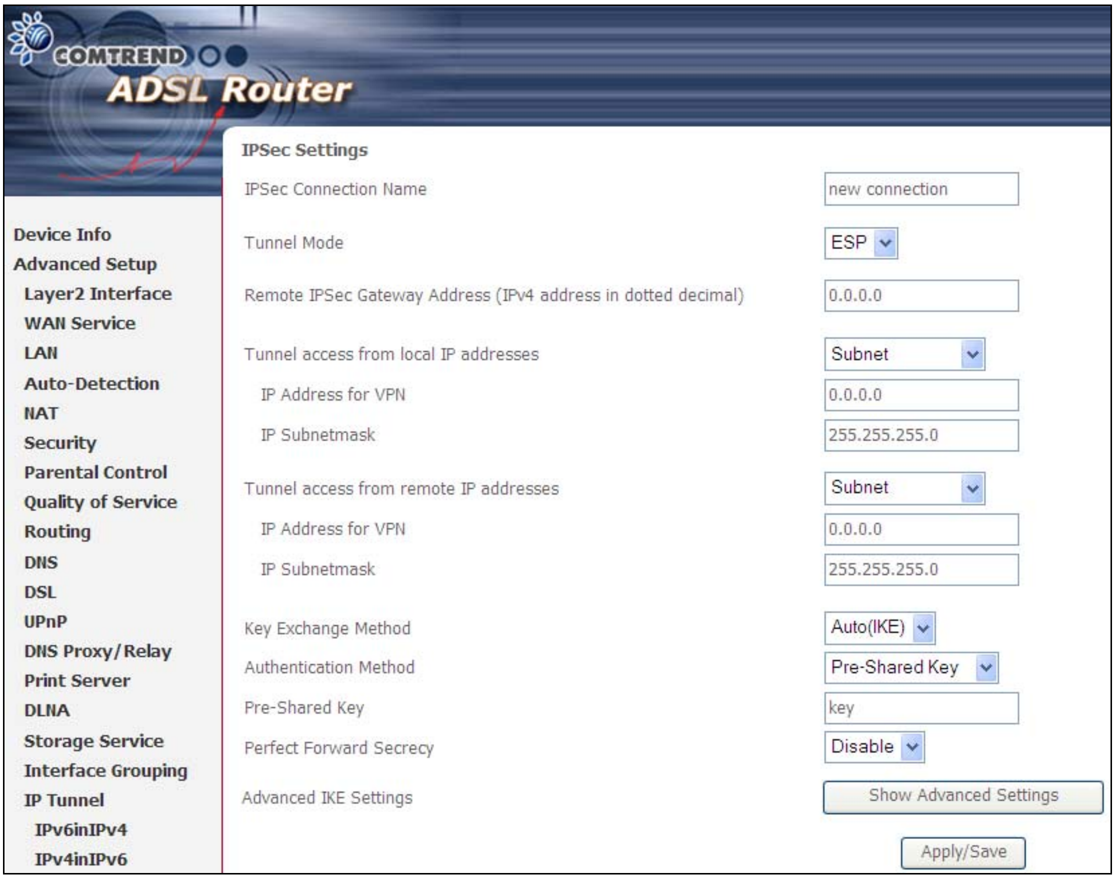


IPSec Settings

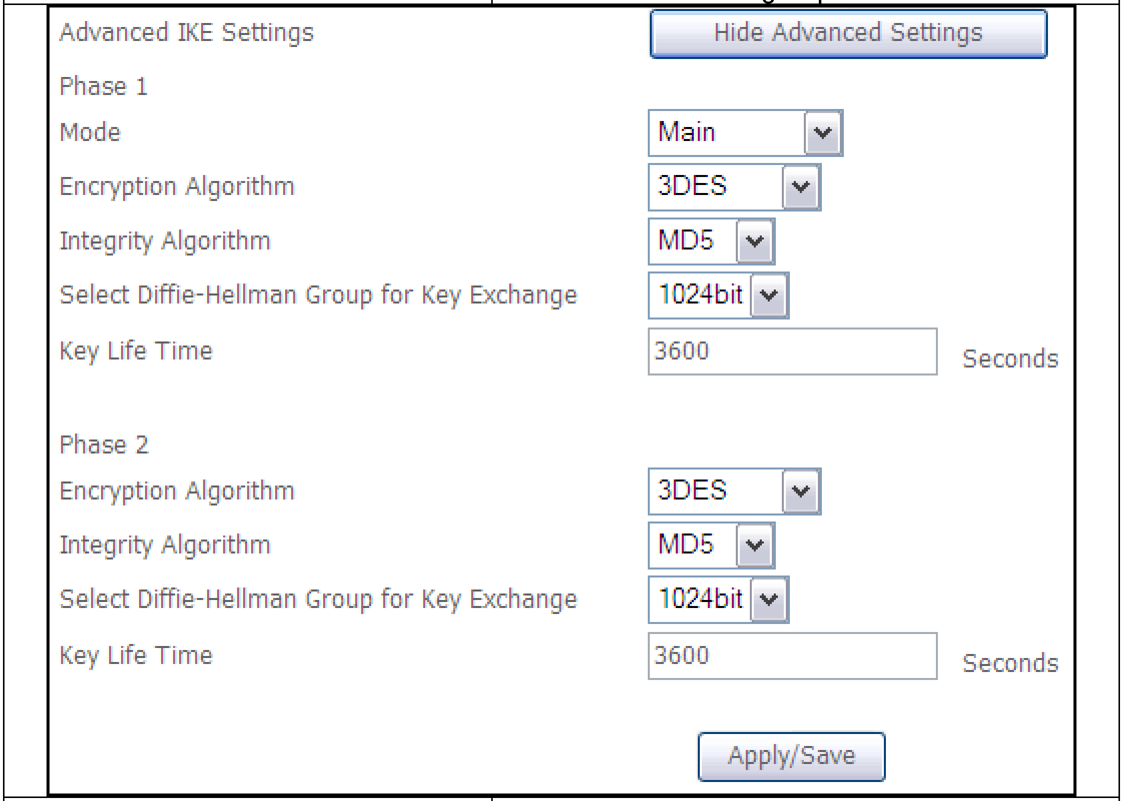
IPSec Connection Name	new connection
Tunnel Mode	ESP
Remote IPSec Gateway Address (IPv4 address in dotted decimal)	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask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

IPSec Connection Name	User-defined label
Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select **Show Advanced Settings** to reveal the advanced settings options shown below.



Advanced IKE Settings

Phase 1

Mode: Main

Encryption Algorithm: 3DES

Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

Phase 2

Encryption Algorithm: 3DES

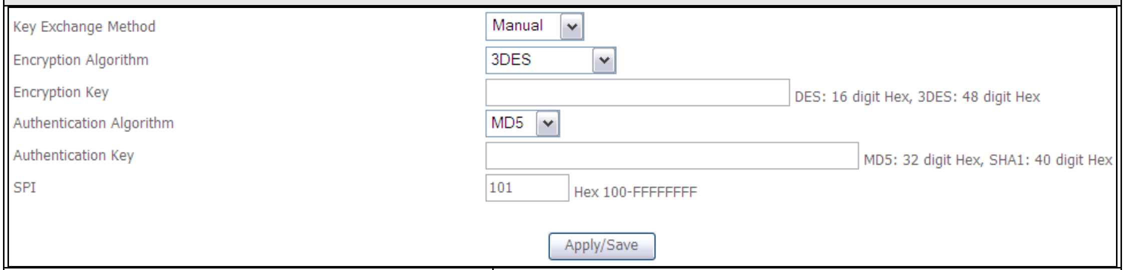
Integrity Algorithm: MD5

Select Diffie-Hellman Group for Key Exchange: 1024bit

Key Life Time: 3600 Seconds

Advanced IKE Settings	Select **Hide Advanced Settings** to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

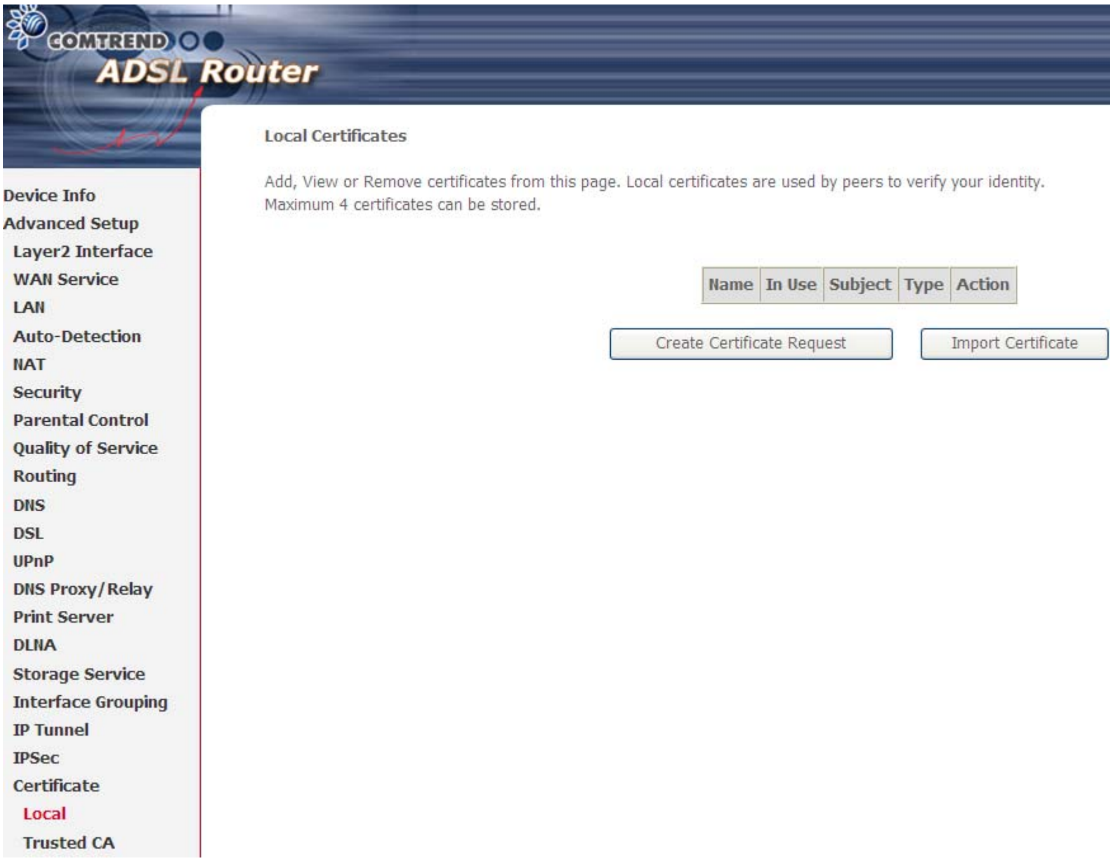
The Manual key exchange method options are summarized in the table below.

Manual Key Exchange Method	
 Key Exchange Method: Manual Encryption Algorithm: 3DES Encryption Key: DES: 16 digit Hex, 3DES: 48 digit Hex Authentication Algorithm: MD5 Authentication Key: MD5: 32 digit Hex, SHA1: 40 digit Hex SPI: 101 Hex 100-FFFFFFFF Apply/Save	
Encryption Algorithm	DES / 3DES / AES (aes-cbc)
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5 / SHA1
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

5.20 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.

5.20.1 Local



Local Certificates

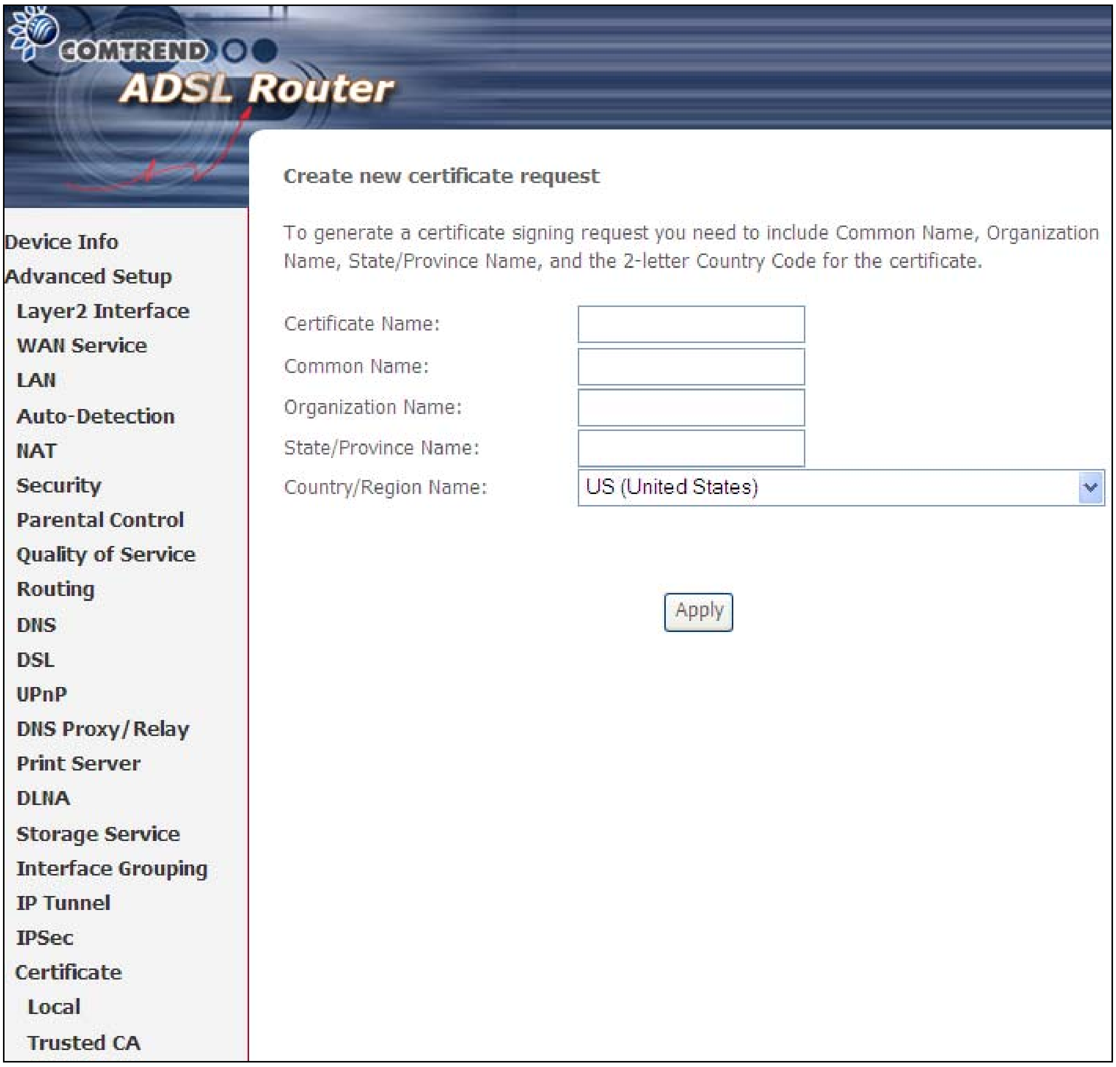
Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

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.

