the router using the Windows "putty" ssh client

For LAN access, type: putty -ssh -l root 192.168.1.1

For WAN access, type: putty -ssh -l support *WAN IP address*

NOTE: The *WAN IP address* can be found on the Device Info → WAN screen

Appendix E - Connection Setup

Creating a WAN connection is a two-stage process.

1 - Setup a Layer 2 Interface (ATM or PTM).
2 - Add a WAN connection to the Layer 2 Interface.

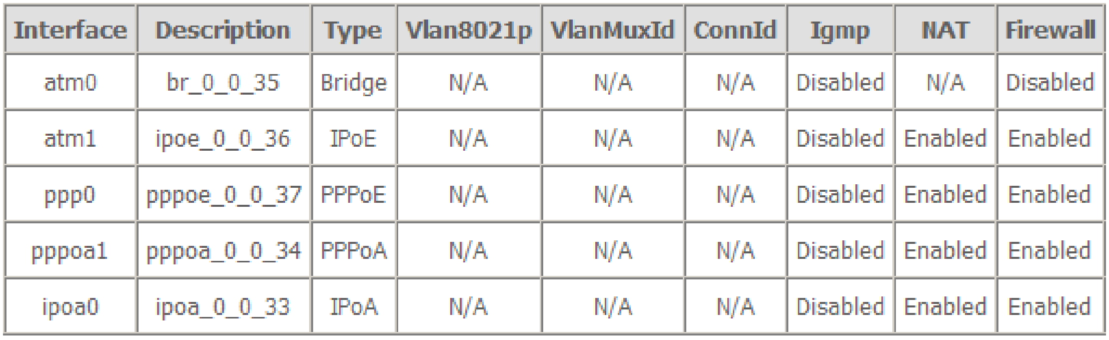
The following sections describe each stage in turn.

E1 ~ Layer 2 Interfaces

Every layer2 interface operates in one of three modes: Default, VLAN Mux or MSC. A short introduction to each of these three modes is included below for reference. It is important to understand the differences between these connection modes, as they determine the number and types of connections that may be configured.

DEFAULT MODE

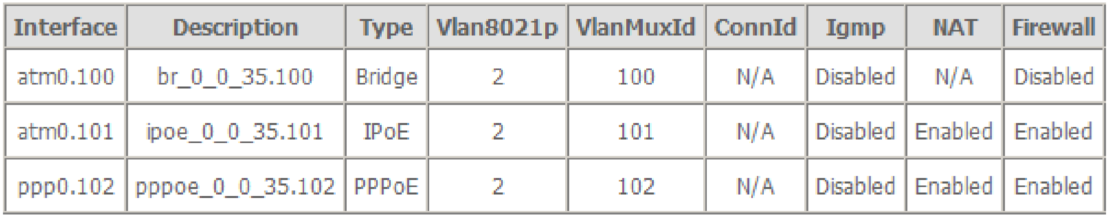
In this mode there is a 1:1 relationship between interfaces and WAN connections, in that an interface in default mode supports just one connection. However, unlike the multiple connection modes described below, it supports all five connection types. The figure below shows the five connection types available in ATM default mode.



Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall
atm0	br_0_0_35	Bridge	N/A	N/A	N/A	Disabled	N/A	Disabled
atm1	ipoe_0_0_36	IPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled
ppp0	pppoe_0_0_37	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled
pppoa1	pppoa_0_0_34	PPPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled
ipoa0	ipoa_0_0_33	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled

VLAN MUX MODE

This mode uses VLAN tags to allow for multiple connections over a single interface. PPPoE, IPoE, and Bridge are supported while PPPoA and IPoA connections are not. The figure below shows multiple connections over a single VLAN Mux interface.



Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall
atm0.100	br_0_0_35.100	Bridge	2	100	N/A	Disabled	N/A	Disabled
atm0.101	ipoe_0_0_35.101	IPoE	2	101	N/A	Disabled	Enabled	Enabled
ppp0.102	pppoe_0_0_35.102	PPPoE	2	102	N/A	Disabled	Enabled	Enabled

MSC MODE

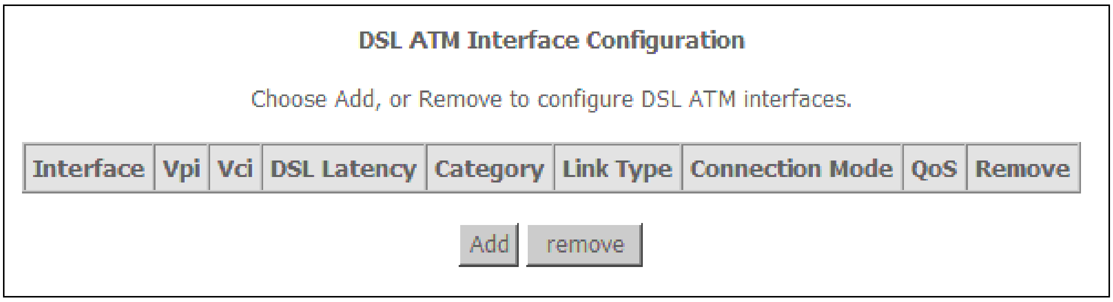
Multi-Service Connection (MSC) mode supports multiple connections over a single interface. As with VLAN Mux mode, PPPoA and IPoA connection types are not supported. After adding WAN connections to an interface, you must also create an Interface Group to connect LAN/WAN interfaces (see section E3 ~ More About MSC Mode).

E1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE: The Proscend 140 supports up to 16 ATM interfaces.

STEP 1: Go to Advanced Setup → Layer2 Interface → ATM Interface.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

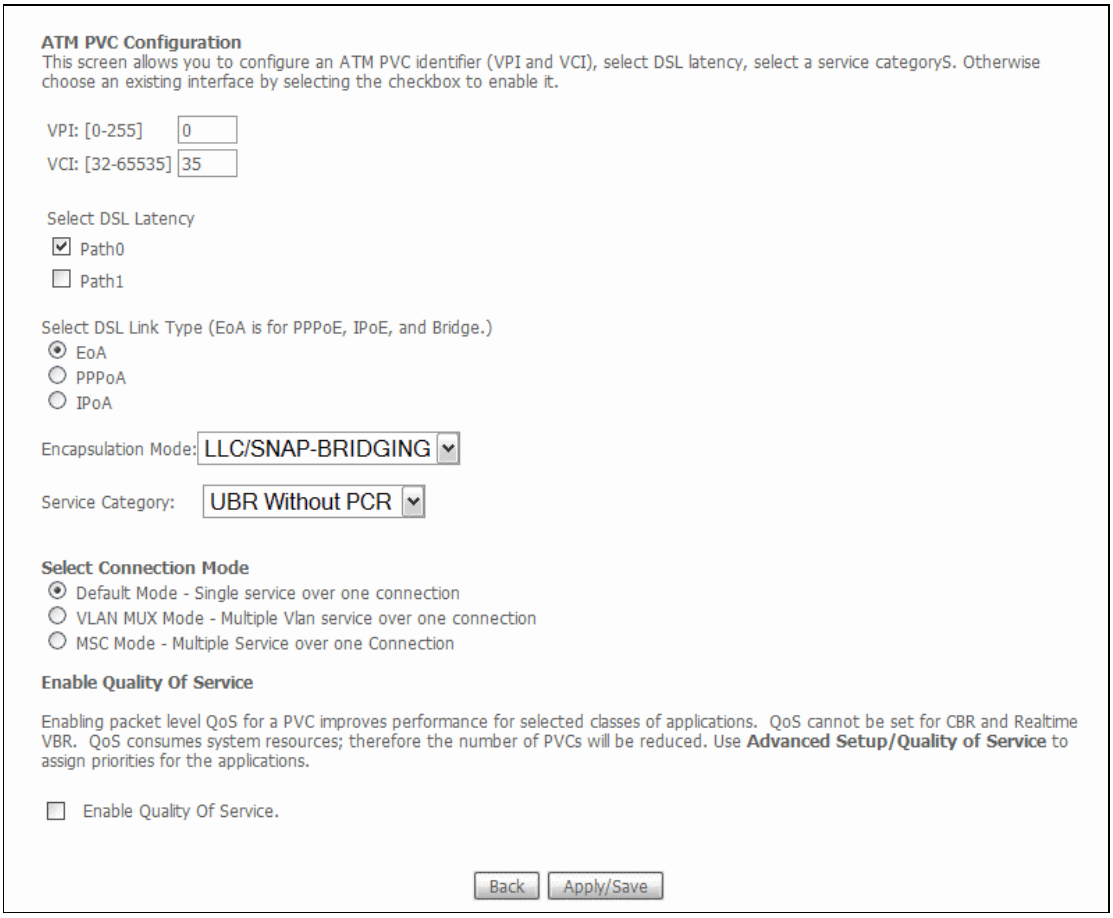
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove

This table is provided here for ease of reference.

Heading	**Description**
Interface	WAN interface name.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	ATM service category
Link Type	Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA.
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection MSC Mode – Multiple Service over one Connection
QoS	Quality of Service (QoS) status
Remove	Select items for removal

STEP 2: Click **Add** to proceed to the next screen.

NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]	0
VCI: [32-65535]	35

Select DSL Latency

☑ Path0

□ Path1

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 Connection Mode

● Default Mode - Single service over one connection

○ VLAN MUX Mode - Multiple Vlan service over one connection

○ MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

□ Enable Quality Of Service.

There are many settings here including: VPI/VCI, DSL Latency, DSL Link Type, Encapsulation Mode, Service Category, Connection Mode and Quality of Service.

The table below shows ADSL Link Type availability with each Connection Mode.

	ADSL Link Type		
Connection Mode	EoA*	PPPoA	IPoA
Default Mode	OK	OK	OK
VLAN Mux Mode	OK	X	X
MSC Mode	OK	X	X

* EoA includes PPPoE, IPoE, and Bridge link types.

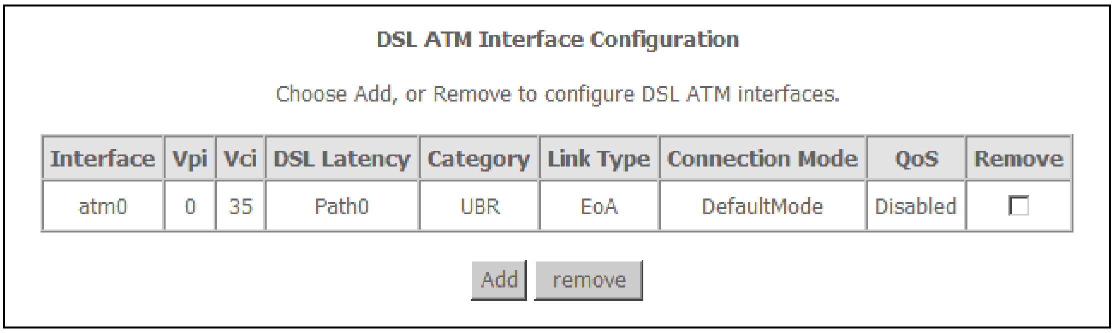
Here are the available encapsulations for each xDSL Link Type:

- EoA- LLC/SNAP-BRIDGING, VC/MUX

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- IPoA- LLC/SNAP-ROUTING, VC MUX

STEP 3: Click **Apply/Save** to confirm your choices.

On the next screen, check that the ATM interface is added to the list. For example, an ATM interface on PVC 0/35 in Default Mode with an EoA Link type is shown below.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Disabled	□

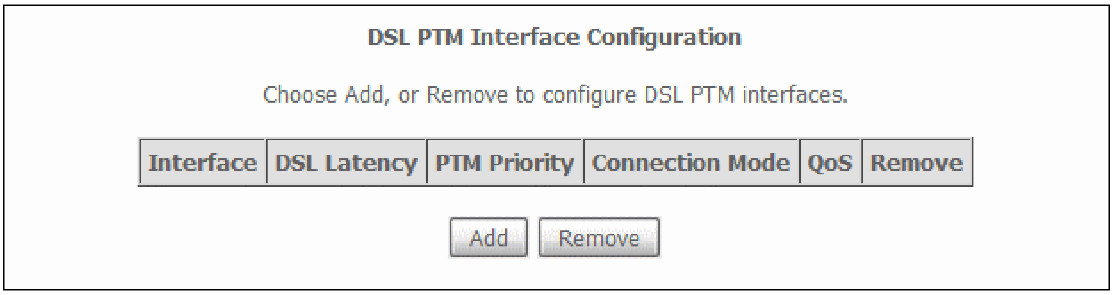
To add a WAN connection go to section E2 ~ WAN Connections.

E1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

NOTE: The Proscend 140 supports up to four PTM interfaces.

STEP 4: Go to Advanced Setup → Layer2 Interface → PTM Interface.



DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

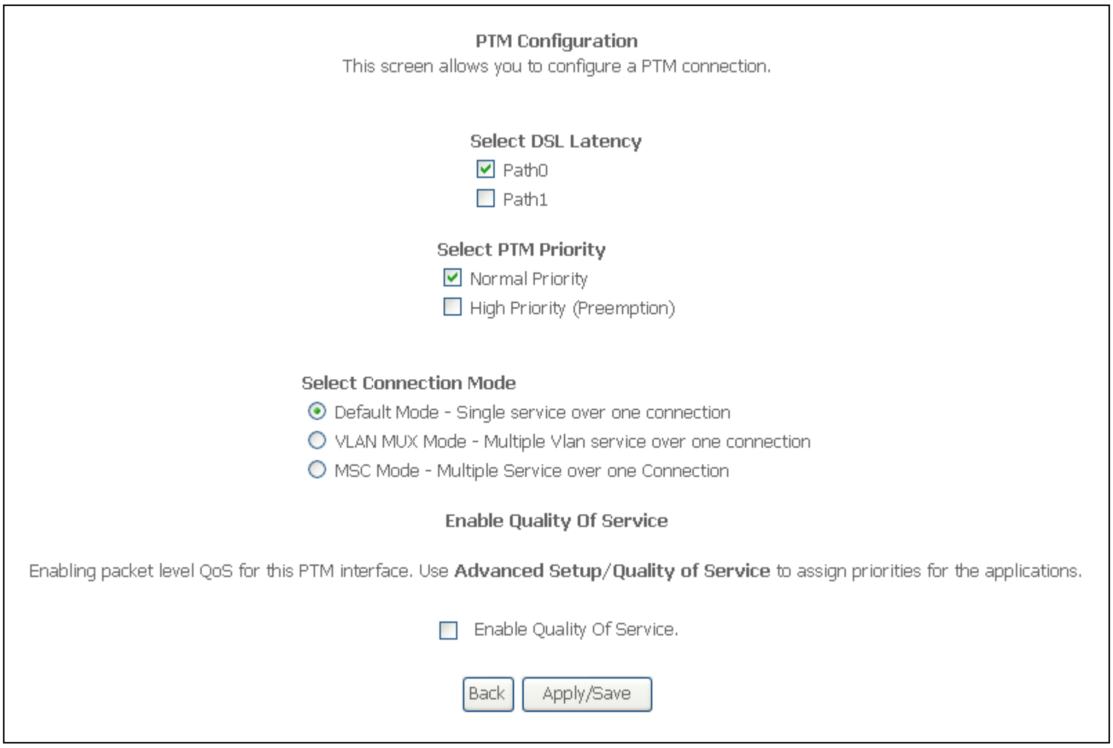
Interface	DSL Latency	PTM Priority	Connection Mode	QoS	Remove

This table is provided here for ease of reference.

Heading	**Description**
Interface	WAN interface name.
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
PTM Priority	Normal or High Priority (Preemption).
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface. MSC Mode – Multiple Services over one interface.
QoS	Quality of Service (QoS) status.
Remove	Select interfaces to remove.

STEP 5: Click **Add** to proceed to the next screen.

NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.



PTM Configuration

This screen allows you to configure a PTM connection.

Select DSL Latency

☑ Path0

□ Path1

Select PTM Priority

☑ Normal Priority

□ High Priority (Preemption)

Select Connection Mode

● Default Mode - Single service over one connection

○ VLAN MUX Mode - Multiple Vlan service over one connection

○ MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for this PTM interface. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

□ Enable Quality Of Service.

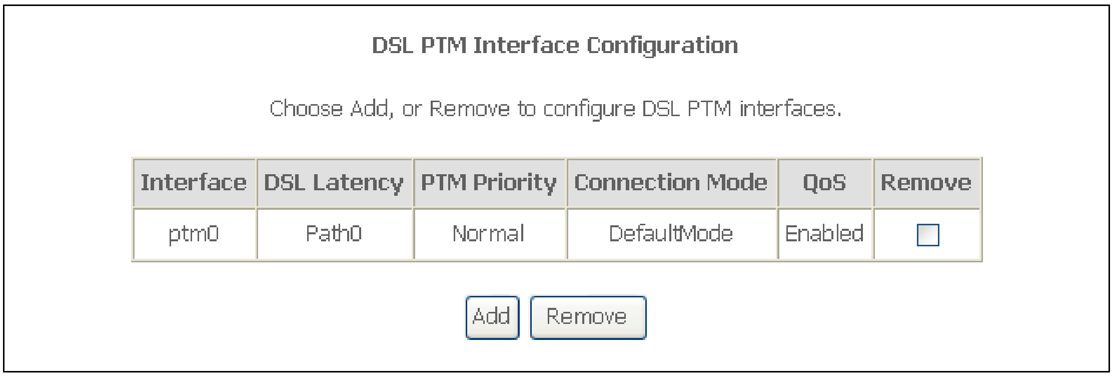
There are many settings that can be configured here including:

DSL Latency, PTM Priority, Connection Mode and Quality of Service.

STEP 6: Click **Apply/Save** to confirm your choices.

On the next screen, check that the PTM interface is added to the list.

For example, an PTM interface in Default Mode is shown below.



DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Connection Mode	QoS	Remove
ptm0	Path0	Normal	DefaultMode	Enabled	□

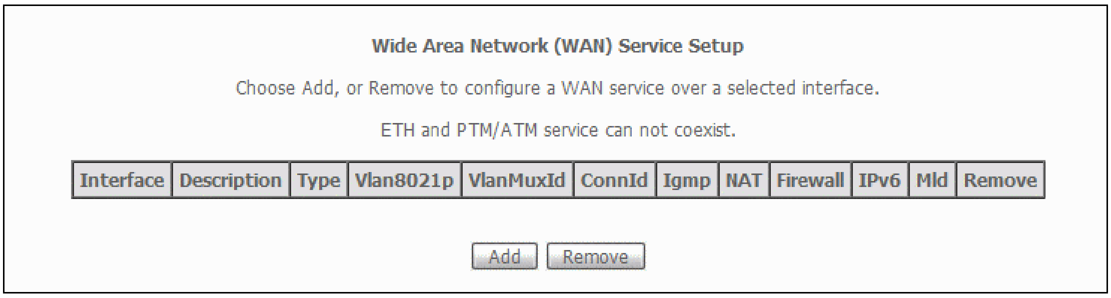
To add a WAN connection go to section E2 ~ WAN Connections.

E2 ~ WAN Connections

In Default Mode, the Proscend 140 supports one WAN connection for each interface, up to a maximum of 8 connections. VLAN Mux and MSC support up to 16 connections.

To setup a WAN connection follow these instructions.

STEP 1: Go to the Advanced Setup → WAN Service screen.



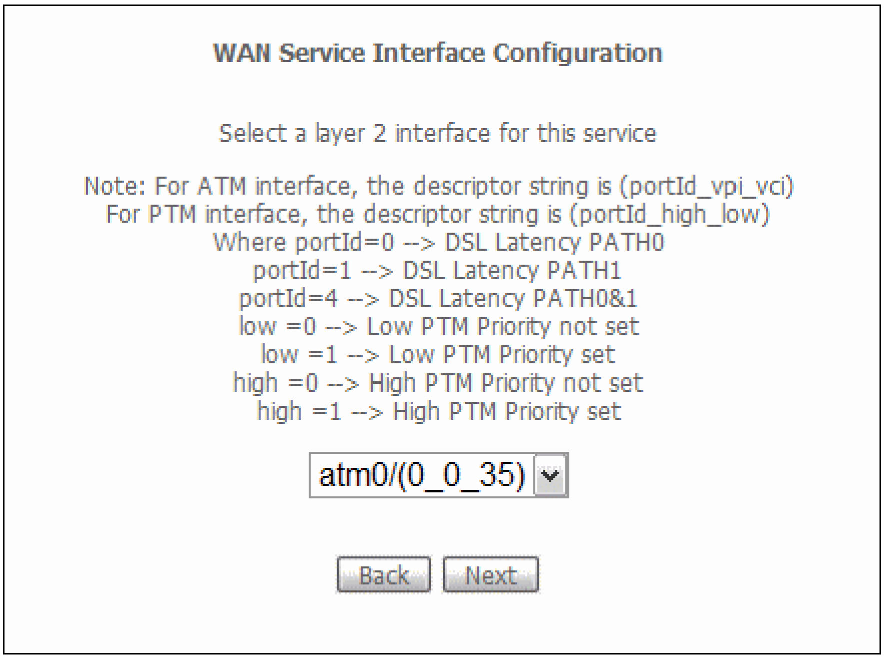
Wide Area Network (WAN) Service Setup

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

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Mld	Remove

STEP 2: Click **Add** to create a WAN connection. The following screen will display.



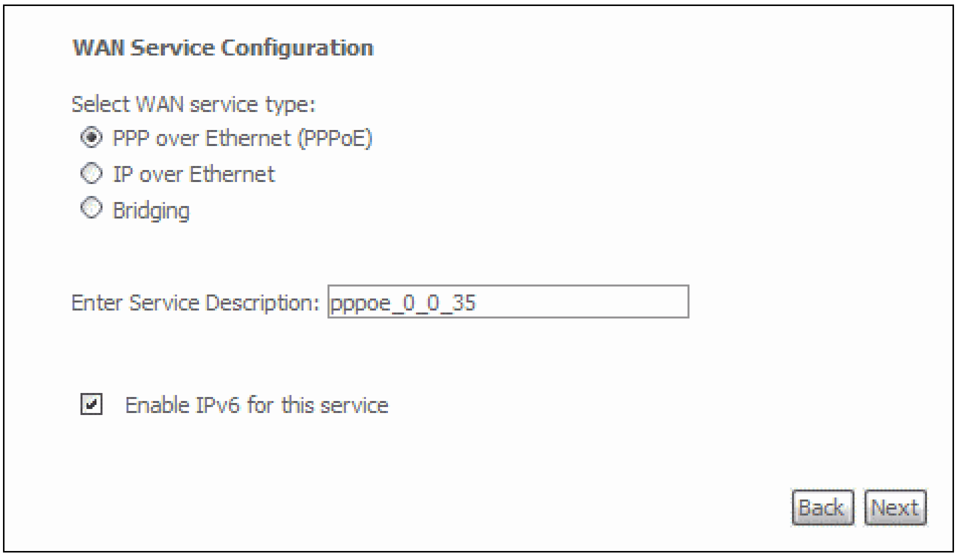
WAN Service Interface Configuration

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
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
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)

STEP 3: Choose a layer 2 interface from the drop-down box and click **Next**. The WAN Service Configuration screen will display as shown below.