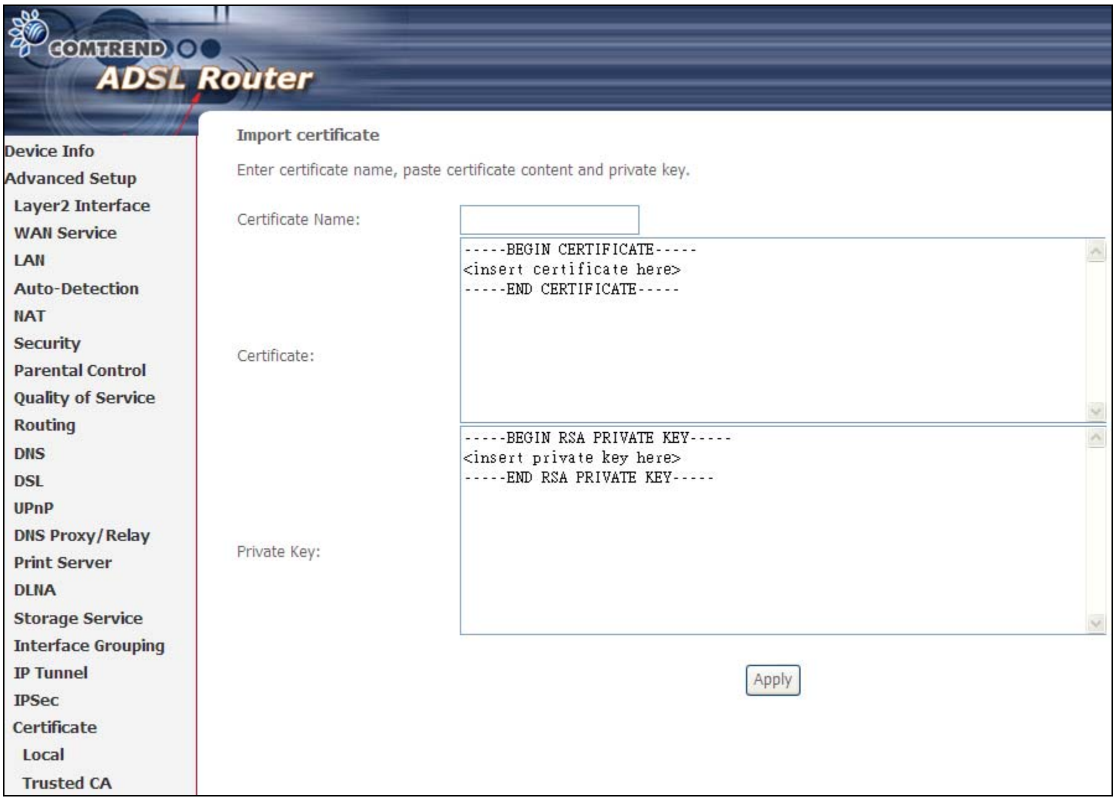
Certificate Name:	
Common Name:	
Organization Name:	
State/Province Name:	
Country/Region Name:	US (United States)

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-----
```

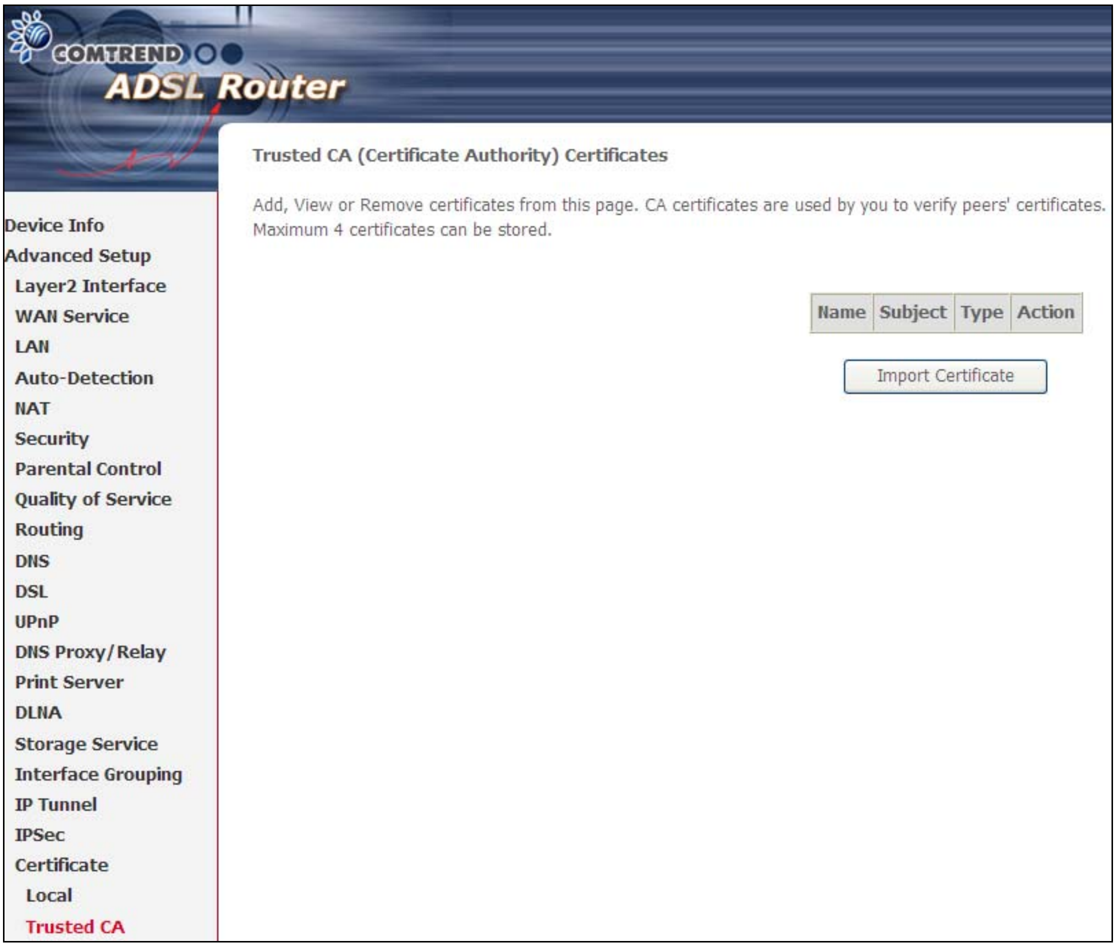
Private Key:

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

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

5.20.2 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.

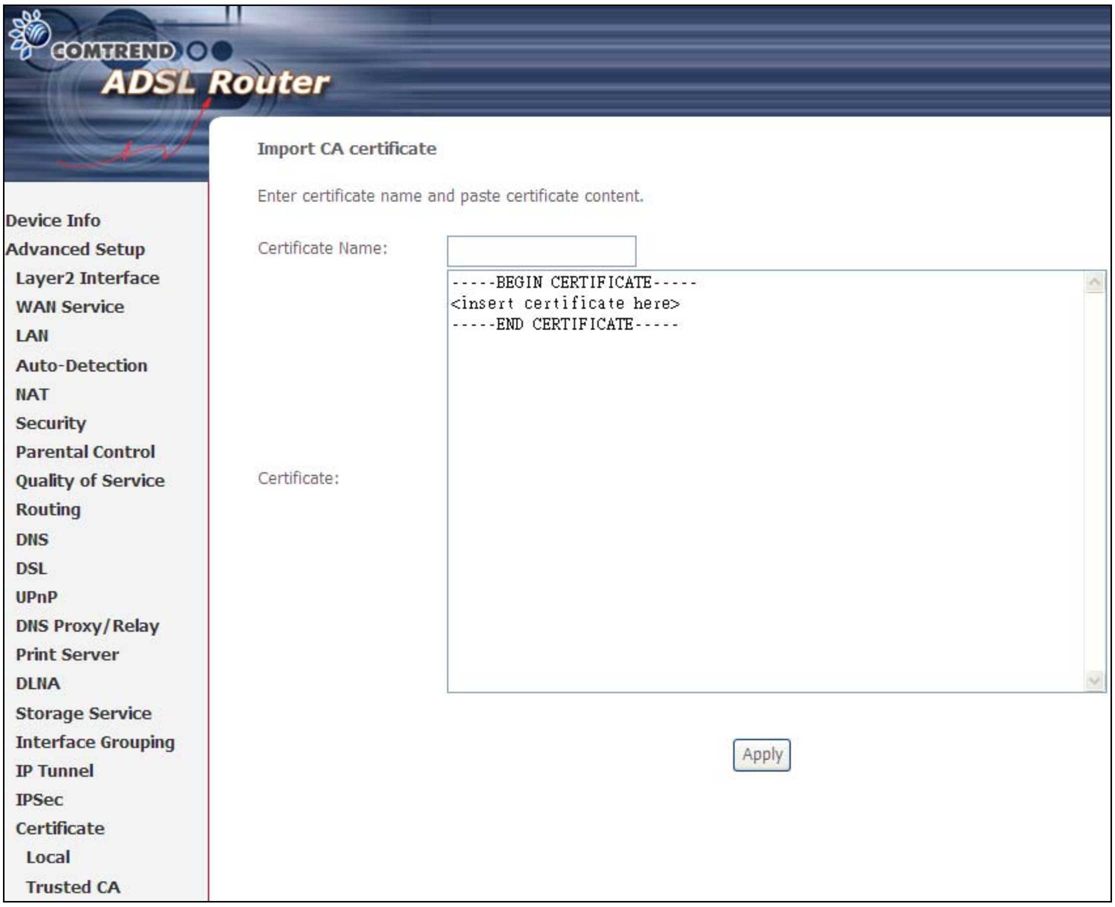


Trusted CA (Certificate Authority) Certificates

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:

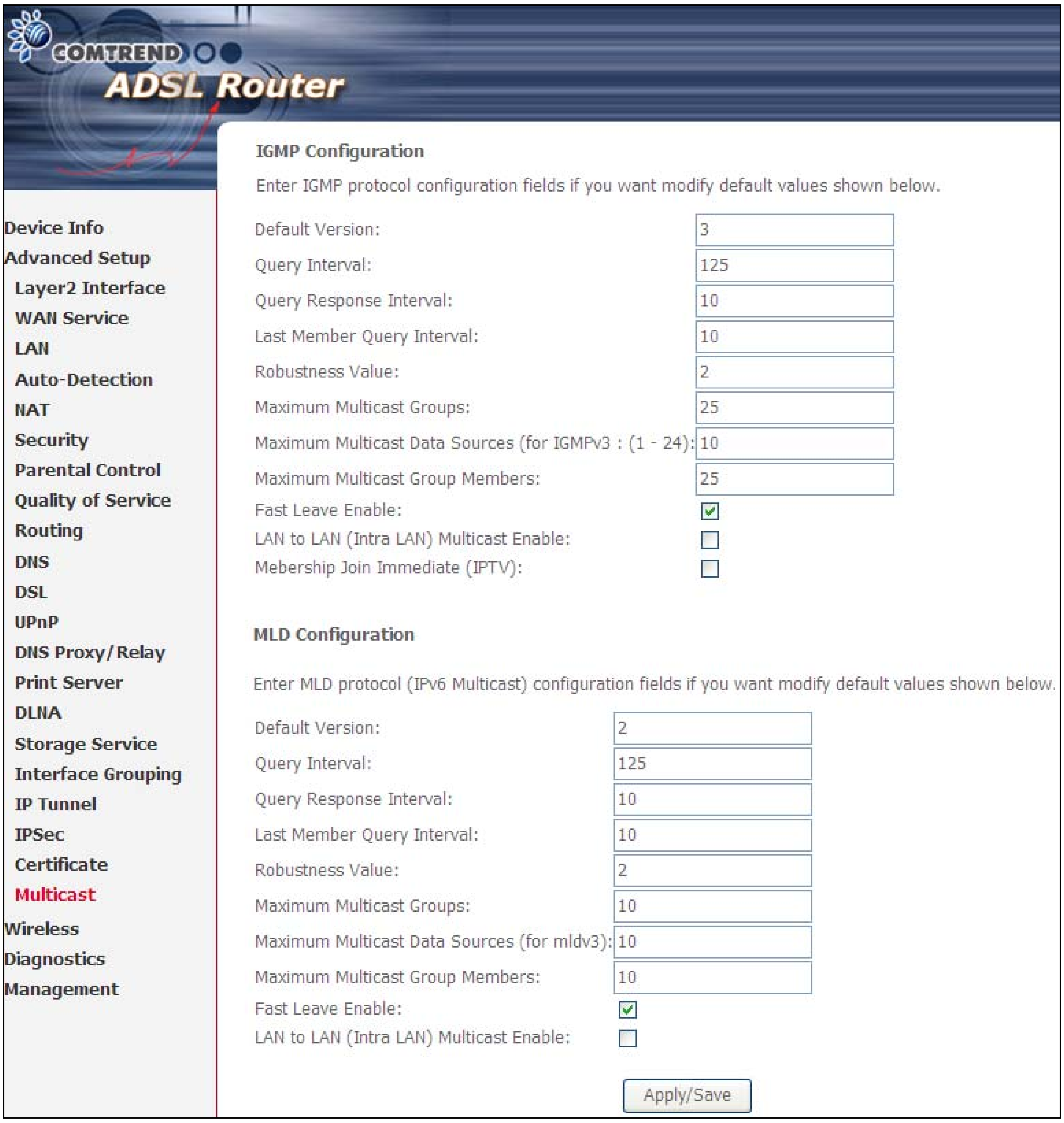
Certificate:

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

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

5.21 Multicast

Input new IGMP or MLD protocol configuration fields if you want modify default values shown. Then click **Apply/Save**.



IGMP Configuration

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

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

MLD Configuration

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

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

Chapter 6 Wireless

The Wireless menu provides access to the wireless options discussed below.

6.1 Basic

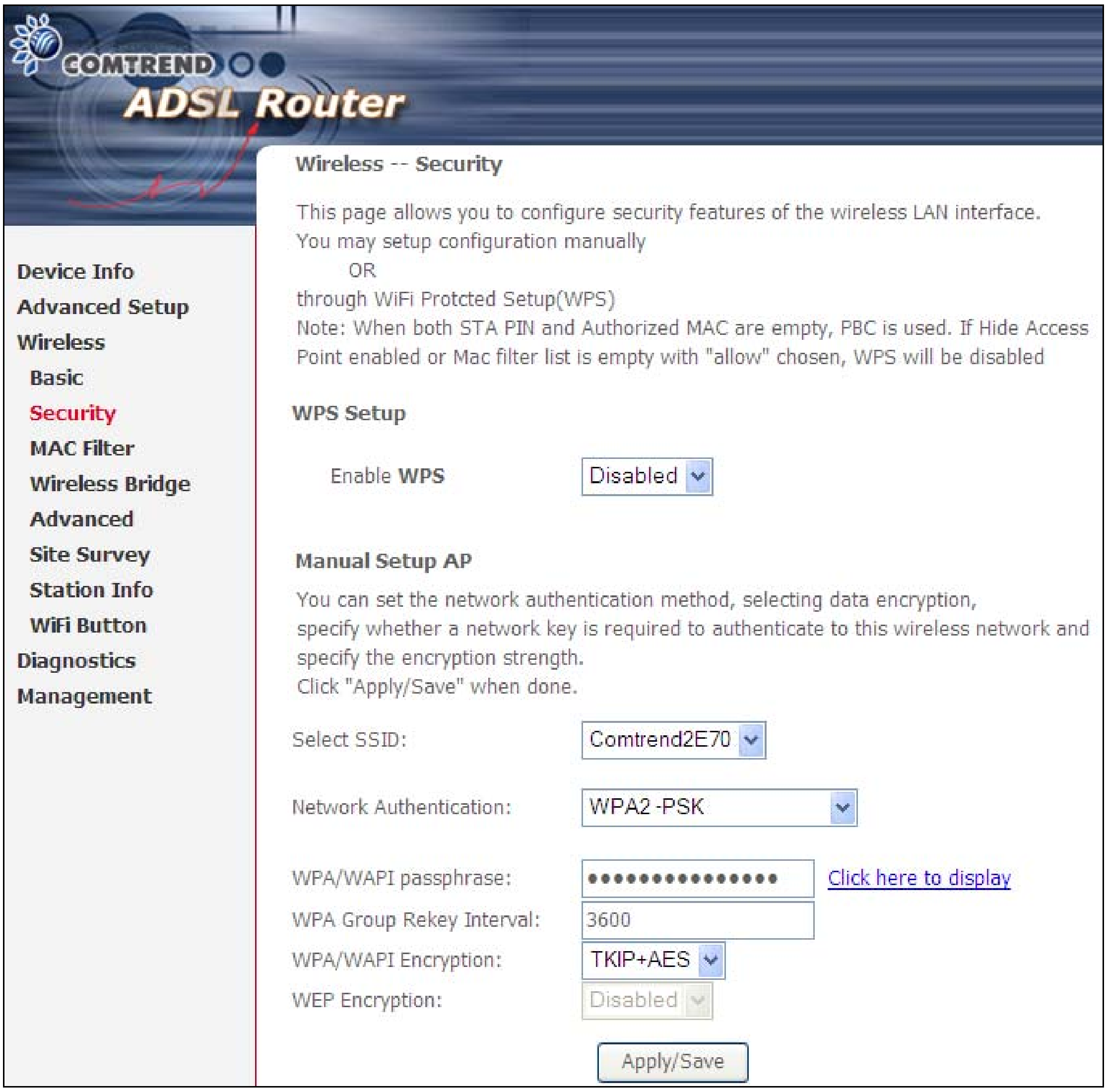
The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID).

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **Network Connections** from the **start** Menu and select **View Available Network Connections**. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Select the checkbox ☑ to enable this function.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the **Enabled** column. To hide a Guest SSID select its checkbox ☑ in the **Hidden** column. Do the same for **Isolate Clients** and **Disable WMM Advertise**. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for **Enable WMF**, **Max Clients** and **BSSID**, consult the matching entries in this table. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

6.2 Security

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.



Wireless -- Security

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

WPS Setup

Enable **WPS**: Disabled

Manual Setup AP

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

Select SSID: Comtrend2E70

Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ••••••••••••••• Click here to display

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

Click **Save / Apply** to implement new configuration settings.

WIRELESS SECURITY

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see

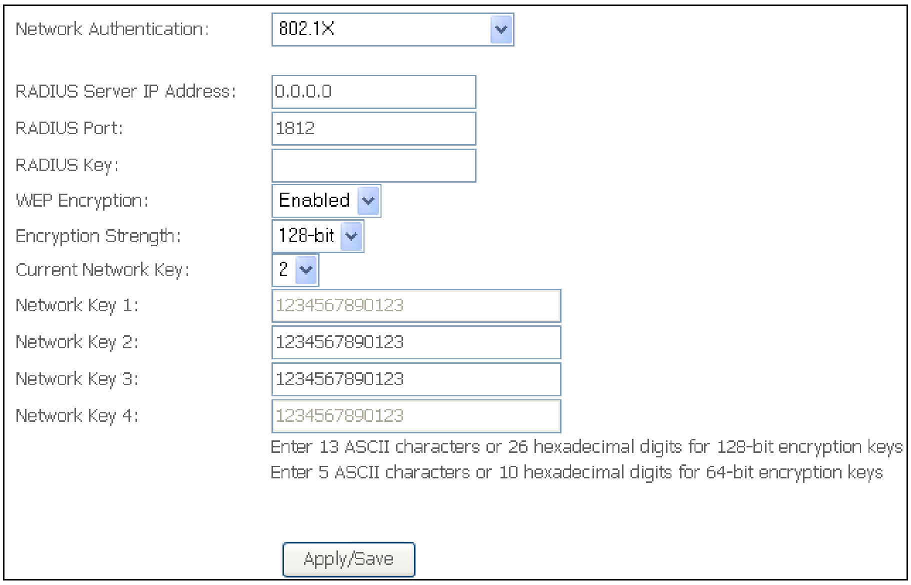
6.2.1 WPS) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID
Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.



Network Authentication: 802.1X

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 2

Network Key 1: 1234567890123

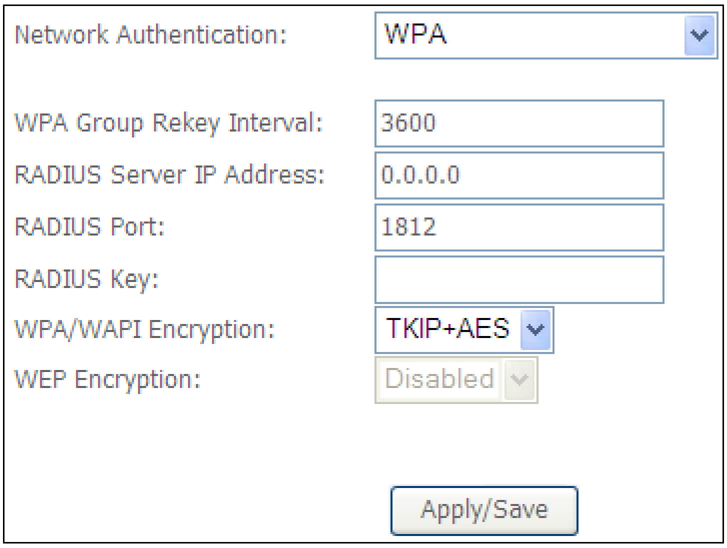
Network Key 2: 1234567890123

Network Key 3: 1234567890123

Network Key 4: 1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

The settings for WPA authentication are shown below.



Network Authentication: WPA

WPA Group Rekey Interval: 3600

RADIUS Server IP Address: 0.0.0.0

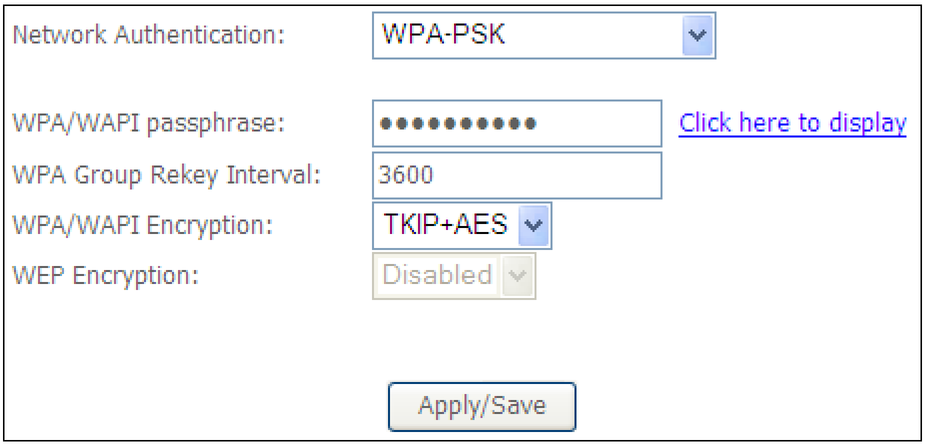
RADIUS Port: 1812

RADIUS Key:

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

The settings for WPA-PSK authentication are shown next.



Network Authentication:	WPA-PSK
WPA/WAPI passphrase:	●●●●●●●●●●● Click here to display
WPA Group Rekey Interval:	3600
WPA/WAPI Encryption:	TKIP+AES
WEP Encryption:	Disabled

WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.2.1 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has a PIN number accessed through device software. The AR-5381u has a virtual button accessible from the web user interface (WUI).

Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase “Wi-Fi Protected Setup”.

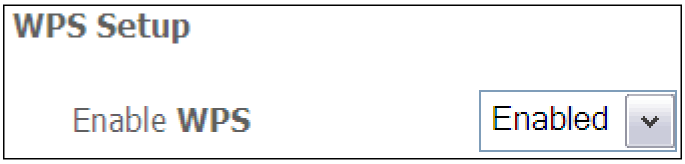
Wi-Fi PROTECTED
SETUP

NOTE: WPS is only available in Open, WPA-PSK, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

To configure security settings with WPS, follow the procedures below. You must choose either the Push-Button or PIN configuration method for Steps 6 and 7.

I. Setup

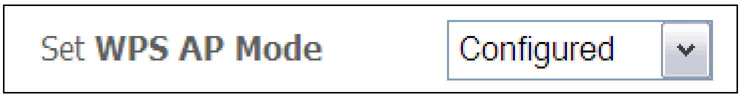
Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.



WPS Setup

Enable WPS: Enabled

Step 2: Set the WPS AP Mode. **Configured** is used when the AR-5381u will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the AR-5381u.