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)

○ IP over Ethernet

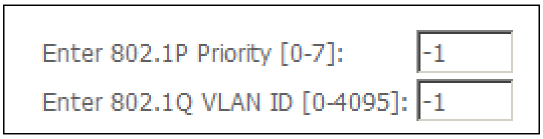
○ Bridging

Enter Service Description: pppoe_0_0_35

☑ Enable IPv6 for this service

NOTE: The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the **Back** button and select a different layer 2 interface.

STEP 4: For VLAN Mux Connections only, you must enter Priority & VLAN ID tags.



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

Enter 802.1Q VLAN ID [0-4095]: -1

STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) PPP over ETHERNET (PPPoE)

(2) IP over ETHERNET (IPoE)

(3) Bridging

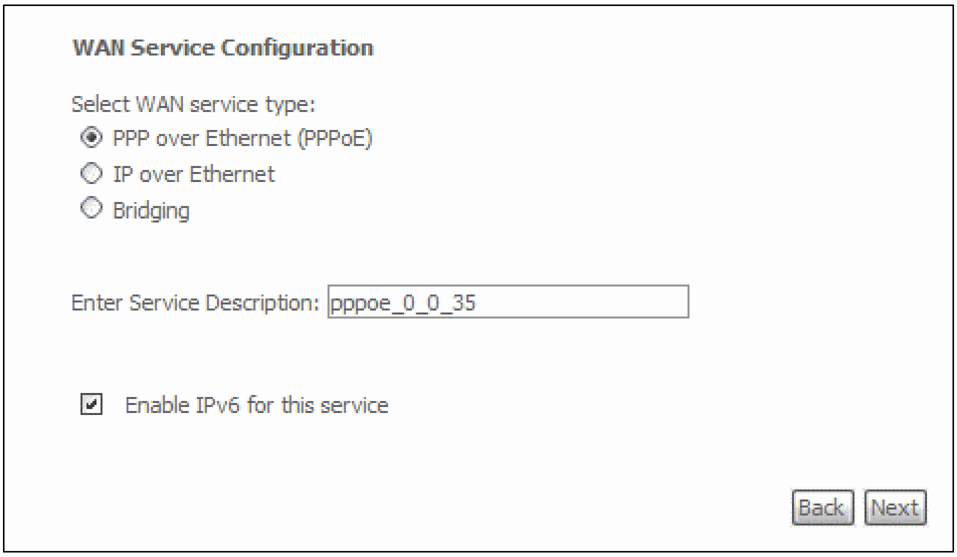
(4) PPP over ATM (PPPoA)

(5) IP over ATM (IPoA)

The subsections that follow continue the WAN service setup procedure.

E2.1 PPP over ETHERNET (PPPoE)

STEP 1: Select the PPP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.



WAN Service Configuration

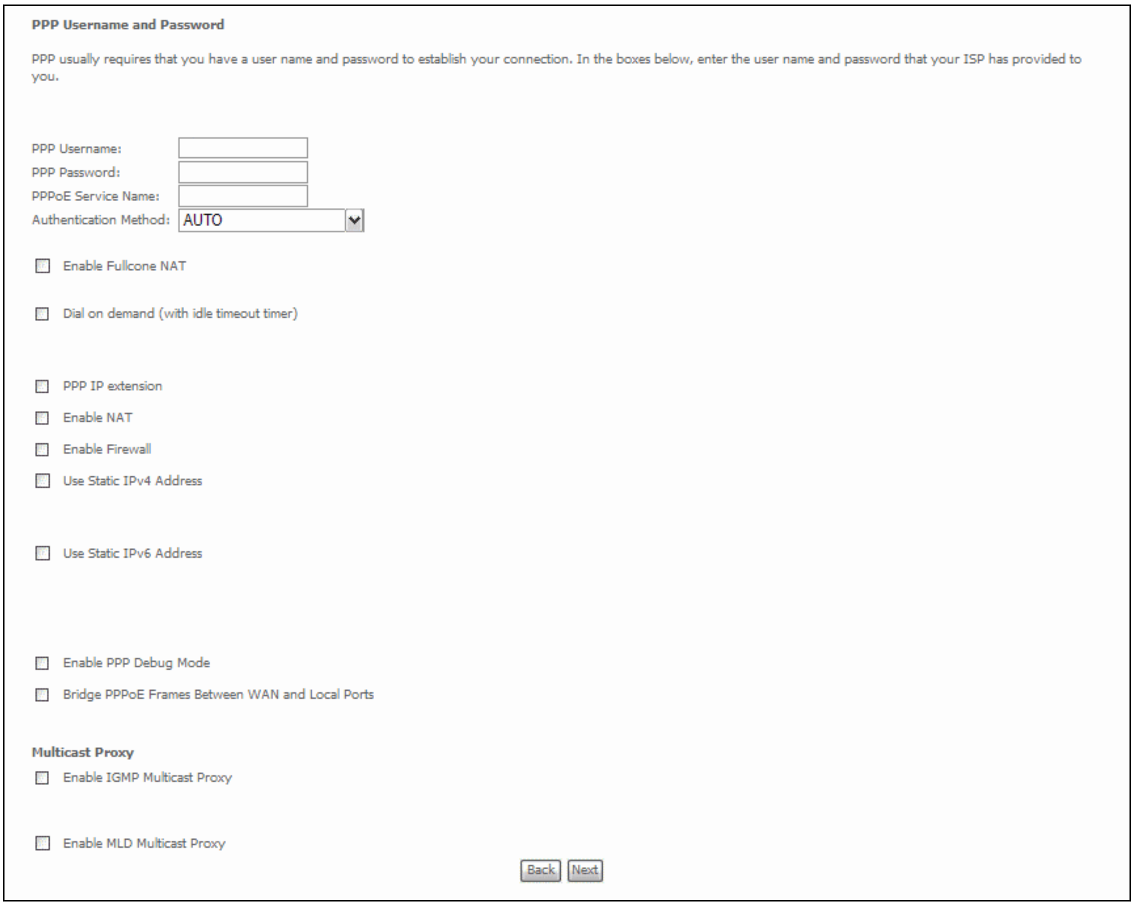
Select WAN service type:

● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_0_35

☑ Enable IPv6 for this service

STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.



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

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Enable NAT

□ Enable Firewall

□ Use Static IPv4 Address

□ Use Static IPv6 Address

□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

□ Enable MLD Multicast Proxy

The settings shown above are described below.

PPP SETTINGS

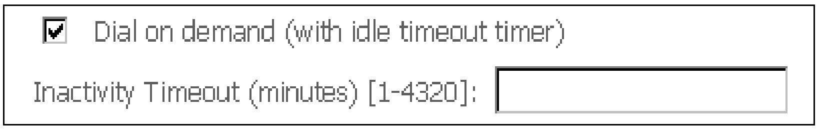
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND

The Proscend 140 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv4 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2.

USE STATIC IPv6 ADDRESS

This option displays when IPv6 is enabled. Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv6 Address** field along with a value for **Prefix Length**. Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2.

ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS

(This option is hidden when PPP IP Extension is enabled)

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The Proscend 140 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

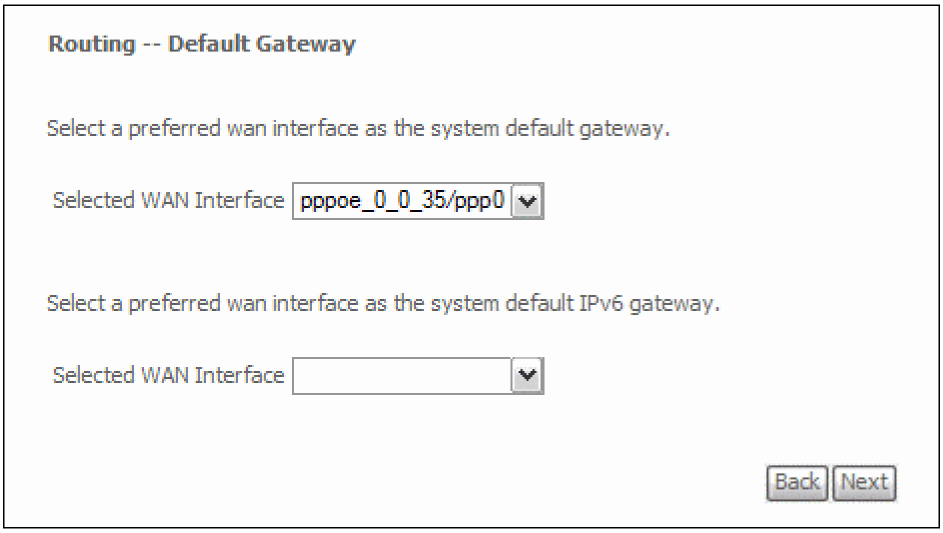
ENABLE IGMP MULTICAST PROXY

Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

ENABLE MLD MULTICAST PROXY

This option displays when IPv6 is enabled. Tick the checkbox ☑ to enable Multicast Listener Discovery (MLD). This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

STEP 3: Select WAN interfaces as system default IPv4/v6 gateways. When IPv6 is enabled a second WAN interface selection box will appear, as shown here.



Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: pppoe_0_0_35/ppp0

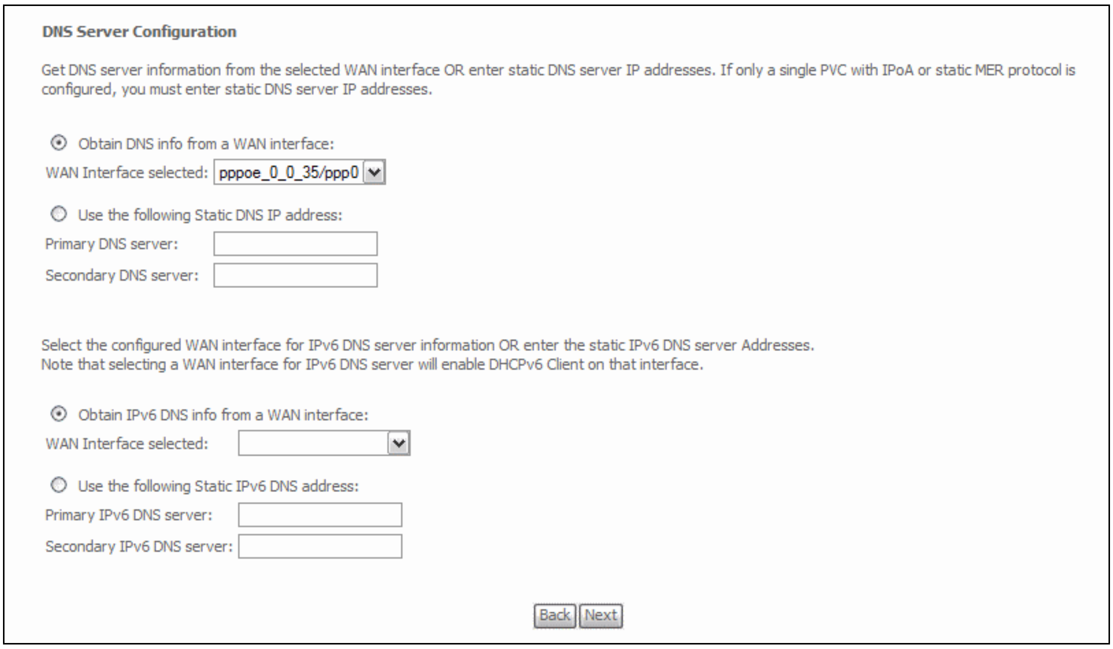
Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface:

Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select a WAN interface or enter static IP address to IPv4/v6 DNS Servers.