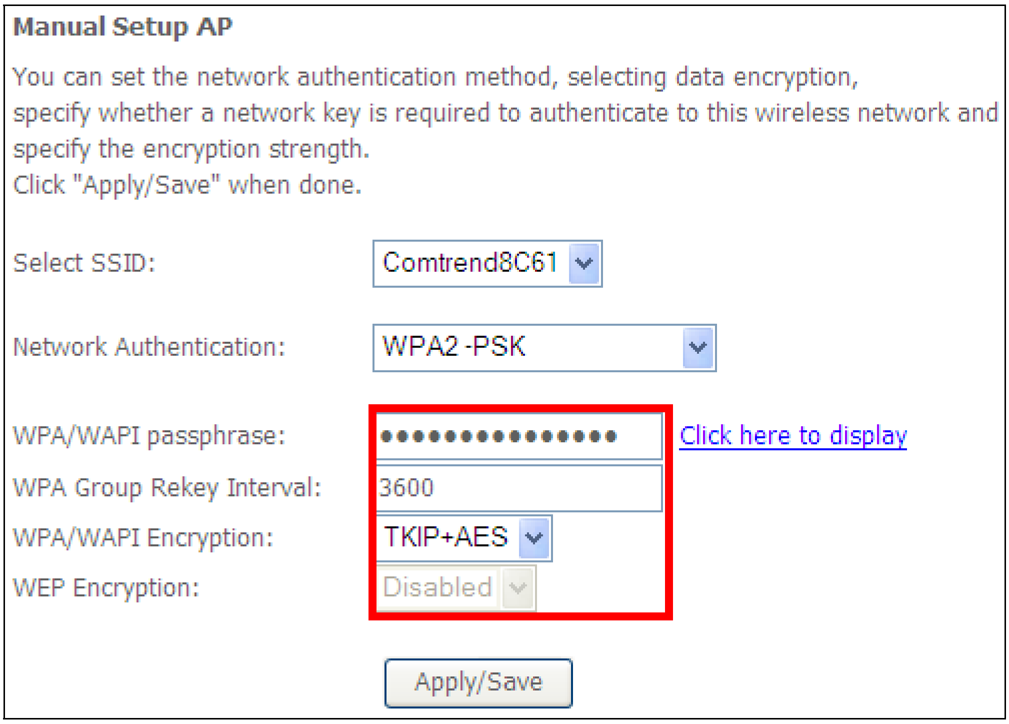
Set WPS AP Mode: Configured

NOTES: Your client may or may not have the ability to provide security settings to the AR-5381u. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

In addition, using Windows Vista, you can add an external registrar using the **StartAddER** button (Appendix D - WPS OPERATION) has detailed instructions).

II. NETWORK AUTHENTICATION

Step 3: Select Open, WPA-PSK, WPA2-PSK, or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The example below shows WPA2-PSK mode.



Manual Setup AP

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

Select SSID: Comtrend8C61

Network Authentication: WPA2 -PSK

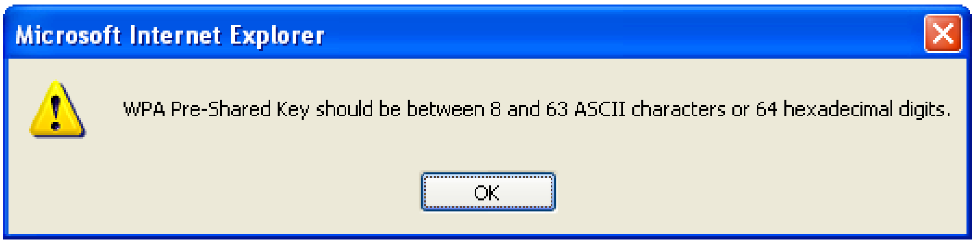
WPA/WAPI passphrase: ••••••••••••••• Click here to display

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

Step 4: For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key. You will see the following dialog box if the Key is too short or too long.



Microsoft Internet Explorer

WPA Pre-Shared Key should be between 8 and 63 ASCII characters or 64 hexadecimal digits.

Step 5: Click the **Save/Apply** button at the bottom of the screen.

IIIa. PUSH-BUTTON CONFIGURATION

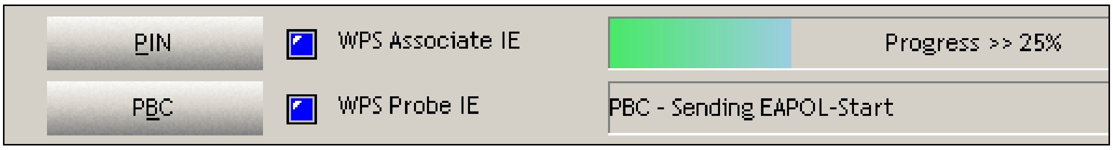
The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE: The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 7, return to Step 6.

Step 6: Press WPS button
Press the WPS button on the front panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Step 7: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.



PBC - Sending EAPOL-Start

Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IIIb. WPS – PIN CONFIGURATION

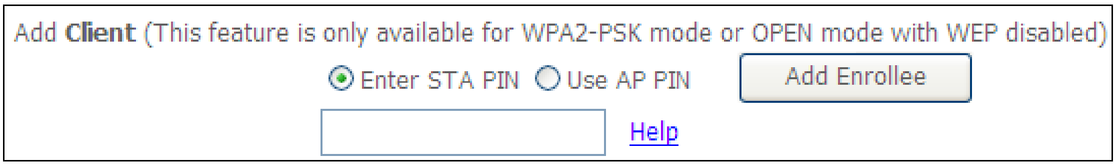
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE: Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

Step 6: Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

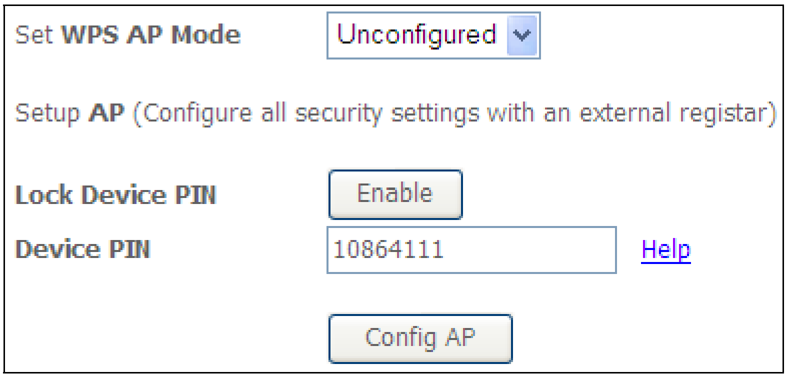
A - For **Configured** mode, click the **Add Enrollee** button.


Add **Client** (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)

● Enter STA PIN ○ Use AP PIN

Enter STA PIN: a Personal Identification Number (PIN) has to be read from either a sticker or the display on the new wireless device. This PIN must then be inputted at representing the network, usually the Access Point of the network.

B - For **Unconfigured** mode, click the **Config AP** button.



Set **WPS AP Mode** Unconfigured

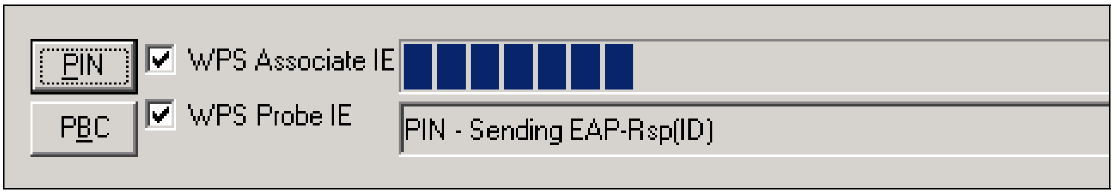
Setup **AP** (Configure all security settings with an external registar)

Lock Device PIN

Device PIN 10864111

Step 7: Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

The figure below provides an example of a WPS client PIN function in-progress.



☑ WPS Associate IE

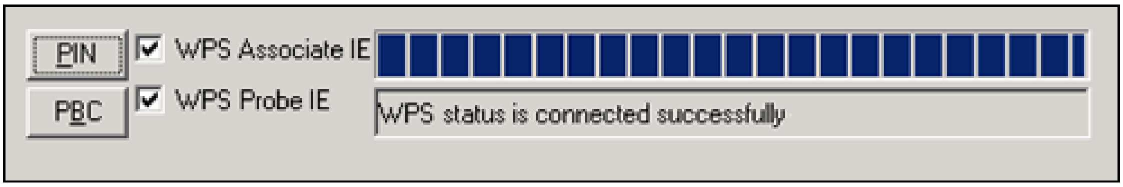
☑ WPS Probe IE

PIN - Sending EAP-Rsp(ID)

Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IV. CHECK CONNECTION

Step 8: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



☑ WPS Associate IE

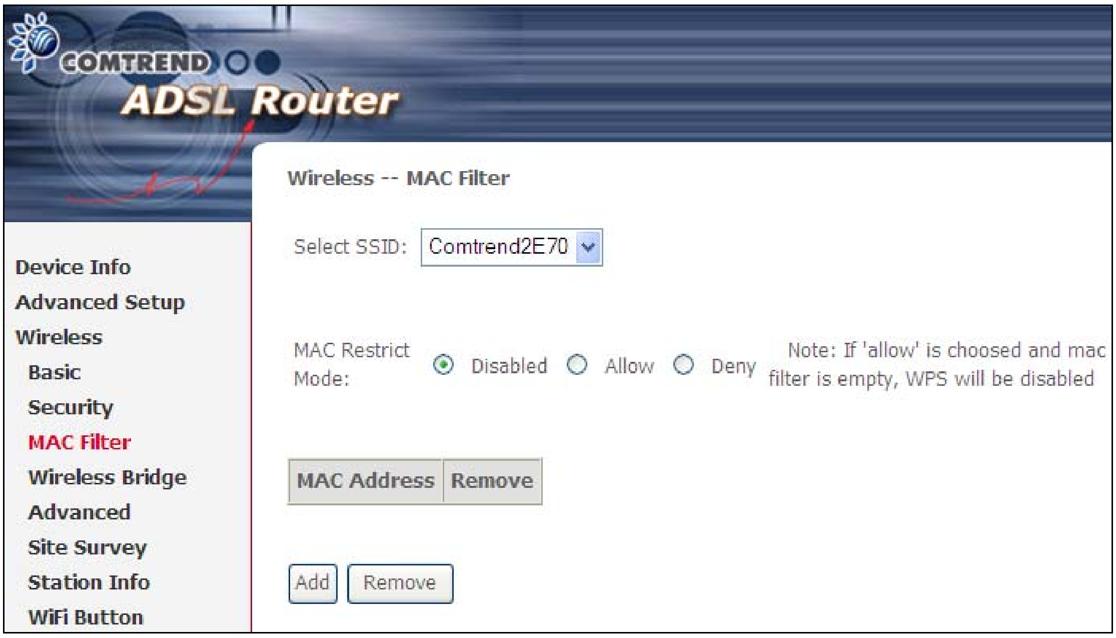
☑ WPS Probe IE

WPS status is connected successfully

You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

6.3 MAC Filter

This option allows access to the router to be restricted based upon MAC addresses. To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the MAC Address table below and click the **Remove** button.



Wireless -- MAC Filter

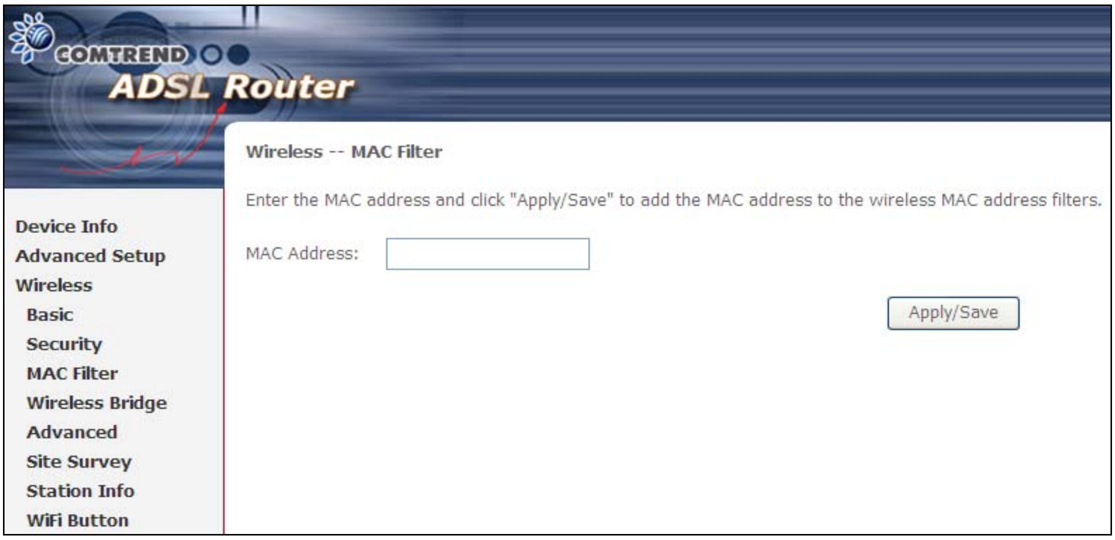
Select SSID: Comtrend2E70

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

MAC Address	Remove

Option	Description
Select SSID	Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

After clicking the **Add** button, the following screen appears.
Enter the MAC address in the box provided and click **Save/Apply**.



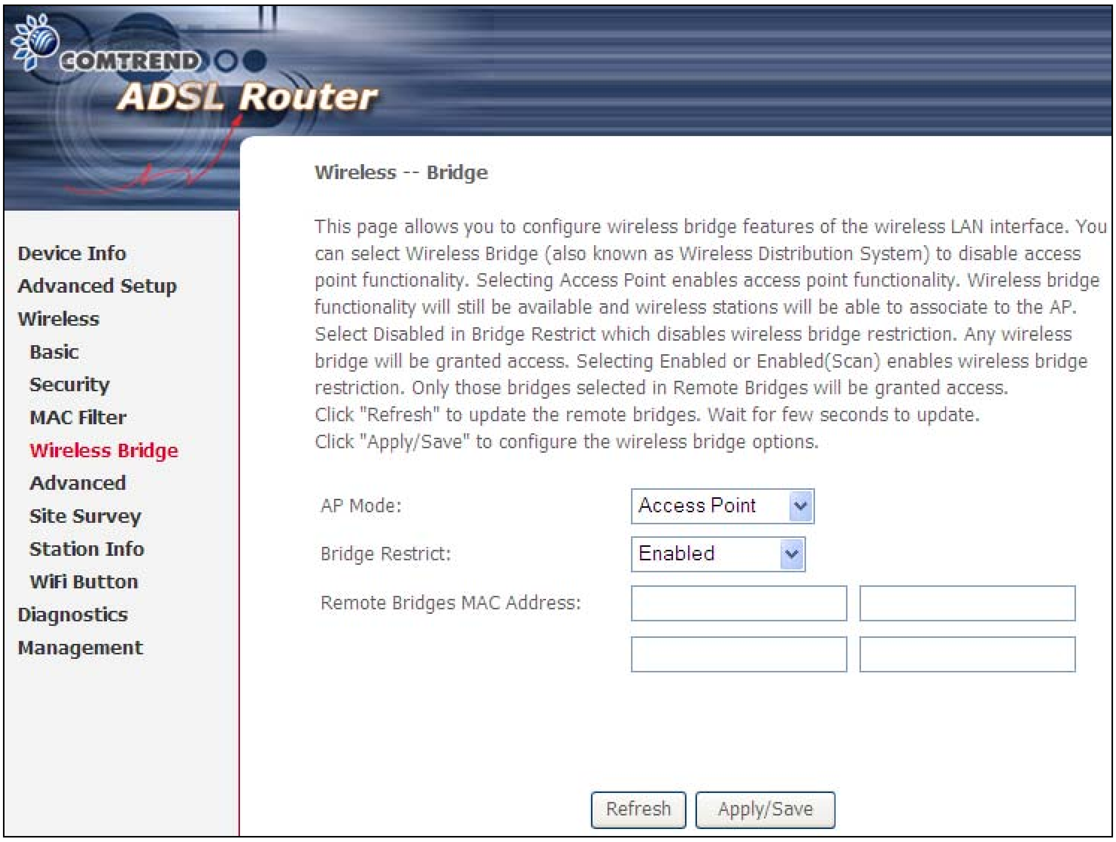
Wireless -- MAC Filter

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

MAC Address:

6.4 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the WIFI interface. See the table beneath for detailed explanations of the various options.



Wireless -- Bridge

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

AP Mode: Access Point

Bridge Restrict: Enabled

Remote Bridges MAC Address:

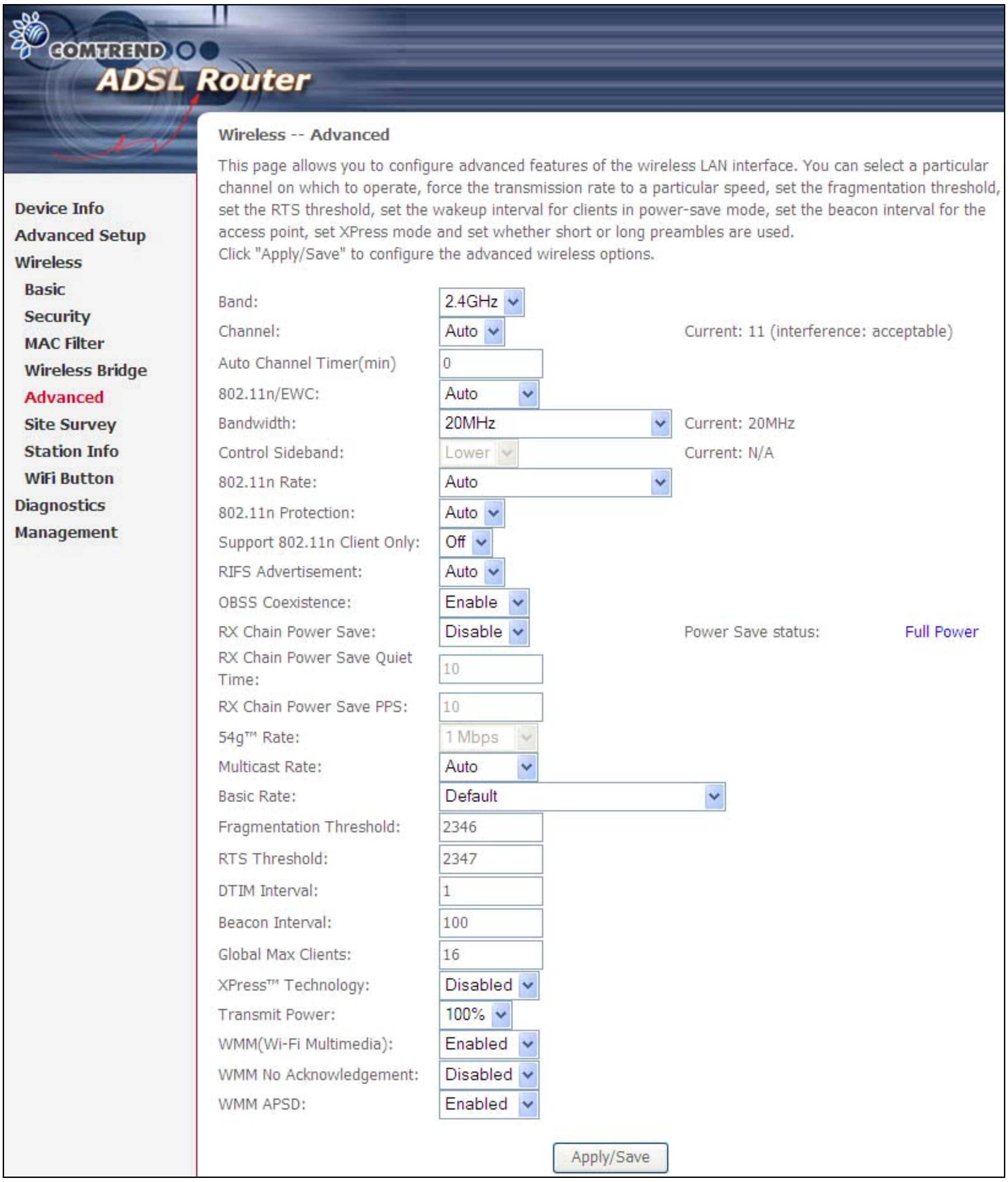
Click **Save / Apply** to implement new configuration settings.

Feature	Description

Feature	**Description**