When IPv6 is enabled, a second set of entries will appear, as shown here.



DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoe_0_0_35/ppp0

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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:

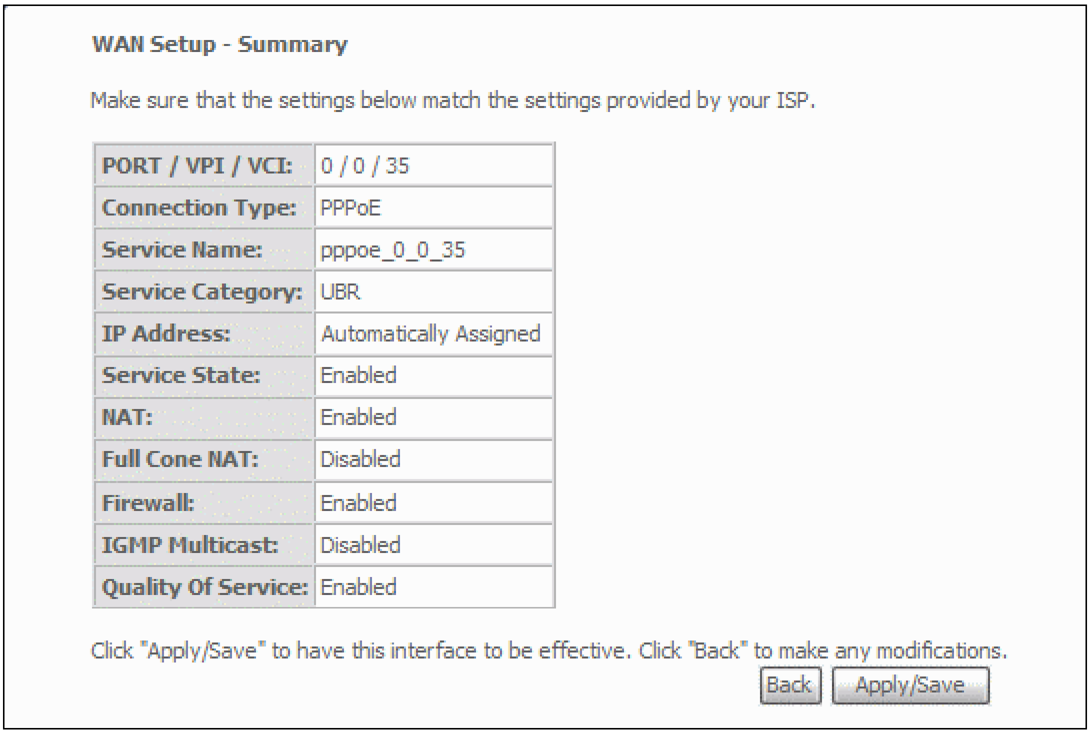
○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

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

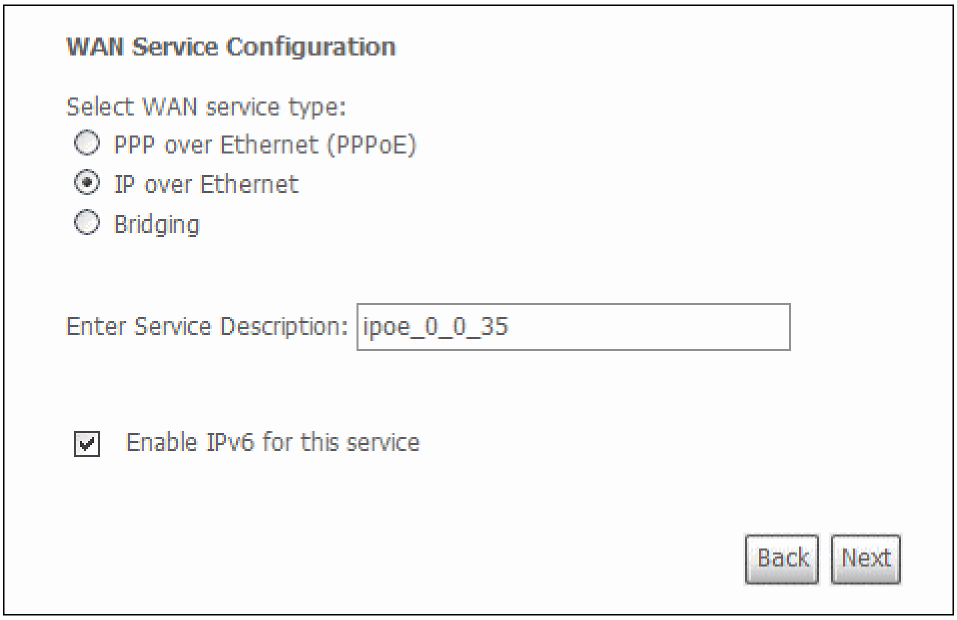
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

E2.2 IP over ETHERNET (IPoE)

STEP 1: Select the IP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.



WAN Service Configuration

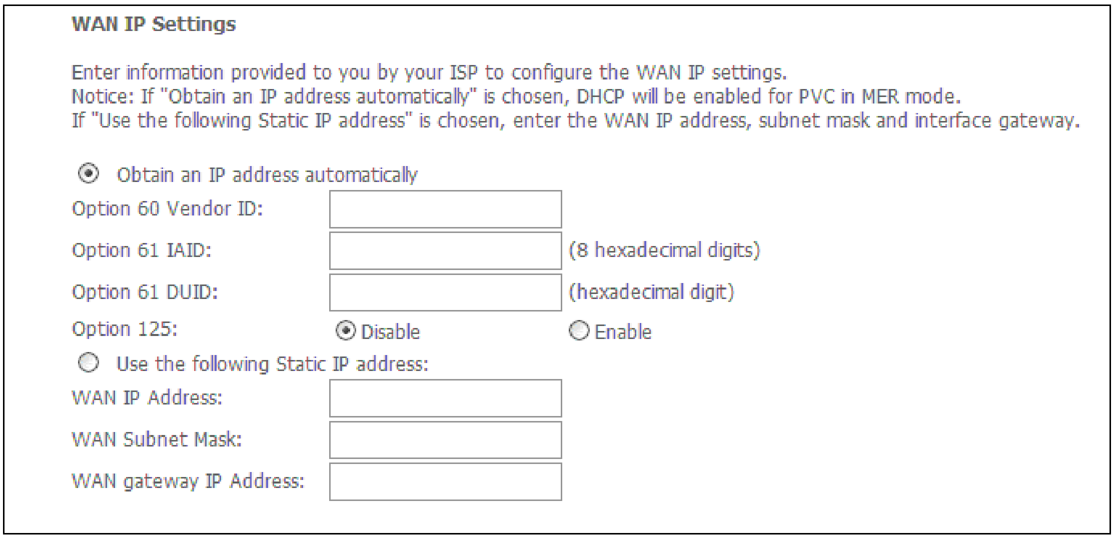
Select WAN service type:

○ PPP over Ethernet (PPPoE)
● IP over Ethernet
○ Bridging

Enter Service Description: ipoe_0_0_35

☑ Enable IPv6 for this service

STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can instead use the **Static IP address** method to assign WAN IP address, Subnet Mask and Default Gateway manually.



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

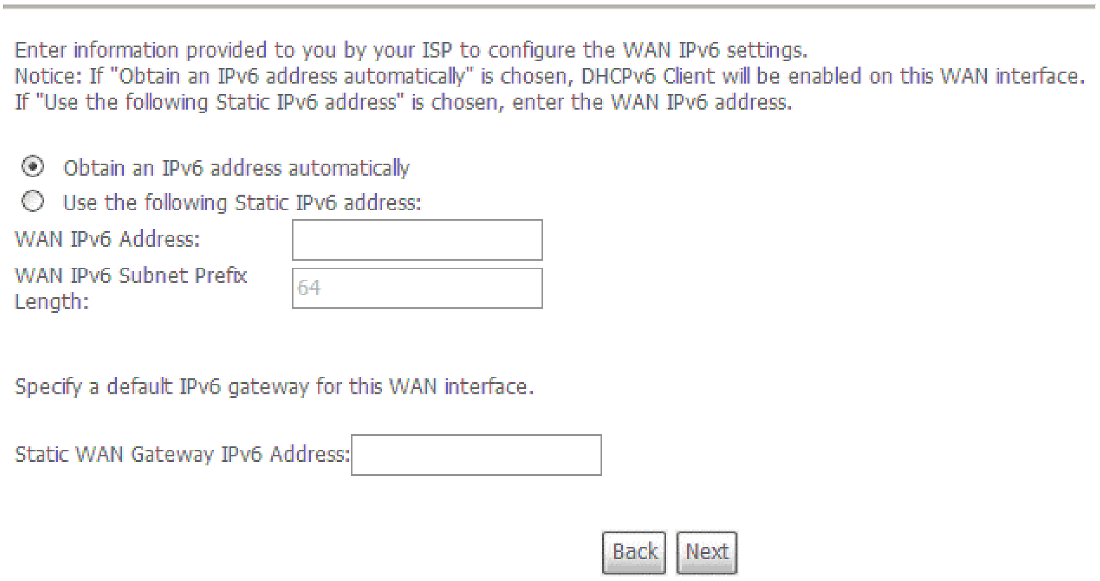
● Obtain an IP address automatically

Option 60 Vendor ID:		
Option 61 IAID:		(8 hexadecimal digits)
Option 61 DUID:		(hexadecimal digit)
Option 125:	● Disable	○ Enable

○ Use the following Static IP address:

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

NOTE: If IPv6 networking is enabled, an additional set of instructions, radio buttons, and text entry boxes will appear at the bottom of the screen. These configuration options are quite similar to those for IPv4 networks.



Enter information provided to you by your ISP to configure the WAN IPv6 settings.
Notice: If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
If "Use the following Static IPv6 address" is chosen, enter the WAN IPv6 address.