AP Mode	Selecting **Wireless Bridge** (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting **Access Point** enables AP functionality. In **Access Point** mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting **Disabled** disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click **Refresh** to update the station list when Bridge Restrict is enabled.

6.5 Advanced

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



Wireless -- Advanced

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

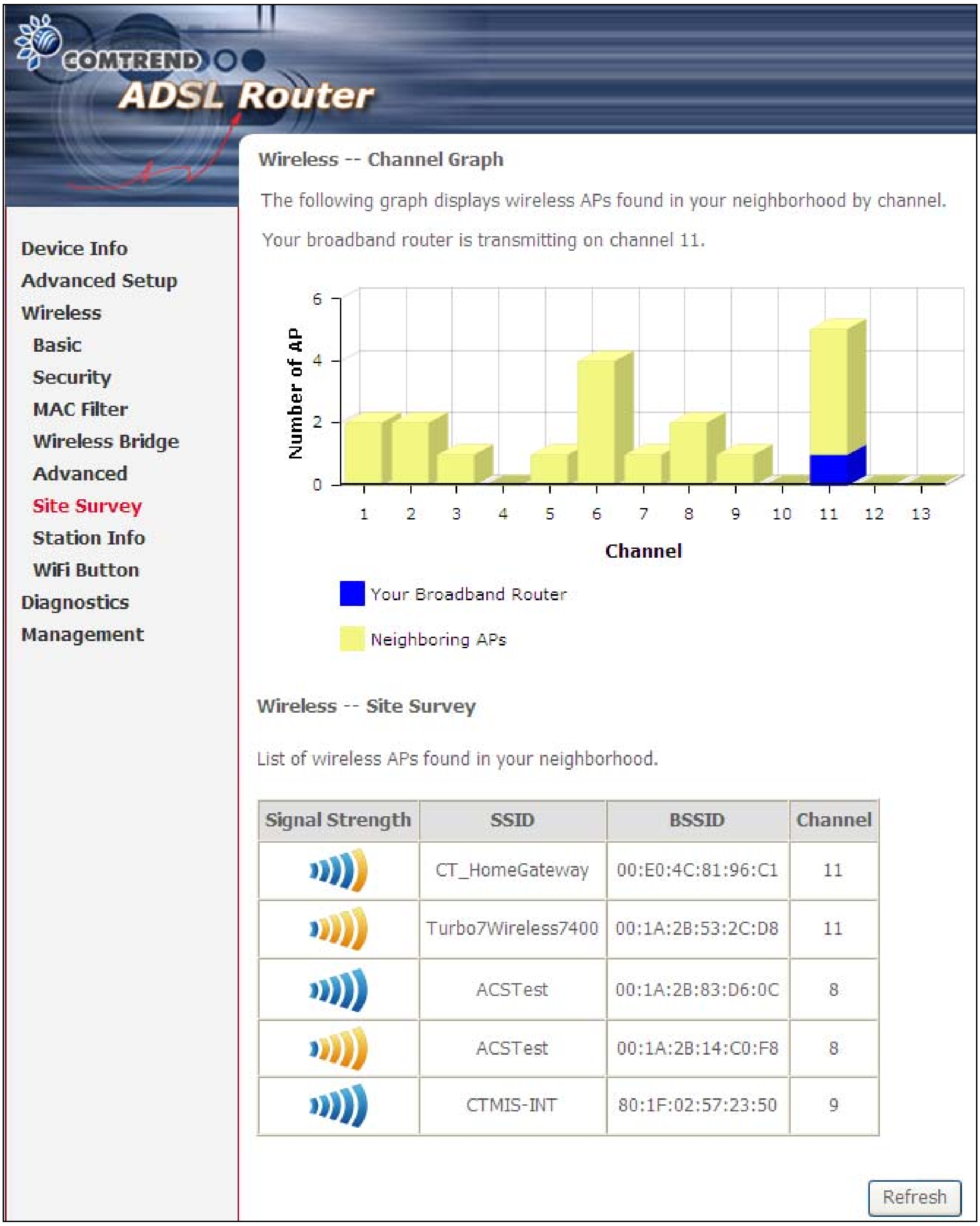
Band:	2.4GHz		
Channel:	Auto	Current: 11 (interference: acceptable)	
Auto Channel Timer(min)	0		
802.11n/EWC:	Auto		
Bandwidth:	20MHz	Current: 20MHz	
Control Sideband:	Lower	Current: N/A	
802.11n Rate:	Auto		
802.11n Protection:	Auto		
Support 802.11n Client Only:	Off		
RIFS Advertisement:	Auto		
OBSS Coexistence:	Enable		
RX Chain Power Save:	Disable	Power Save status:	Full Power
RX Chain Power Save Quiet Time:	10		
RX Chain Power Save PPS:	10		
54g™ Rate:	1 Mbps		
Multicast Rate:	Auto		
Basic Rate:	Default		
Fragmentation Threshold:	2346		
RTS Threshold:	2347		
DTIM Interval:	1		
Beacon Interval:	100		
Global Max Clients:	16		
XPress™ Technology:	Disabled		
Transmit Power:	100%		
WMM(Wi-Fi Multimedia):	Enabled		
WMM No Acknowledgement:	Disabled		
WMM APSD:	Enabled		

Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20GHz or 40GHz bandwidth. 40GHz bandwidth uses two adjacent 20GHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40GHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g clients access to the router.
RIFS Advertisement	One of several draft-n features designed to improve efficiency. Provides a shorter delay between OFDM transmissions than in802.11a or g.
OBSS Co-Existence	Co-existence between 20 MHZ AND 40 MHZ overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting for basic transmission rate.

Field	**Description**
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress ^{TM} Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

6.6 Site Survey

The graph displays wireless APs found in your neighborhood by channel.



Wireless -- Channel Graph

The following graph displays wireless APs found in your neighborhood by channel.

Your broadband router is transmitting on channel 11.

🟦 Your Broadband Router

🟨 Neighboring APs

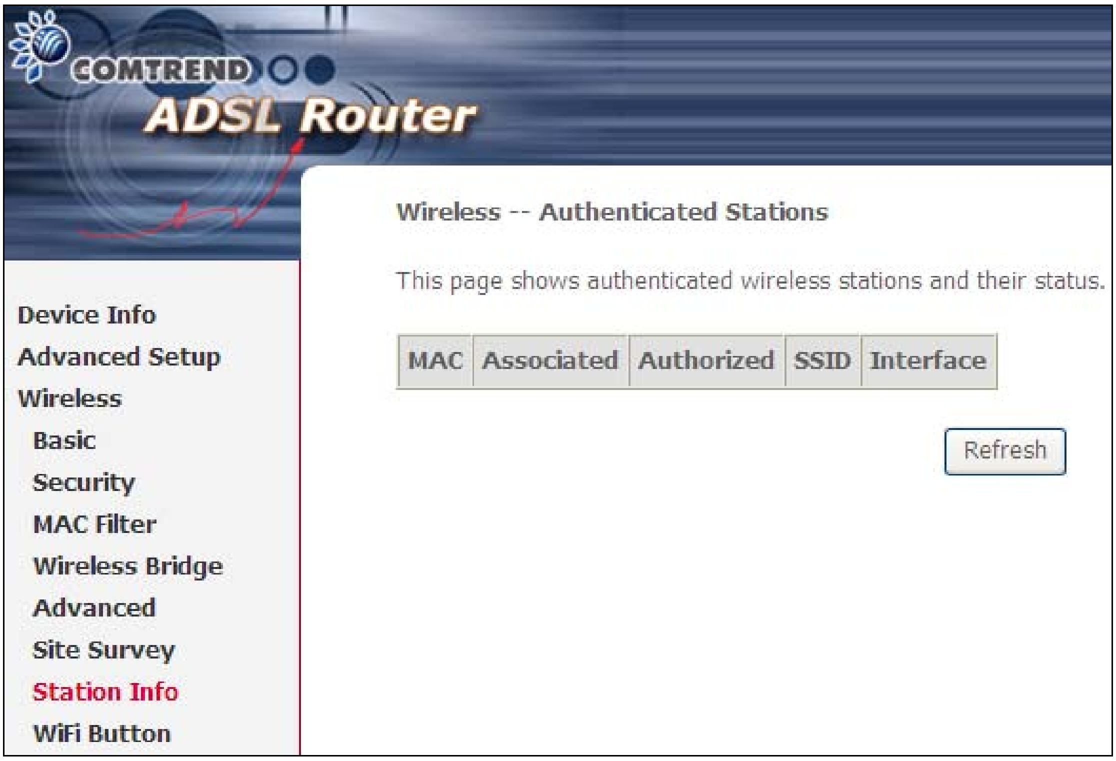
Wireless -- Site Survey

List of wireless APs found in your neighborhood.

Signal Strength	SSID	BSSID	Channel
📶	CT_HomeGateway	00:E0:4C:81:96:C1	11
📶	Turbo7Wireless7400	00:1A:2B:53:2C:D8	11
📶	ACSTest	00:1A:2B:83:D6:0C	8
📶	ACSTest	00:1A:2B:14:C0:F8	8
📶	CTMIS-INT	80:1F:02:57:23:50	9

6.7 Station Info

This page shows authenticated wireless stations and their status. Click the **Refresh** button to update the list of stations in the WLAN.



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

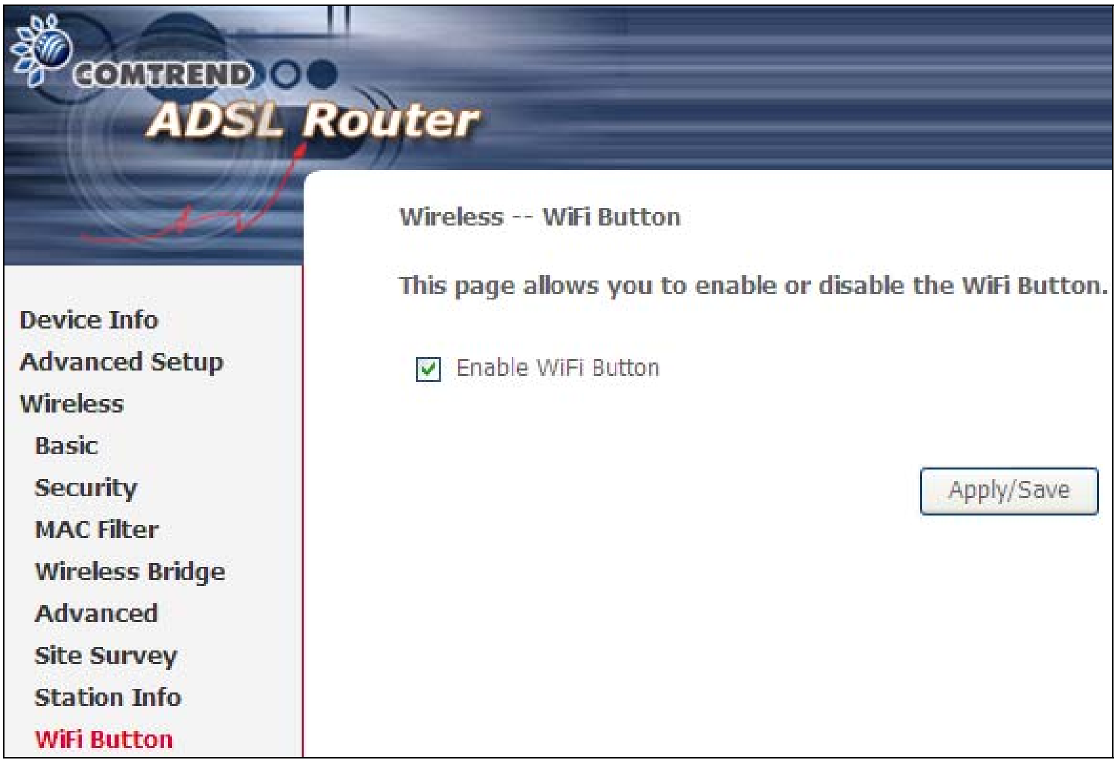
MAC	Associated	Authorized	SSID	Interface

Consult the table below for descriptions of each column heading.

Heading	Description
MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

6.8 WiFi Button

This page allows you to enable or disable the WiFi Button.



Wireless -- WiFi Button

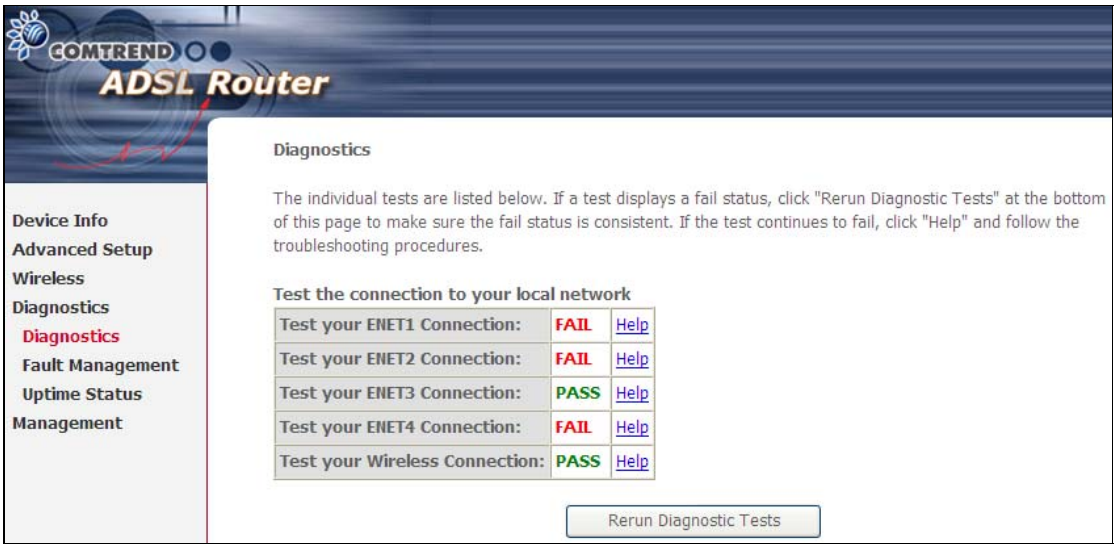
This page allows you to enable or disable the WiFi Button.

☑ Enable WiFi Button

Chapter 7 Diagnostics

7.1 Diagnostics – Individual Tests

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.



Diagnostics

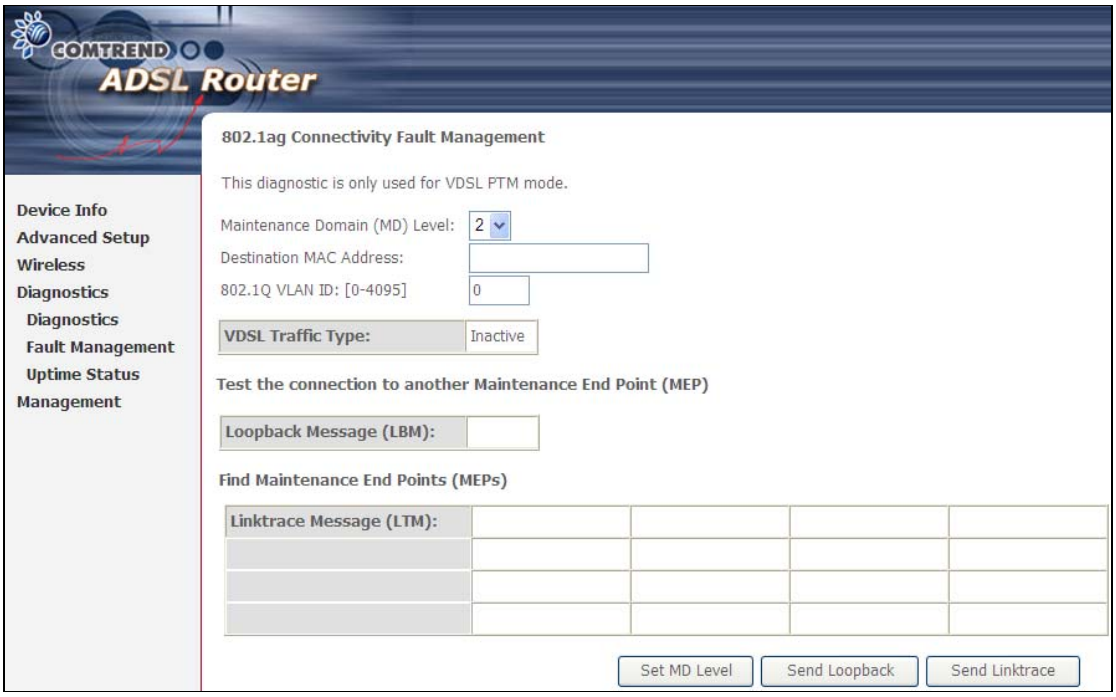
The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

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

7.2 Fault Management

Please note this function is not available on the AR5381U.



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):

Item	Description
Maintenance Domain (MD) Level	Management space on the network, the larger the domain, the higher the level value
Destination MAC Address	Destination MAC address for sending the loopback message
802.1Q VLAN ID: [0-4095]	802.1Q VLAN used in VDSL PTM mode

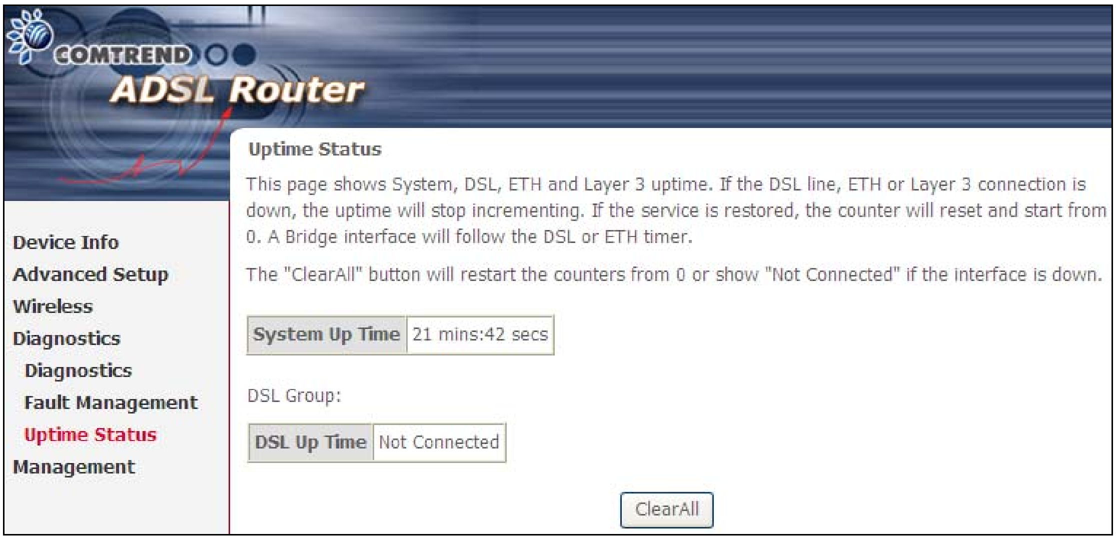
Set MD Level
Save the Maintenance domain level.

Send Loopback
Send loopback message to destination MAC address.

Send Linktrace
Send traceroute message to destination MAC address.

7.3 Uptime Status

This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.



Uptime Status

This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.

The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.

System Up Time	21 mins:42 secs

DSL Group:

DSL Up Time	Not Connected

The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.

Chapter 8 Management

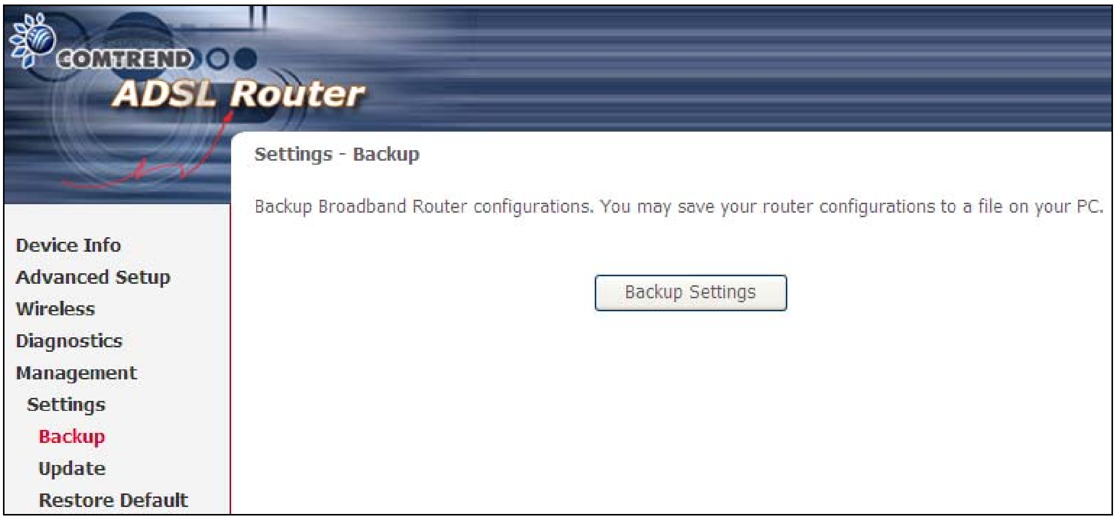
Click on the link to jump to a specific section:

8.1 Settings

This includes 8.1.1 Backup Settings, 8.1.2 Update Settings, and 8.1.3 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 backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.

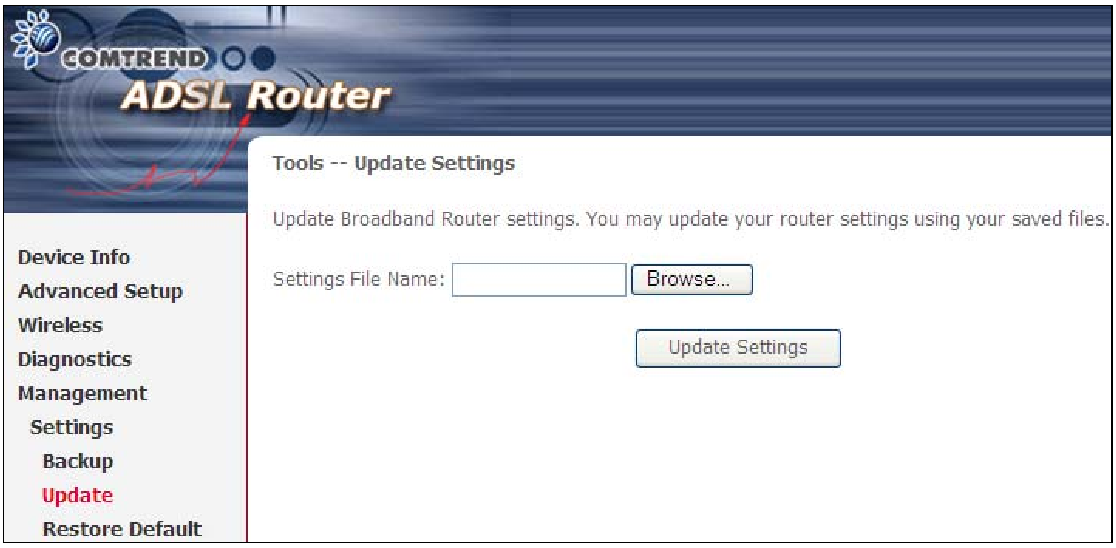


Settings - Backup

Backup Broadband 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.



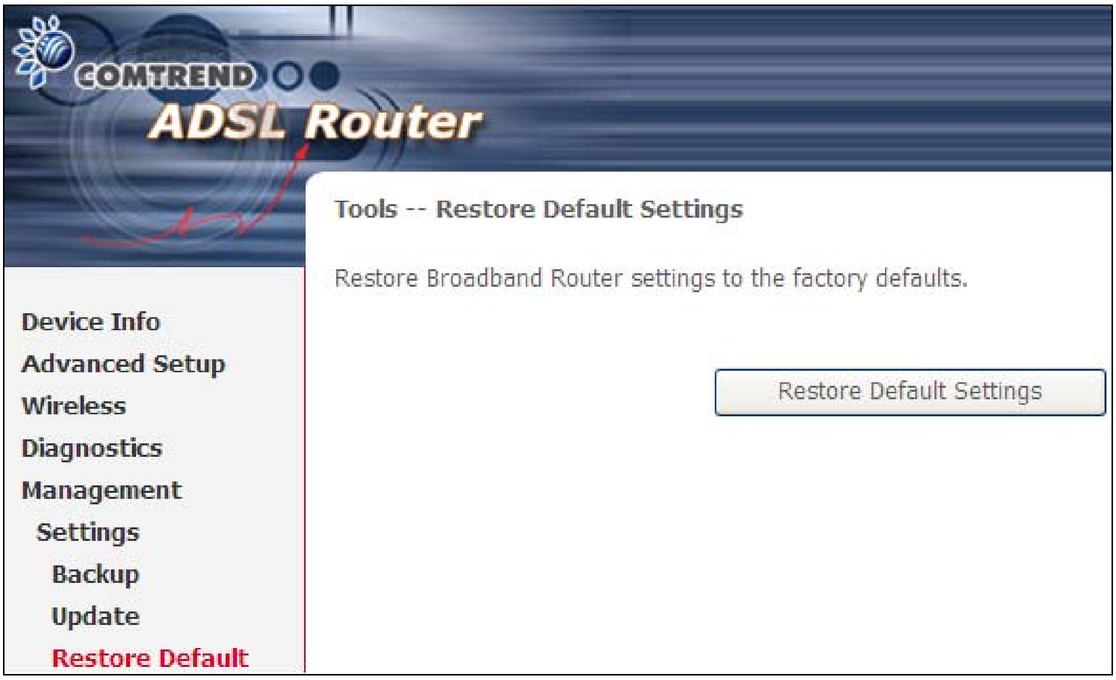
Tools -- Update Settings

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

Settings File Name:

8.1.3 Restore Default

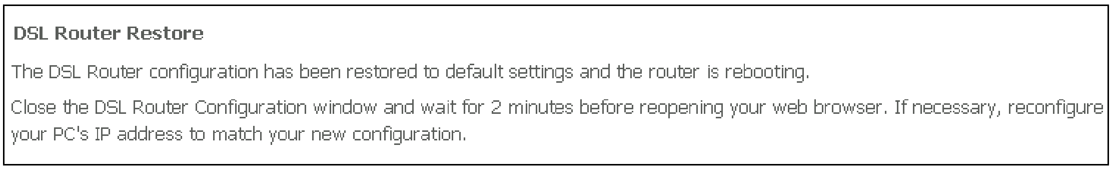
Click **Restore Default Settings** to restore factory default settings.



Tools -- Restore Default Settings

Restore Broadband 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.

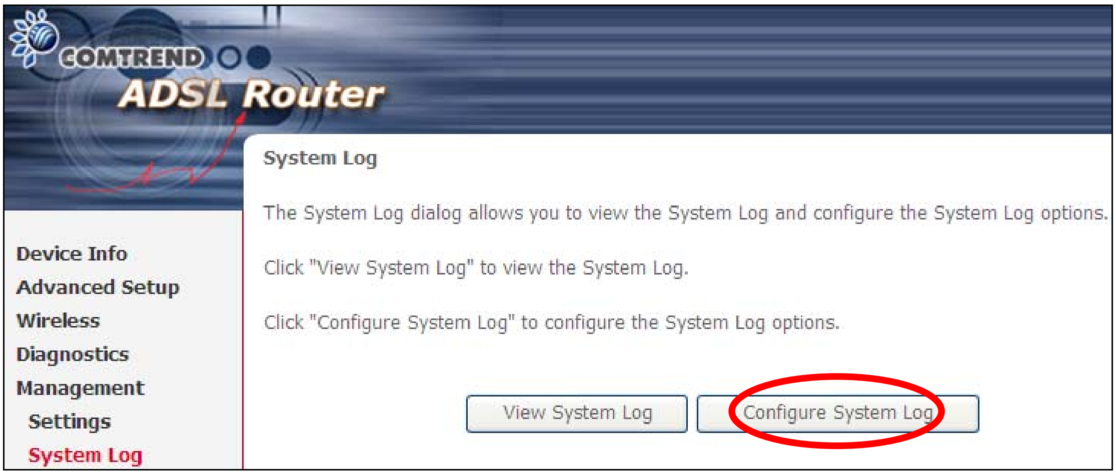
NOTE: This entry has the same effect as the **Reset** button. The AR-5381u board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 60 seconds, the boot loader will erase the configuration data saved in flash memory.

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**, as shown below (circled in **Red**).



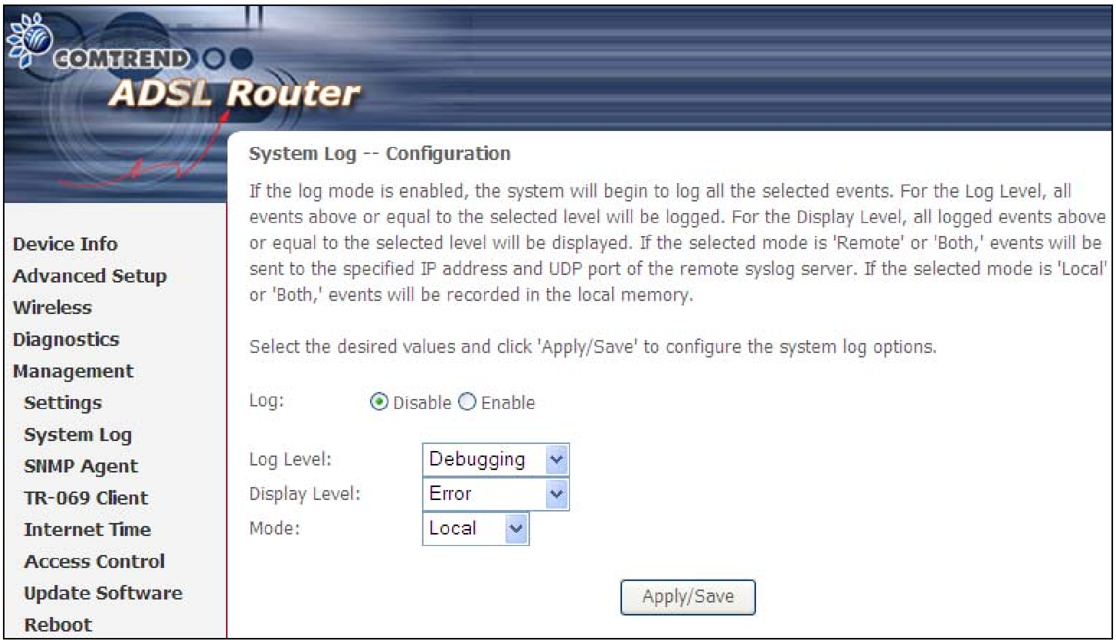
System Log

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

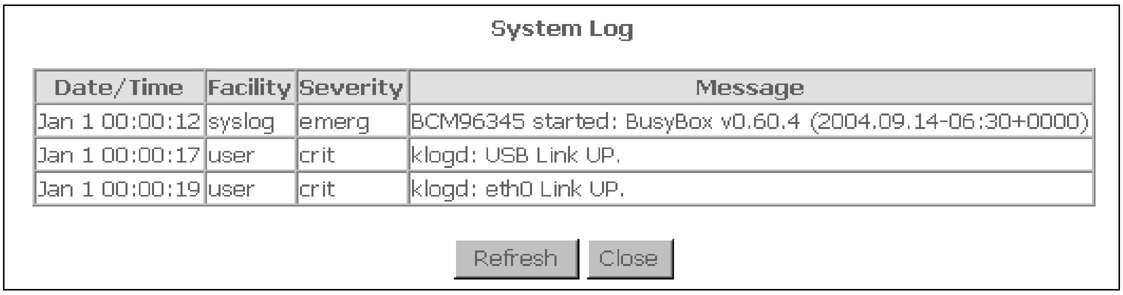
Mode: Local

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**.

Option	Description
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 AR-5381u 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 mode 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.

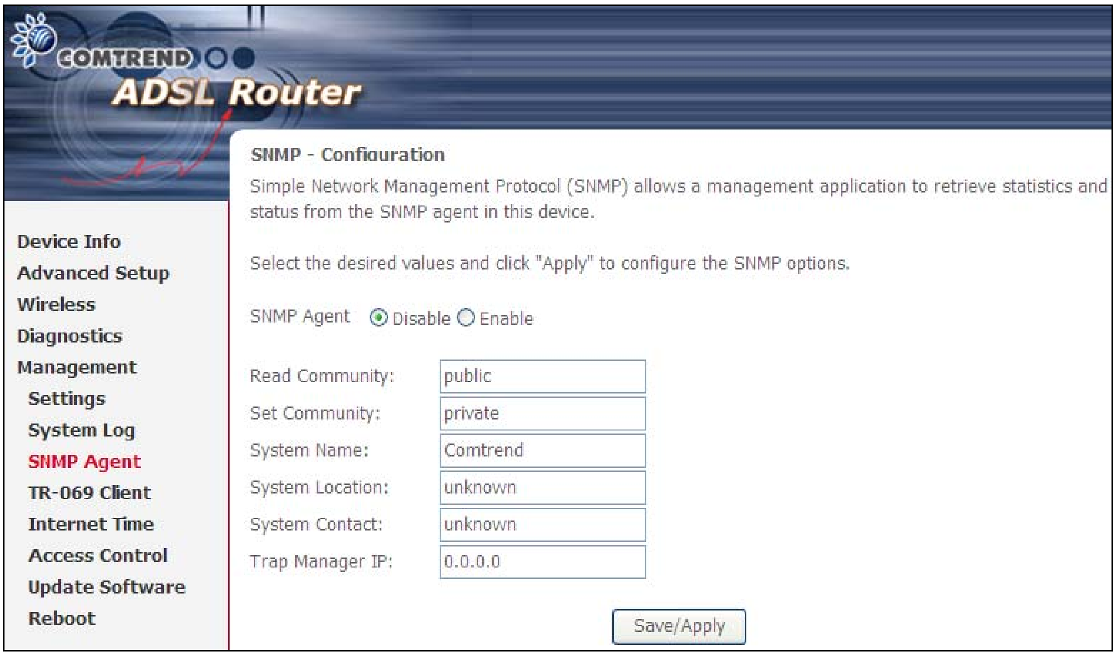


System Log

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 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options, and click **Save/Apply** to activate SNMP.



SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

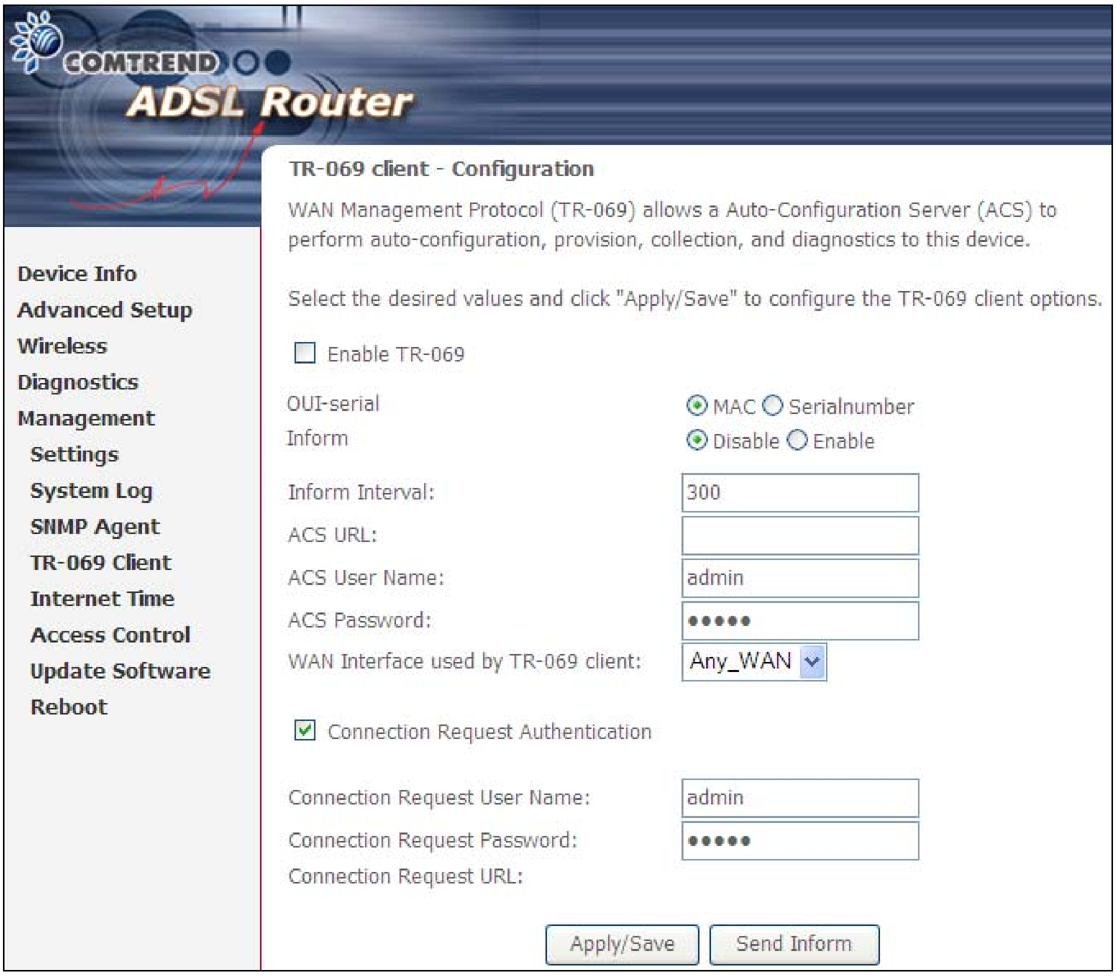
SNMP Agent ● Disable ○ Enable

Read Community:	public
Set Community:	private
System Name:	Comtrend
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

Save/Apply

8.4 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.

☐ Enable TR-069

OUI-serial ● MAC ○ Serialnumber

Inform ● Disable ○ Enable

Inform Interval: 300

ACS URL:

ACS User Name: admin

ACS Password: •••••

WAN Interface used by TR-069 client: Any_WAN

☑ Connection Request Authentication

Connection Request User Name: admin

Connection Request Password: •••••

Connection Request URL:

The table below is provided for ease of reference.

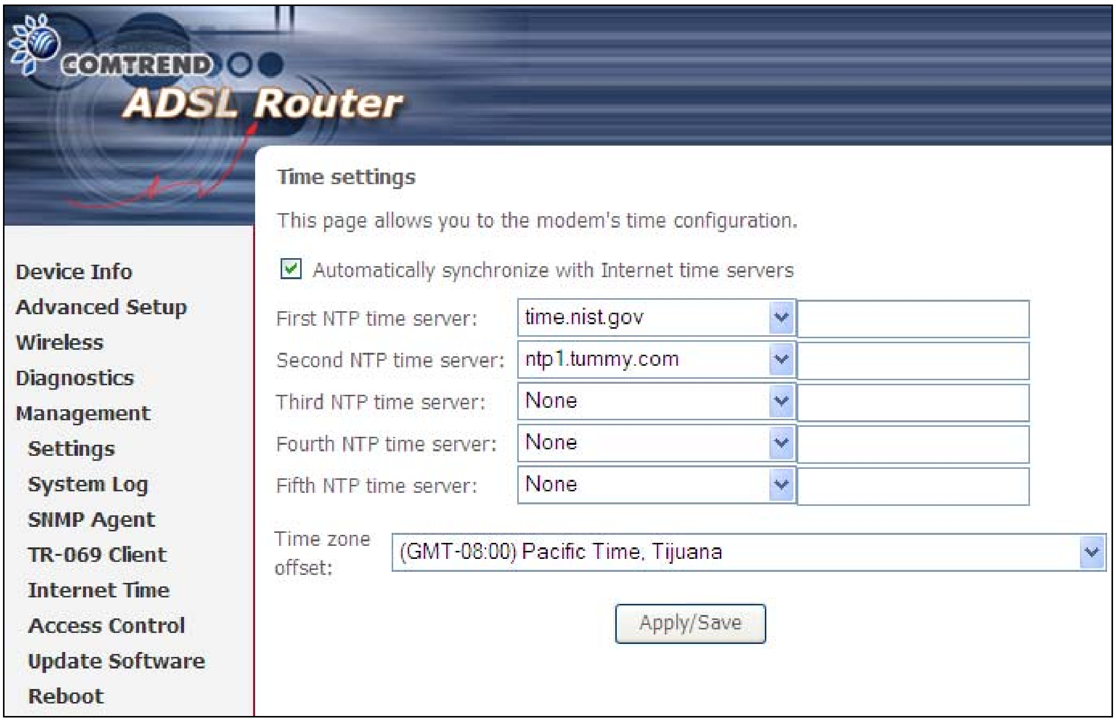
Option	Description
Enable TR-069	Tick the checkbox ☑ to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with ACS or select serial number to use router's serial number.
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.

Option	Description
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.
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.
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 AR5381U.

The **Send Inform** button forces the CPE to establish an immediate connection to the ACS.

8.5 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) Pacific Time, Tijuana

NOTE:	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.

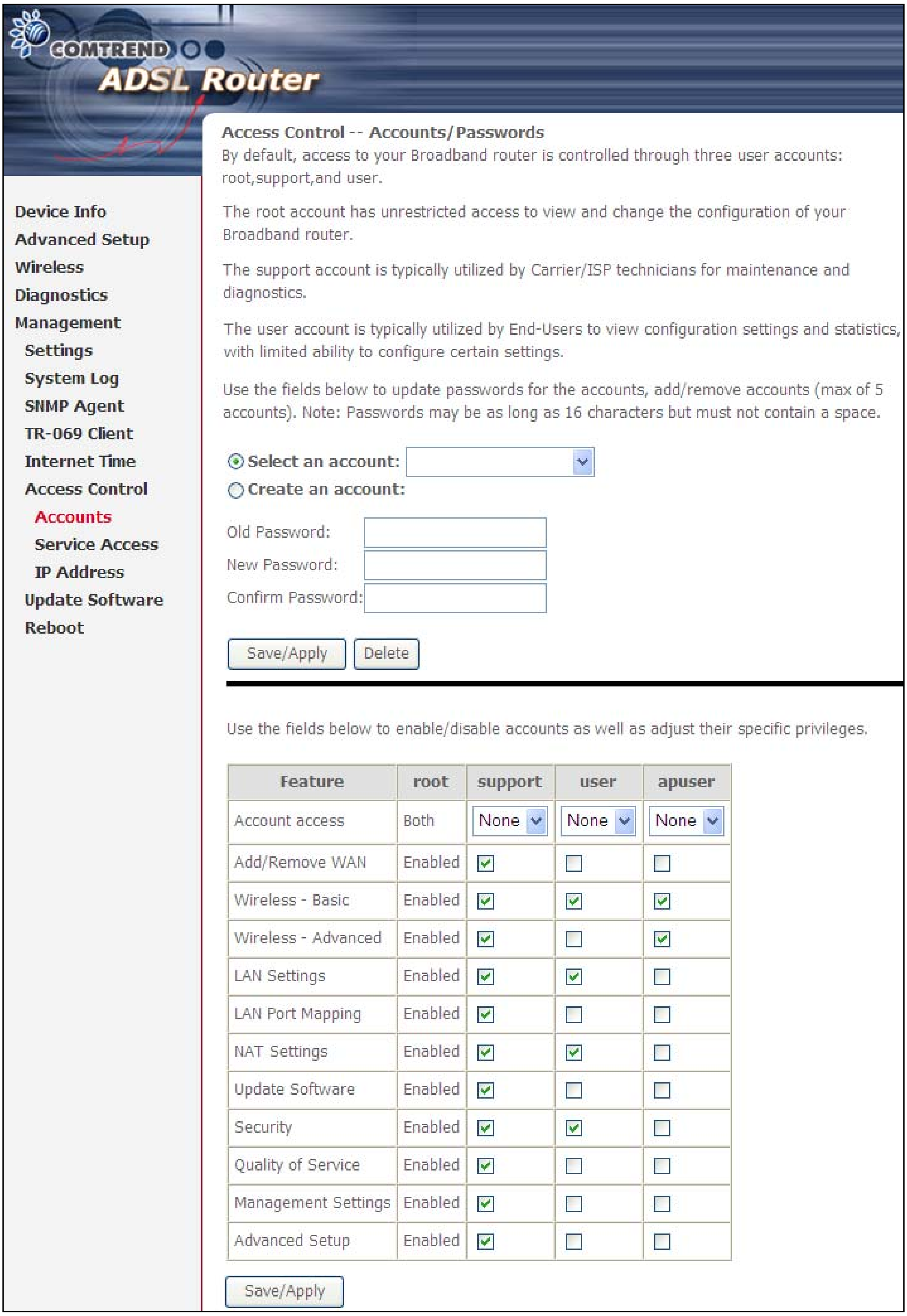
8.6 Access Control

8.6.1 Accounts/Passwords

This screen is used to configure the user account access passwords for the device. Access to the AR5381U is controlled through the following user accounts:

- **root** - unrestricted access to change and view the configuration.
- **support** - typically utilized by Carrier/ISP technicians for maintenance and diagnostics.
- **user** - can view configuration settings & statistics and update firmware.
- **apuser** - can configure wireless settings

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



Access Control -- Accounts/Passwords

By default, access to your Broadband router is controlled through three user accounts: root,support,and user.

The root account has unrestricted access to view and change the configuration of your Broadband router.

The support account is typically utilized by Carrier/ISP technicians for maintenance and diagnostics.