● Obtain an IPv6 address automatically
○ Use the following Static IPv6 address:

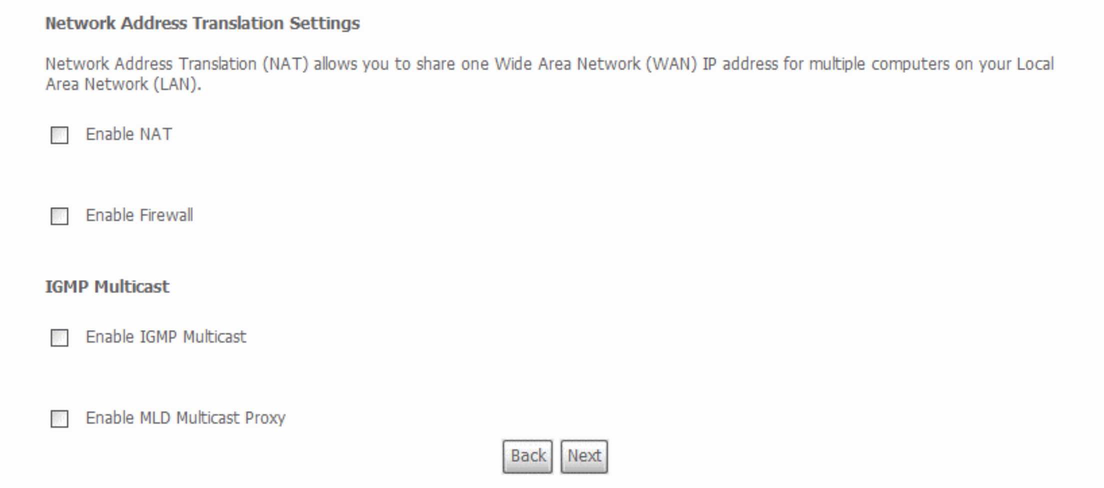
WAN IPv6 Address:
WAN IPv6 Subnet Prefix Length: 64

Specify a default IPv6 gateway for this WAN interface.

Static WAN Gateway IPv6 Address:

Click **Next** to continue or click **Back** to return to the previous step.

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.



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

□ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast

□ Enable MLD Multicast Proxy

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

ENABLE FIREWALL

If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

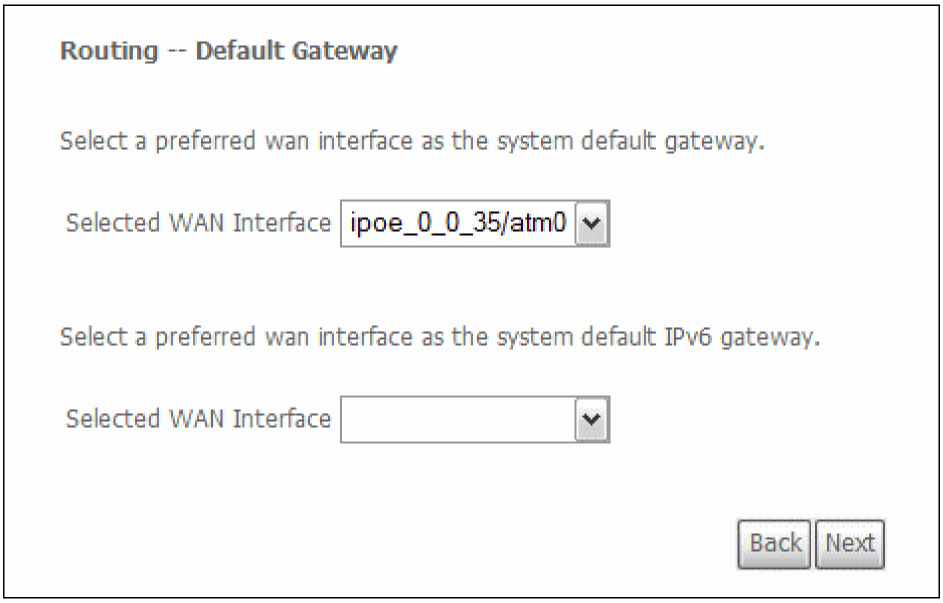
ENABLE IGMP MULTICAST

Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

ENABLE MLD MULTICAST PROXY

This option displayed when IPv6 is enabled. Tick the checkbox ☑ to enable Multicast Listener Discovery (MLD). This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

STEP 4: Select WAN interfaces as system default IPv4/v6 gateways. When IPv6 is enabled a second WAN interface selection box will appear, as shown here.



Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

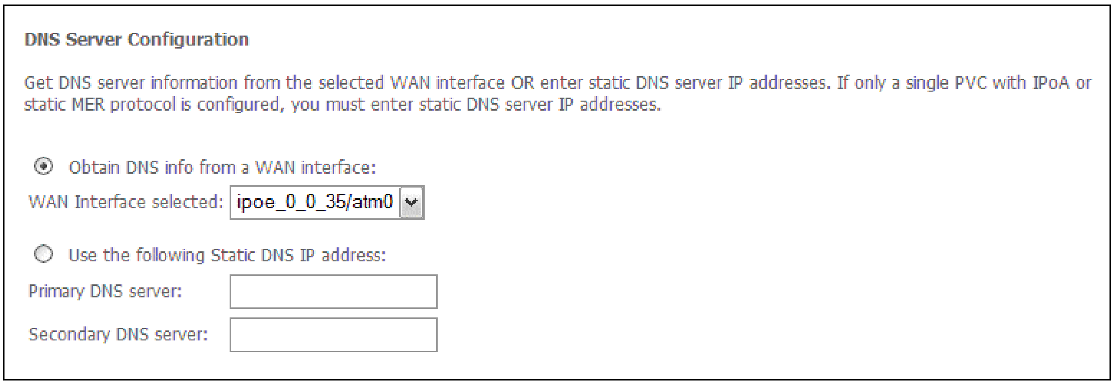
Selected WAN Interface ipoe_0_0_35/atm0

Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: Select a WAN interface or enter static IP address to IPv4/v6 DNS Servers.



DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

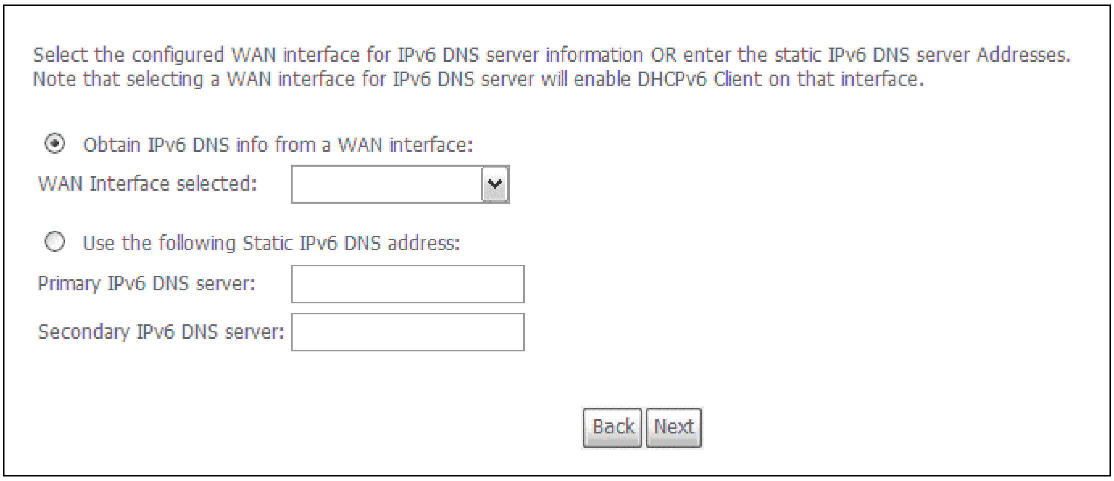
WAN Interface selected: ipoe_0_0_35/atm0

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

If IPv6 is enabled, an additional set of options will be shown.



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:

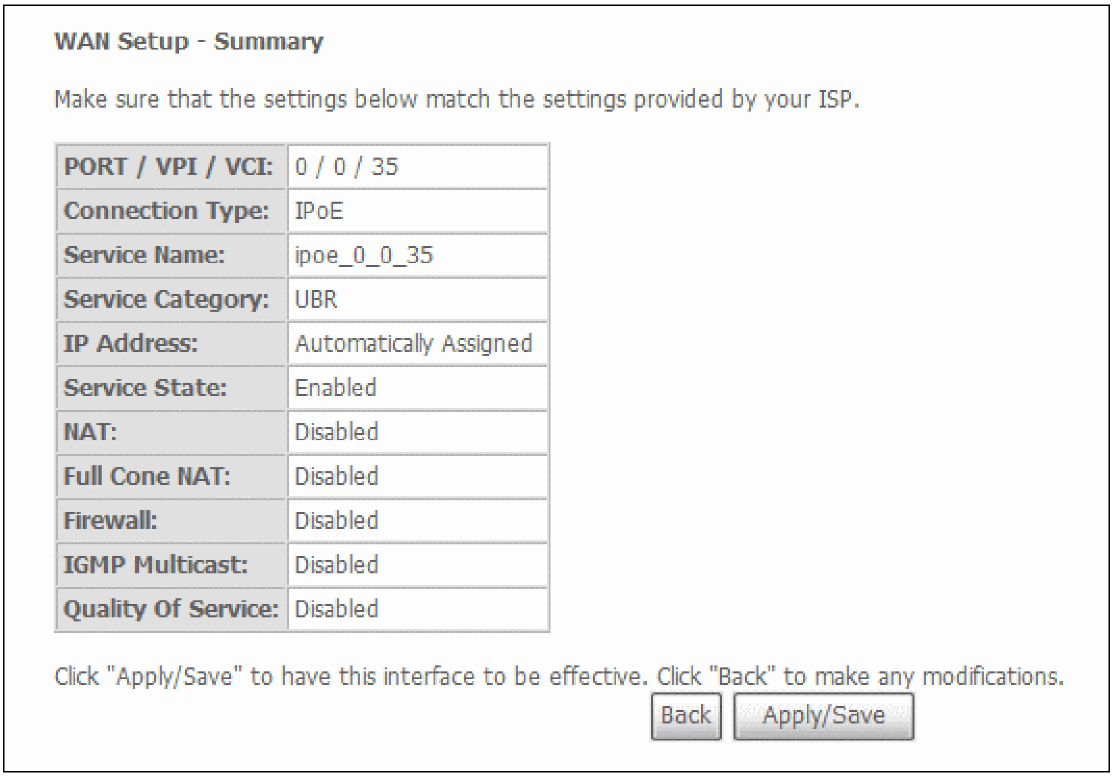
○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

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

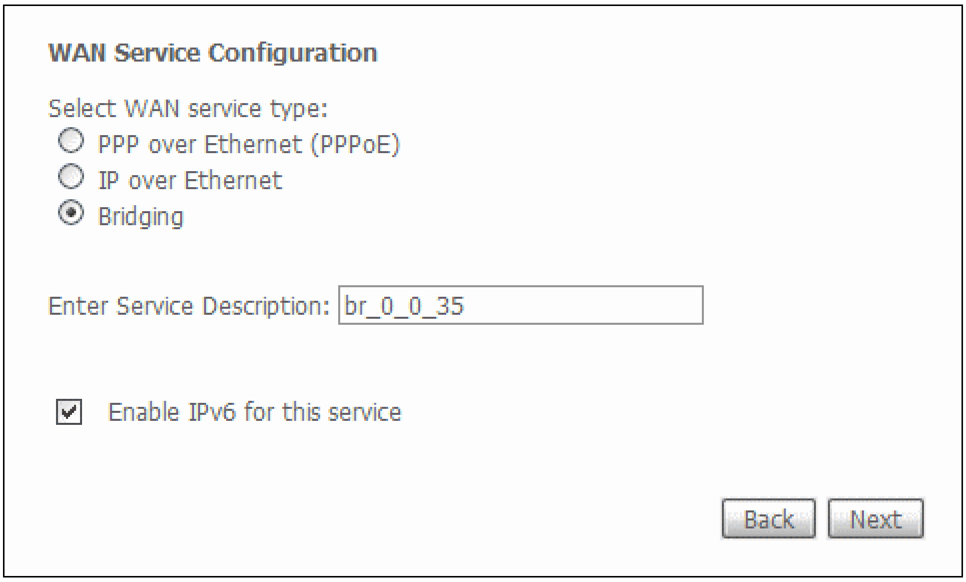
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoE
Service Name:	ipoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

E2.3 Bridging

STEP 1: Select the Bridging radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.