The user account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure certain settings.

Use the fields below to update passwords for the accounts, add/remove accounts (max of 5 accounts). Note: Passwords may be as long as 16 characters but must not contain a space.

● Select an account:

○ Create an account:

Old Password:

New Password:

Confirm Password:

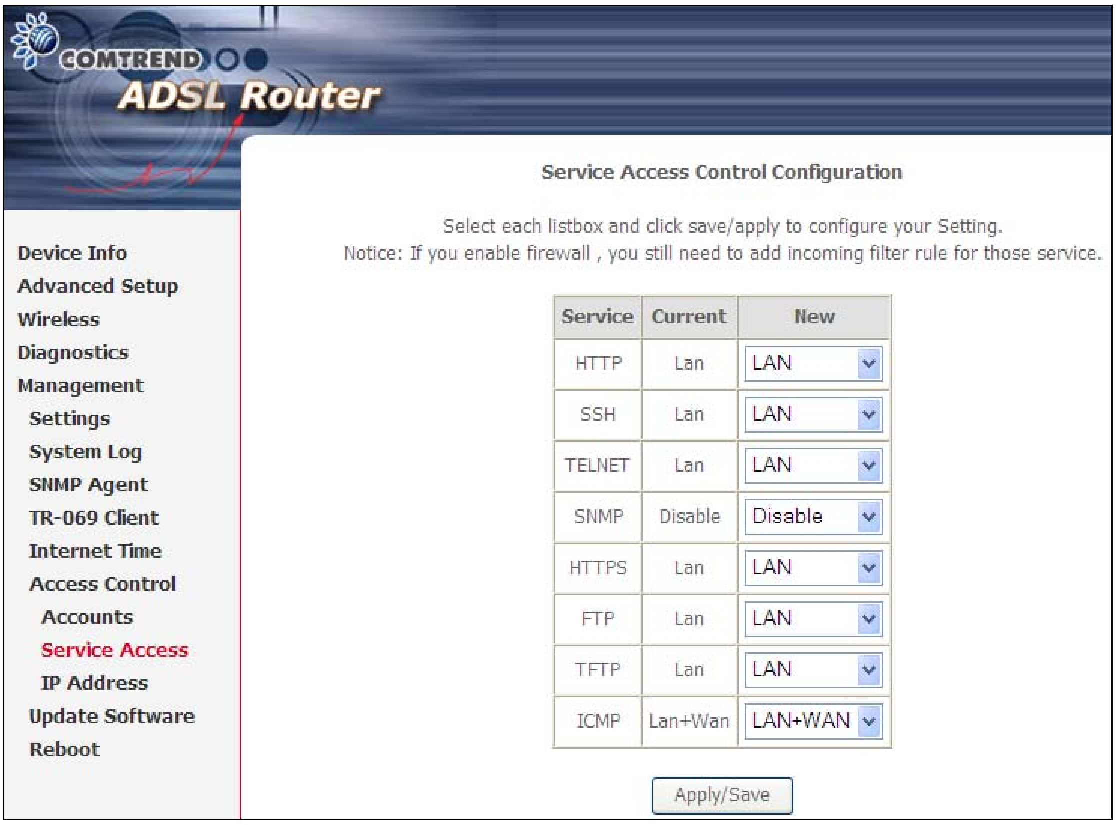
Use the fields below to enable/disable accounts as well as adjust their specific privileges.

Feature	root	support	user	apuser
Account access	Both	None	None	None
Add/Remove WAN	Enabled	☑	□	□
Wireless - Basic	Enabled	☑	☑	☑
Wireless - Advanced	Enabled	☑	□	☑
LAN Settings	Enabled	☑	☑	□
LAN Port Mapping	Enabled	☑	□	□
NAT Settings	Enabled	☑	☑	□
Update Software	Enabled	☑	□	□
Security	Enabled	☑	☑	□
Quality of Service	Enabled	☑	□	□
Management Settings	Enabled	☑	□	□
Advanced Setup	Enabled	☑	□	□

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

8.6.2 Service Access

The Services option limits or opens the access services over the LAN or WAN. These access services available are: FTP, HTTP, ICMP, SNMP, TELNET and TFTP. Enable a service by selecting its dropdown listbox. Click **SAVE / APPLY** to activate.



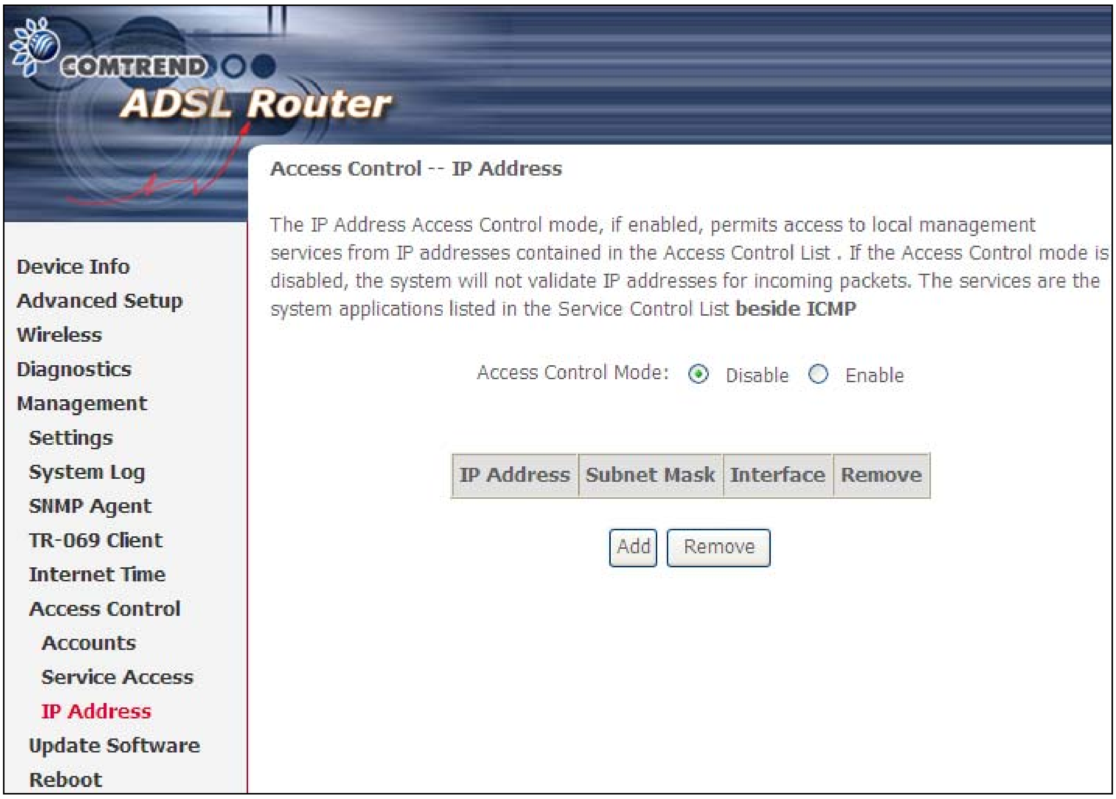
Service Access Control Configuration

Select each listbox and click save/apply to configure your Setting.
Notice: If you enable firewall , you still need to add incoming filter rule for those service.

Service	Current	New
HTTP	Lan	LAN
SSH	Lan	LAN
TELNET	Lan	LAN
SNMP	Disable	Disable
HTTPS	Lan	LAN
FTP	Lan	LAN
TFTP	Lan	LAN
ICMP	Lan+Wan	LAN+WAN

8.6.3 IP Address

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



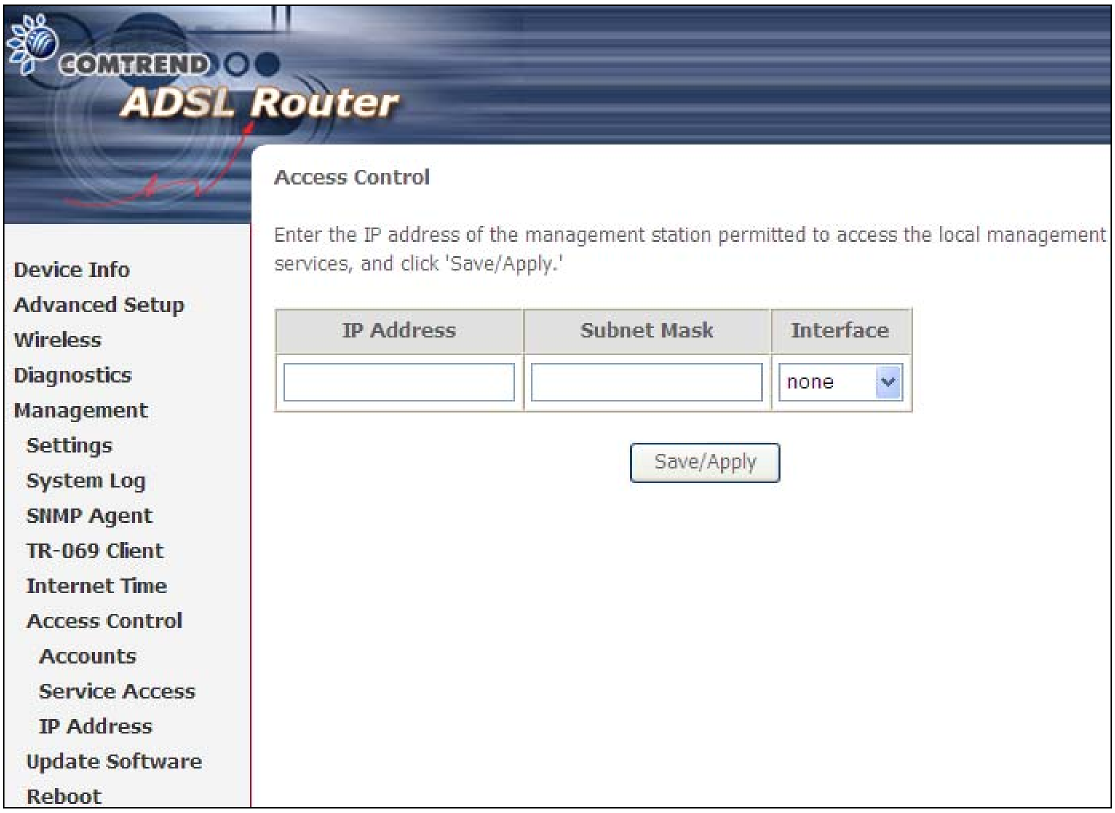
Access Control -- IP Address

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

Access Control Mode: ● Disable ○ Enable

IP Address	Subnet Mask	Interface	Remove

Click the Add button to display the following.



Access Control

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

IP Address	Subnet Mask	Interface
		none

Configure the address and subnet of the management station permitted to access the local management services, and click **Save/Apply**.

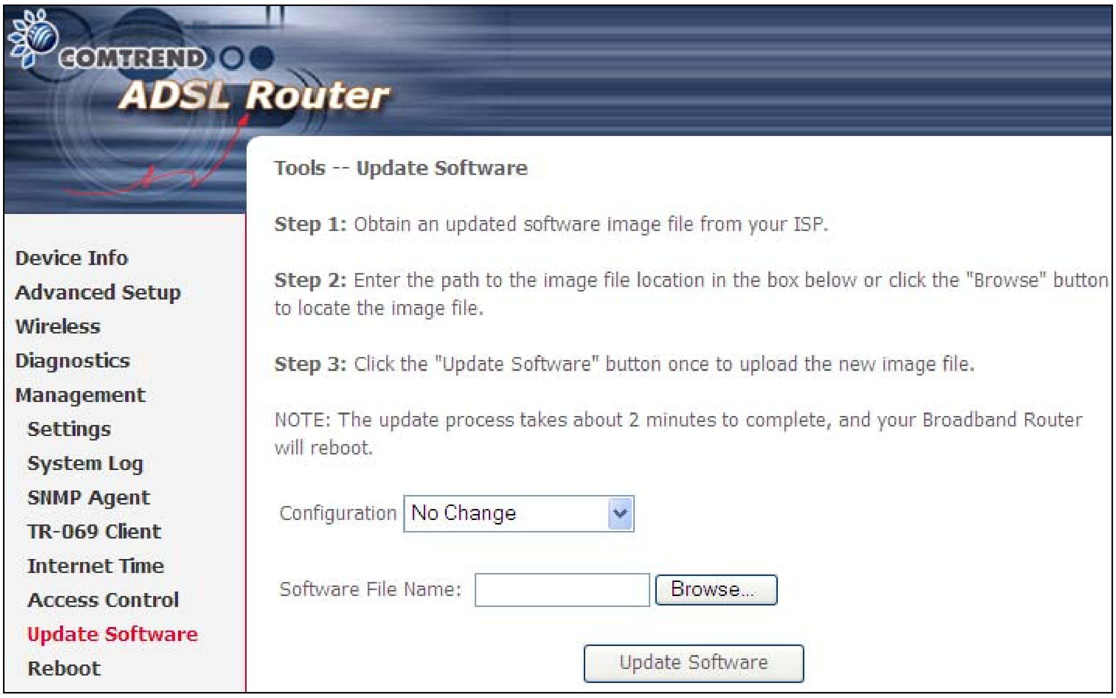
IP Address – IP address of the management station.

Subnet Mask – Subnet address for the management station.

Interface – Access permission for the specified address, allowing the address to access the local management service from none/lan/wan/lan&wan interfaces.

8.7 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 Broadband Router will reboot.

Configuration: No Change

Software File Name:

Configuration: Select for the three options available.

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

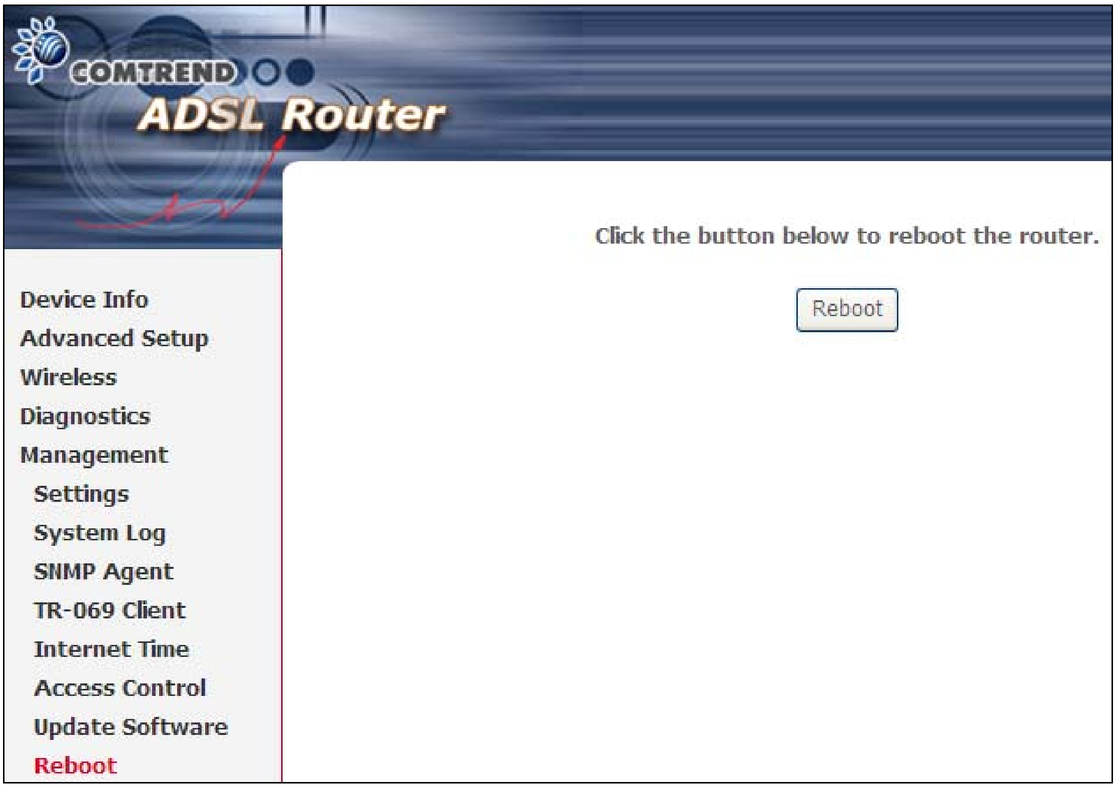
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

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 Chapter 4 Device Information screen with the firmware version installed, to confirm the installation was successful.

8.8 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.

Appendix B - Specifications

Hardware Interface

- RJ-11 X 1 for ADSL
- RJ-45 X 4 for LAN (10/100 Base-T auto-sense)
- Reset Button X 1
- WPS Button X 1
- Wi-Fi On/Off Button X 1
- Power Switch X 1
- USB Host X 1
- Wi-Fi internal Antenna X 2

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
- ADSL2 Downstream : 12 Mbps Upstream : 1.3 Mbps

LAN Interface

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

Wireless Interface

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption/ WPA/WPA2 encryption
- 11 Channels
- Up to 300Mbps data rate
- WPA/WPA2 Yes
- IEEE 802.1x Yes
- Afterburner mode (Turbo mode) Yes (this feature is optional)
- RF operating Frequency 2.412-2.462GHz
- WMM Yes

Management

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

Networking Protocols

- RFC2684 VC-MUX, LLC/SNAP encapsulations for bridged or routed packet
- RFC2364 PPP over AAL5
- IPoA, PPPoA, PPPoE, Multiple PPPoE sessions on single PVC, PPPoE pass-through
- PPPoE filtering of on-PPPoE packets between WAN and LAN
- Transparent bridging between all LAN and WAN interfaces
- 802.1p/802.1q VLAN support

- Spanning Tree Algorithm
- IGMP Proxy V1/V2/V3, IGMP Snooping V1/V2/V3, Fast leave
- Static route, RIP v1/v2, ARP, RARP, SNTP, DHCP Server/Client/Relay,