WAN Service Configuration

Select WAN service type:

○ PPP over Ethernet (PPPoE)

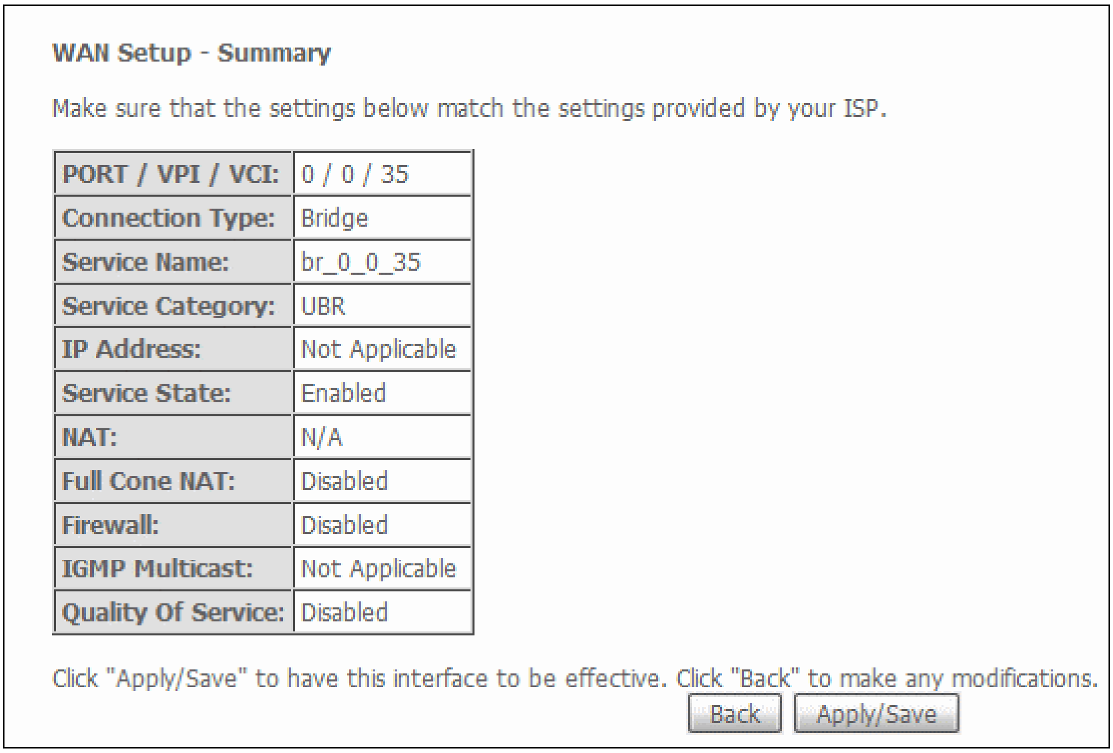
○ IP over Ethernet

● Bridging

Enter Service Description: br_0_0_35

☑ Enable IPv6 for this service

STEP 2: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to return to the previous screen.


WAN Setup - Summary

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

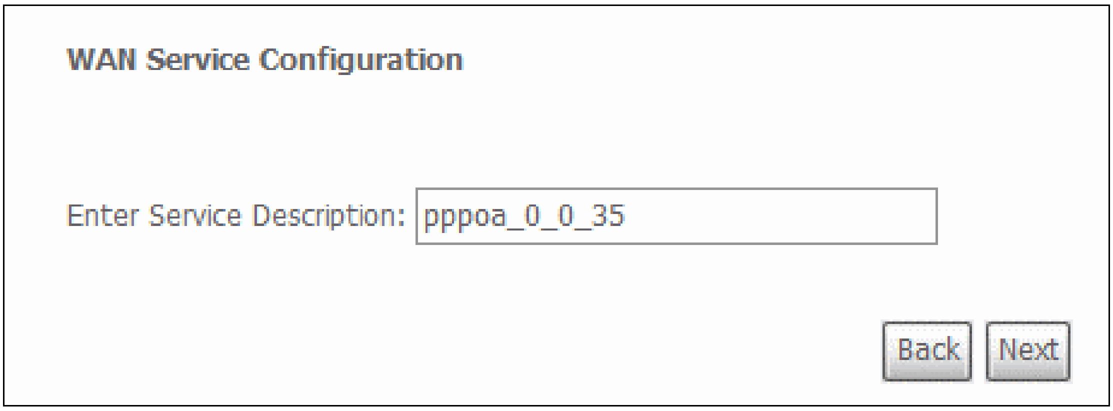
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	Bridge
Service Name:	br_0_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

NOTE: If this bridge connection is your only WAN service, the Proscend 140 will be inaccessible for remote management or technical support from the WAN.

E2.4 PPP over ATM (PPPoA)

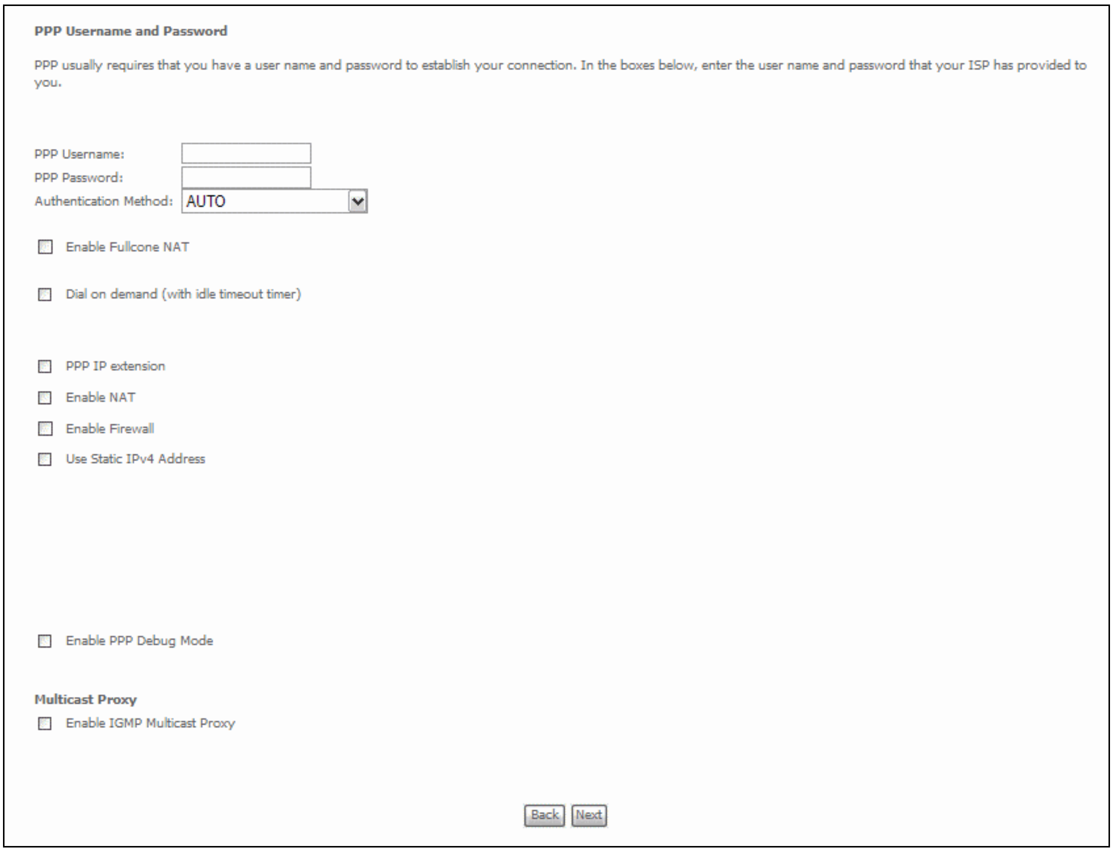


WAN Service Configuration

Enter Service Description: pppoa_0_0_35

STEP 1: Click **Next** to continue.

STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.



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)

□ PPP IP extension
□ Enable NAT
□ Enable Firewall
□ Use Static IPv4 Address

□ Enable PPP Debug Mode

Multicast Proxy
□ Enable IGMP Multicast Proxy

PPP SETTINGS

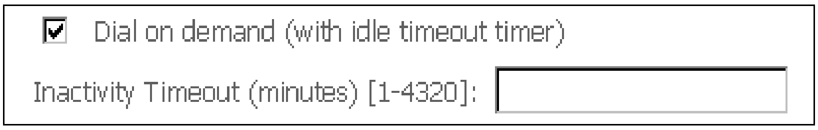
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND

The Proscend 140 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



☑ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device’s LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot.

On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2.

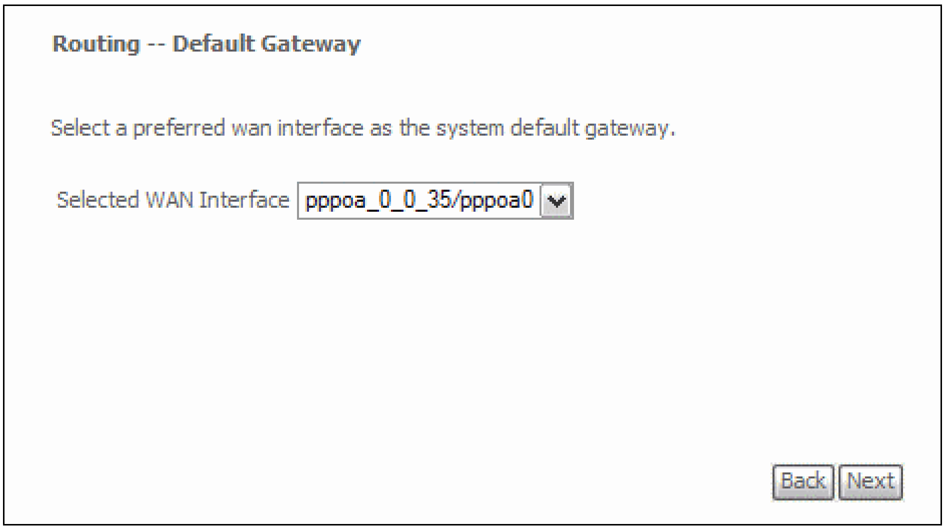
ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

ENABLE IGMP MULTICAST

Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

STEP 3: Select a WAN interface as the preferred default gateway route.



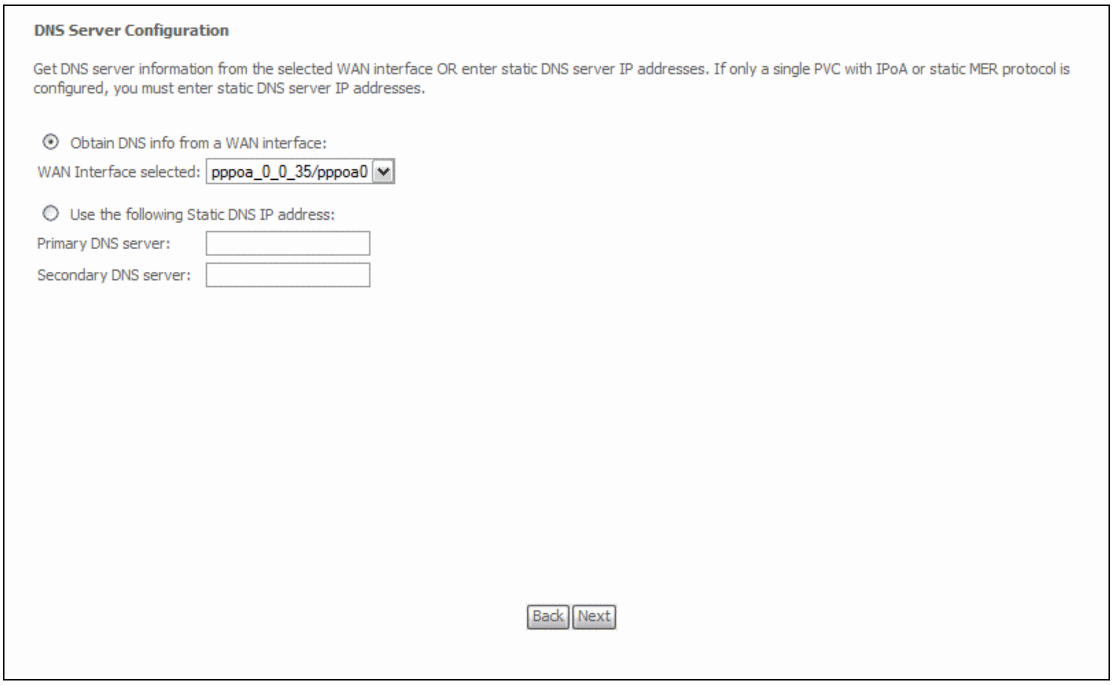
Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface pppoa_0_0_35/pppoa0

Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select a WAN interface or enter a static IP address to the DNS Server.



DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoa_0_0_35/pppoa0

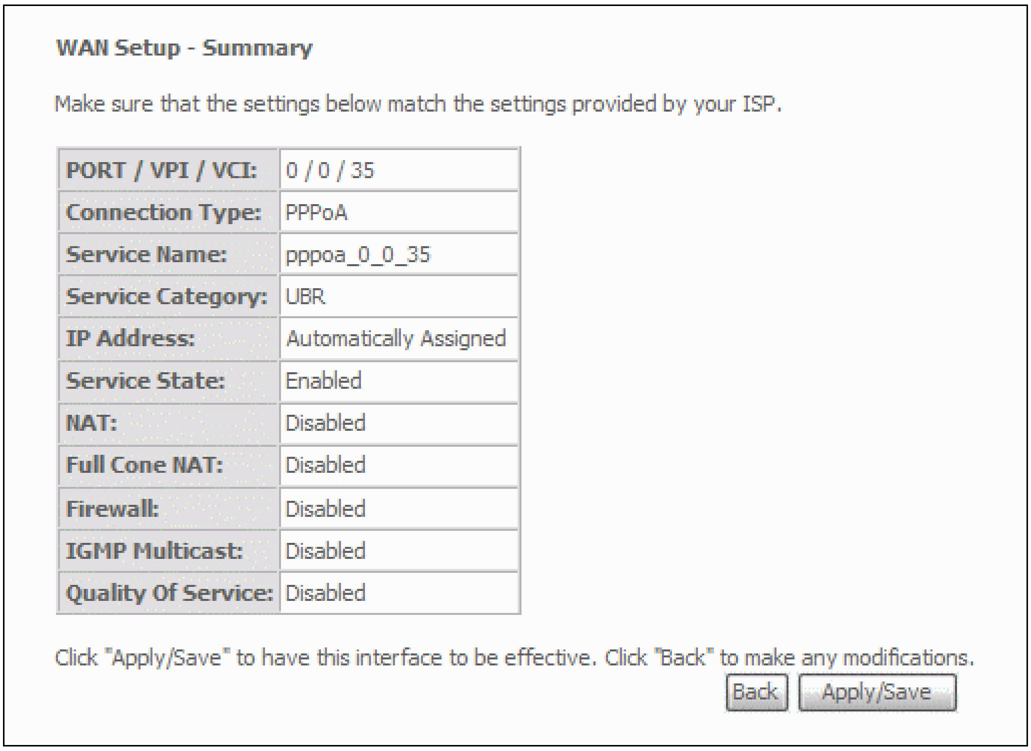
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

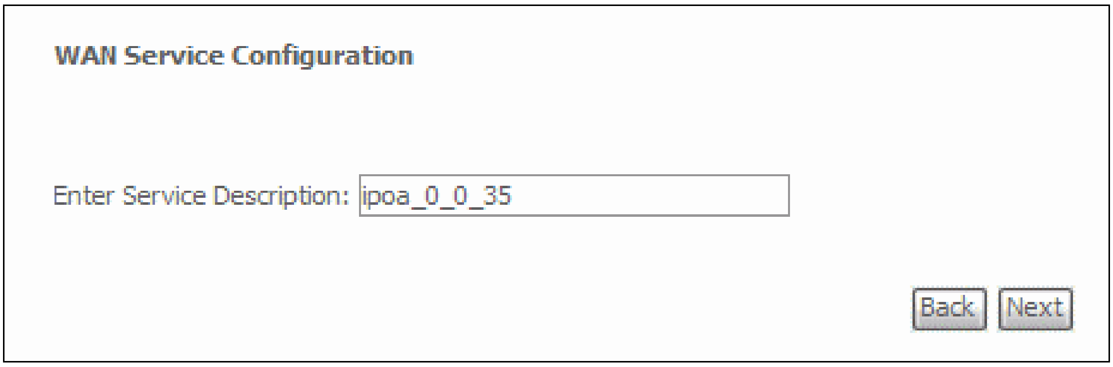
Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

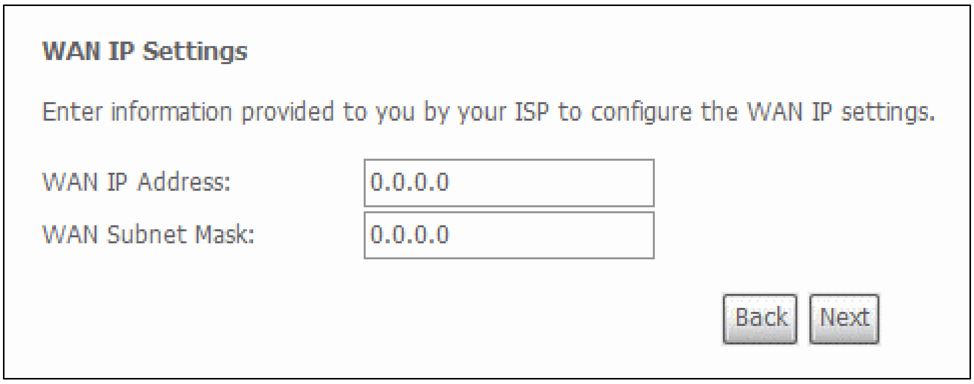
E2.5 IP over ATM (IPoA)


WAN Service Configuration

Enter Service Description: ipoa_0_0_35

STEP 1: Click **Next** to continue.

STEP 2: Enter the WAN IP settings provided by your ISP. Click **Next** to continue.

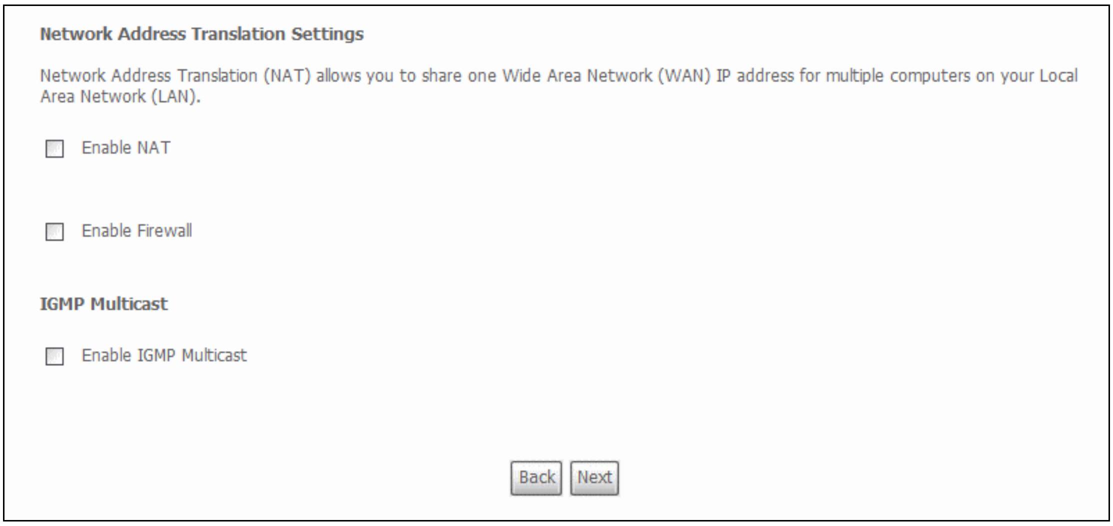

WAN IP Settings

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

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.



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

□ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host by sending a packet to the mapped external address.

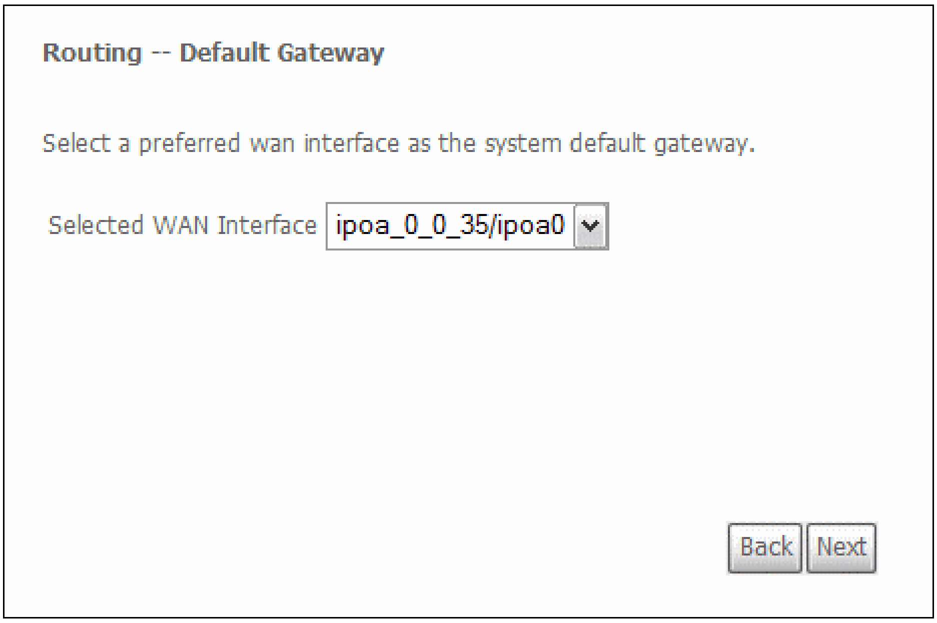
ENABLE FIREWALL

If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST

Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

STEP 4: Select a WAN interface as the preferred default gateway route.



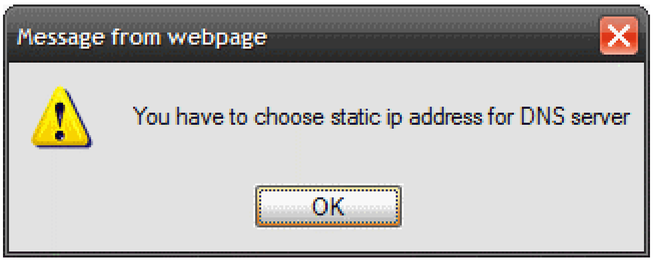
Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: ipoa_0_0_35/ipoa0

Click **Next** to continue or click **Back** to return to the previous step.

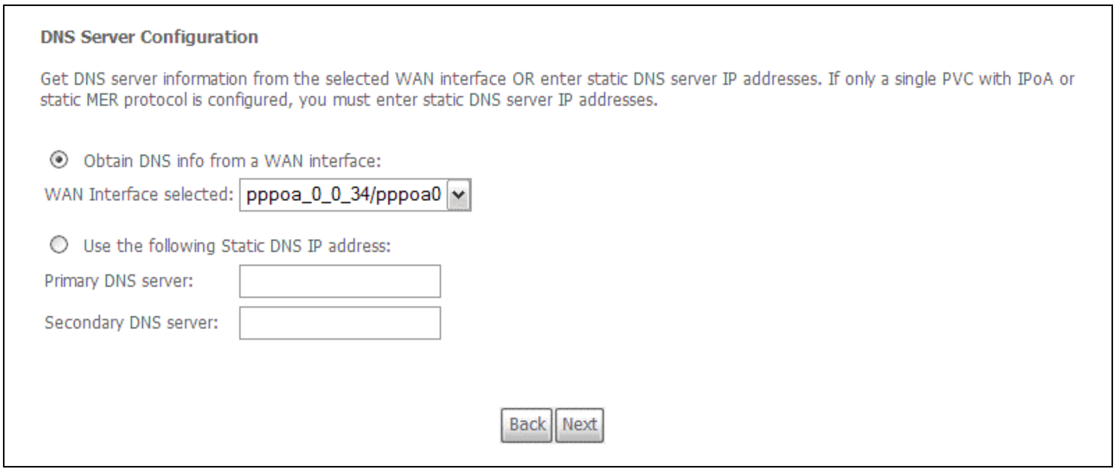
NOTE: If the DHCP server is not enabled on another WAN interface then the following notification will be shown before the next screen.



Message from webpage

You have to choose static ip address for DNS server

STEP 5: Select a WAN interface or enter a static IP address to the DNS Server.



DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoa_0_0_34/pppoa0

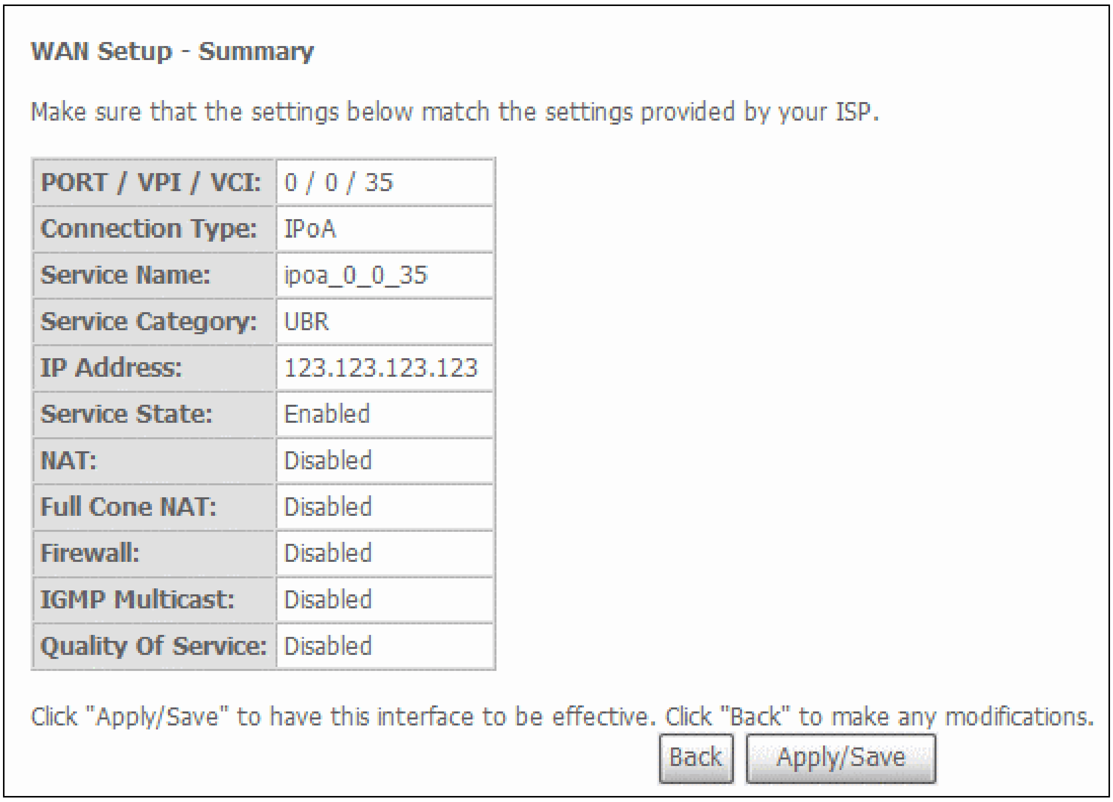
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Click **Next** to continue or click **Back** to return to the previous step.

STEP 7: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_0_35
Service Category:	UBR
IP Address:	123.123.123.123
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

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

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

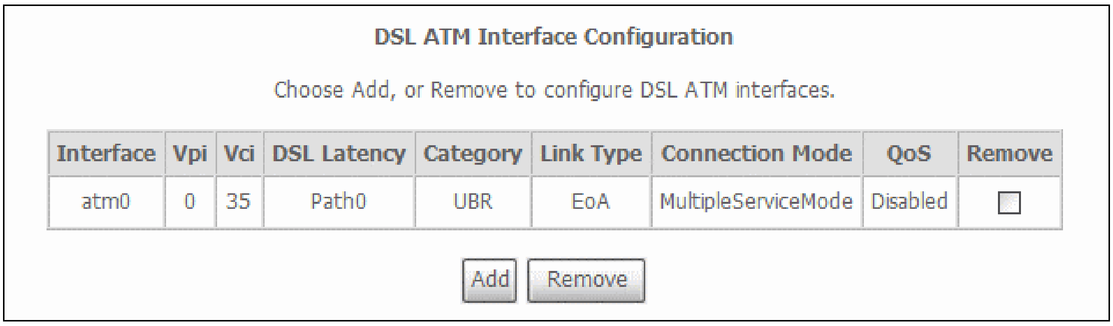
E3 ~ More About MSC Mode

The procedure for WAN connection setup in MSC mode is as follows:

STEP 1: Create a Layer2 interface in MSC connection mode.
STEP 2: Add WAN connections to the interface (Bridge, PPPoE or IPoE).
STEP 3: Use Interface Grouping to connect LAN and WAN interfaces.

These three steps are repeated below with screenshots added for reference.

STEP 1: Create a Layer2 interface in MSC connection mode.

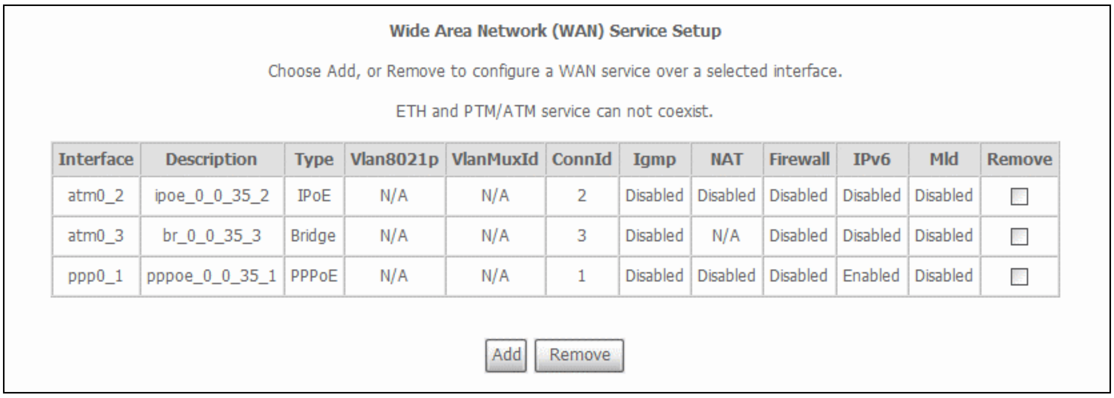


DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	0	35	Path0	UBR	EoA	MultipleServiceMode	Disabled	☐

STEP 2: Add WAN connections to the interface (Bridge, PPPoE or IPoE).



Wide Area Network (WAN) Service Setup

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

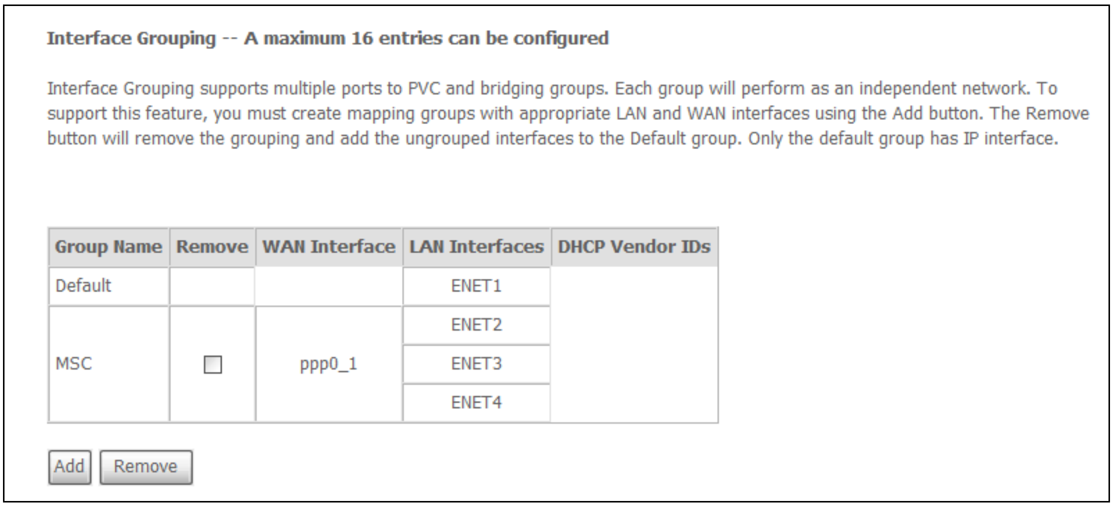
ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	IPv6	Mld	Remove
atm0_2	ipoe_0_0_35_2	IPoE	N/A	N/A	2	Disabled	Disabled	Disabled	Disabled	Disabled	☐
atm0_3	br_0_0_35_3	Bridge	N/A	N/A	3	Disabled	N/A	Disabled	Disabled	Disabled	☐
ppp0_1	pppoe_0_0_35_1	PPPoE	N/A	N/A	1	Disabled	Disabled	Disabled	Enabled	Disabled	☐

NOTES: If QoS is configured on the first MSC connection, it will be configured by default for all subsequent connections.

If a MSC connection is removed every other MSC connection should be removed to avoid potential configuration problems.

STEP 3: Use Interface Grouping to connect LAN and WAN interfaces.



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			ENET1	
MSC	☐	ppp0_1	ENET2 ENET3 ENET4	

See the instructions in Interface Grouping for help with this final step.