- DNS Relay, Dynamic DNS,
- IPv6 subset

Security Functions

- PAP, CHAP, TCP/IP/Port filtering rules
- Port triggering/Forwarding,
- Packet and MAC address filtering, Access control, SSH access

QoS

- L3 policy-based QoS, IP QoS, ToS

Firewall/Filtering

- Stateful Inspection Firewall
- Stateless Packet Filter
- Denial of Service (DOS): ARP attacks, Ping attacks, Ping of Death, LAND,SYNC, Smurf, Unreachable, Teardrop
- TCP/IP/Port/interface filtering rules Support both incoming and outgoing filtering

NAT/NAPT

- Support Port Triggering and Port forwarding
- Symmetric port-overloading NAT, Full-Cone NAT
- Dynamic NAPT (NAPT N-to-1)
- Support DMZ host
- Virtual Server
- VPN Passthrough (PPTP, L2TP, IPSec)

Application Passthrough

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

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.................................. 158 mm (W) x 40 mm (H) x 136 mm (D)

Certifications................................. CE, Wi-Fi 802.11n

Kit Weight

(1*AR-5381u, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM) =0.6 kg

NOTE: Specifications are subject to change without notice

Appendix C - 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 admin 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 admin 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

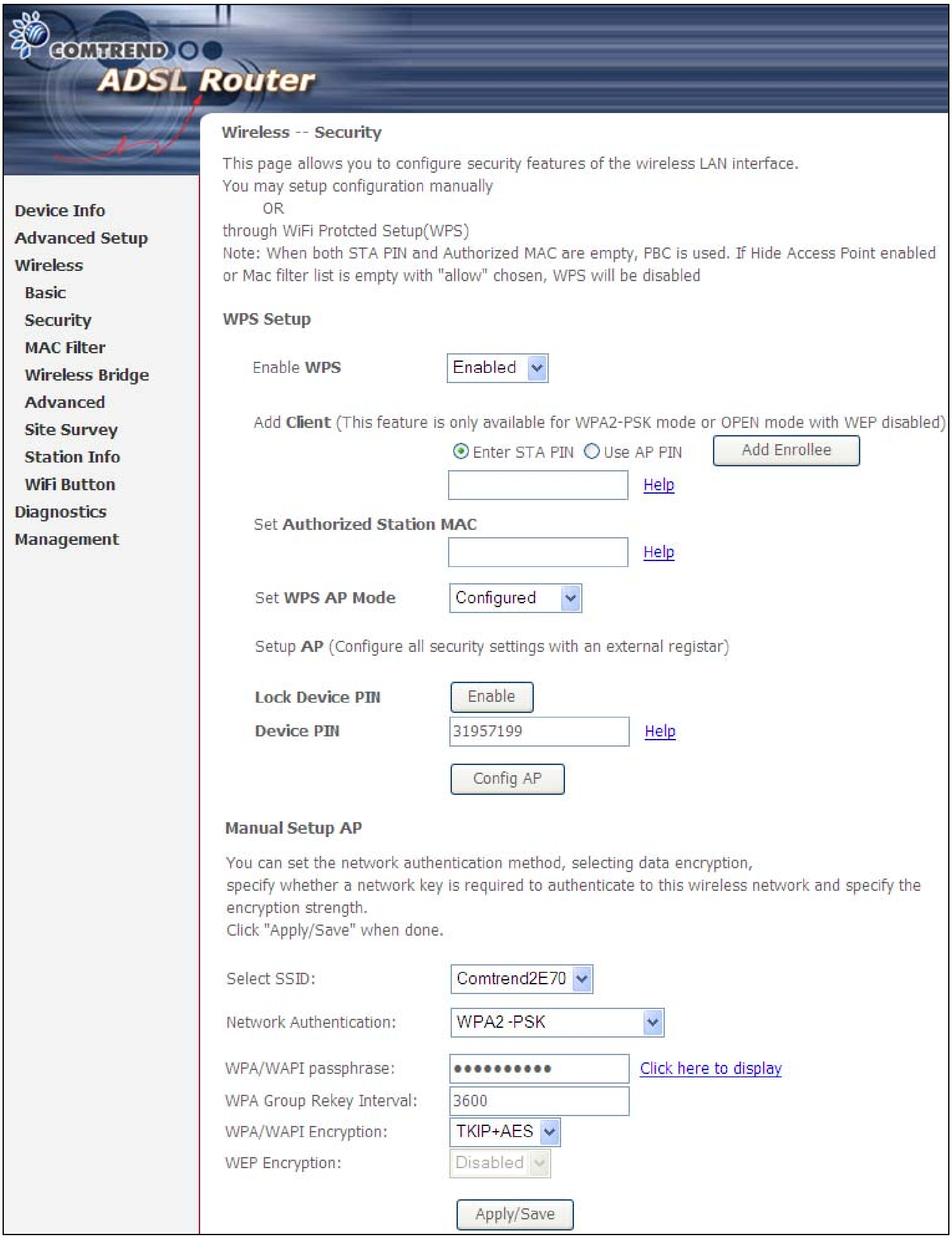
Appendix D - WPS OPERATION

This Section shows the basic AP WPS Operation procedure.

E1 Add Enrollee with Pin Method

1) Select Radio button “STA Pin”
2) Input Pin from Enrollee Station (31957199 in this example)

3) Click “Add Enrollee”



Wireless -- Security

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

WPS Setup

Enable **WPS**: Enabled

Add **Client** (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)
● Enter STA PIN ○ Use AP PIN

Set **Authorized Station MAC**

Set **WPS AP Mode**: Configured

Setup **AP** (Configure all security settings with an external registar)

Lock Device PIN

Device PIN: 31957199

Manual Setup AP

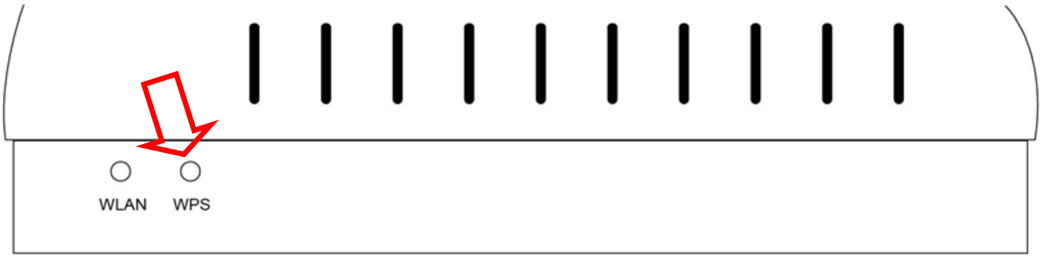
You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID: Comtrend2E70
Network Authentication: WPA2 -PSK
WPA/WAPI passphrase: ●●●●●●●●●●●
WPA Group Rekey Interval: 3600
WPA/WAPI Encryption: TKIP+AES
WEP Encryption: Disabled

4) Operate Station to start WPS Adding Enrollee.

E2 Add Enrollee with PBC Method

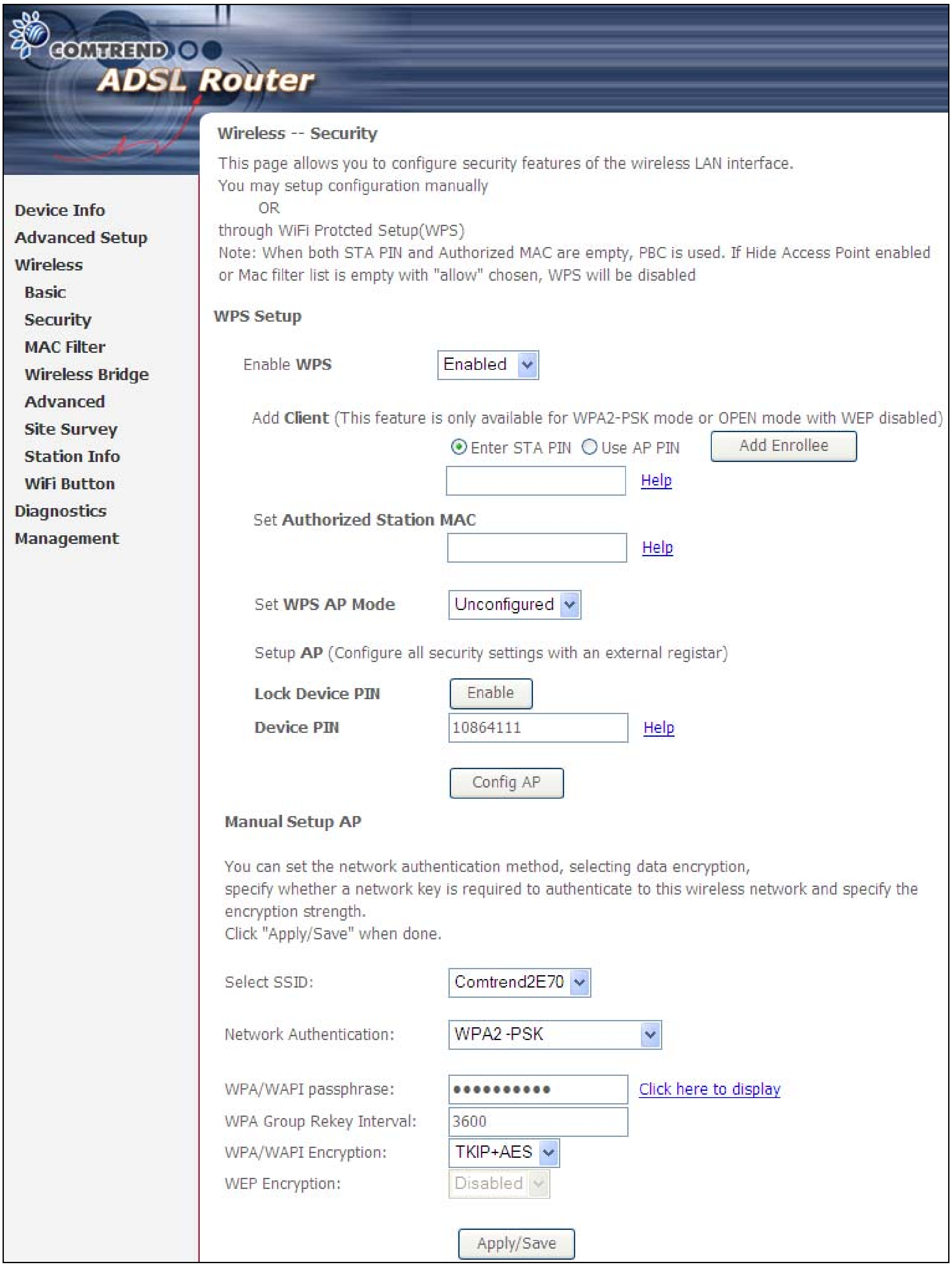
1) Press the WPS button at back of the device to activate WPS PBC operation.



2) Operate Station (your dongle for example) to start WPS Adding Enrollee.

E3 Configure AP

1) Set AP to “Unconfigured Mode” and Click “Config AP” button.



Wireless -- Security

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

WPS Setup

Enable WPS: Enabled

Add Client (This feature is only available for WPA2-PSK mode or OPEN mode with WEP disabled)
● Enter STA PIN ○ Use AP PIN [Add Enrollee]
Help

Set Authorized Station MAC
Help

Set WPS AP Mode: Unconfigured

Setup AP (Configure all security settings with an external registar)

Lock Device PIN [Enable]
Device PIN: 10864111 Help

[Config AP]

Manual Setup AP

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

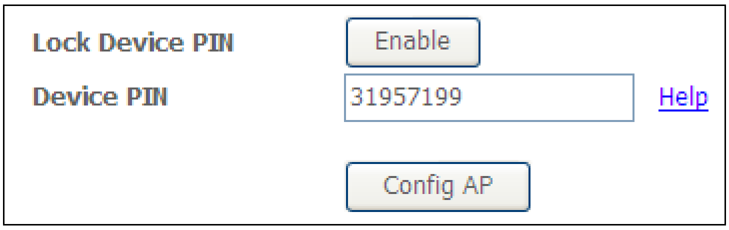
Select SSID: Comtrend2E70

Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ●●●●●●●●●●● Click here to display
WPA Group Rekey Interval: 3600
WPA/WAPI Encryption: TKIP+AES
WEP Encryption: Disabled

[Apply/Save]

Please see the further description below.

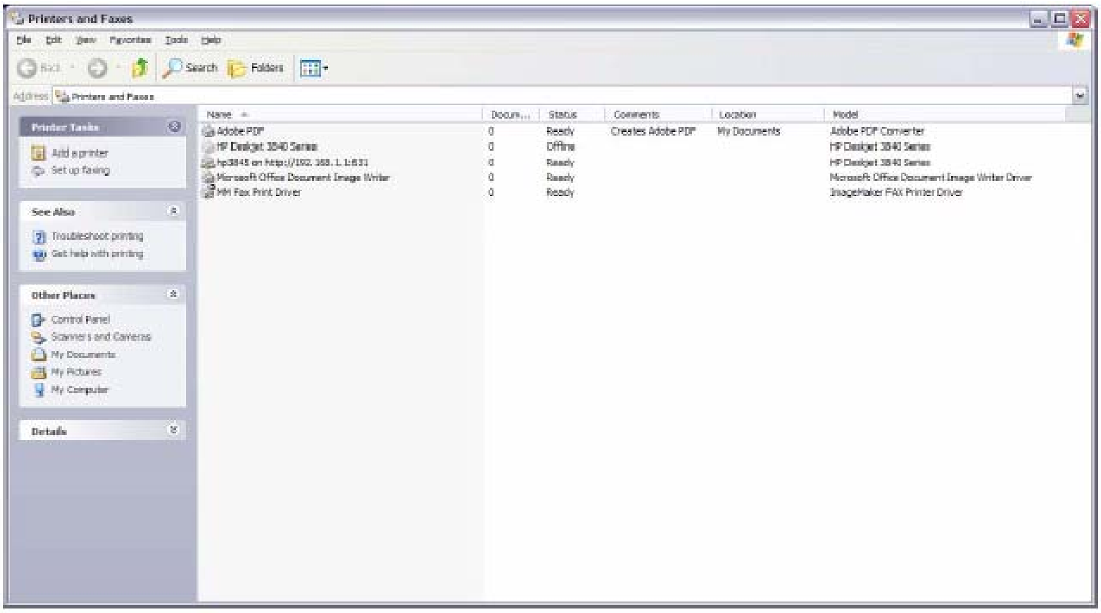


Lock Device PIN	Enable	
Device PIN	31957199	Help
	Config AP	

Lock Device PIN
When enabled, device PIN is locked and cannot be used for WPS operation.

2) Read the Device Pin (31957199 in this example) and input to External Registrar(ER – your dongle for example) when ER asks Device Pin ER could be wired (for example Windows Vista) or wireless (Intel Station).

3) Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.



Name	Docum...	Status	Comments	Location	Model
Adobe PDF	0	Ready	Creates Adobe PDF	My Documents	Adobe PDF Converter
HP Deskjet 3840 Series	0	Offline			HP Deskjet 3840 Series
hp3845 on http://192.168.1.1:631	0	Ready			HP Deskjet 3840 Series
Microsoft Office Document Image Writer	0	Ready			Microsoft Office Document Image Writer Driver
MM Fax Print Driver	0	Ready			ImageMaker FAX Printer Driver

Appendix E - Connection Setup

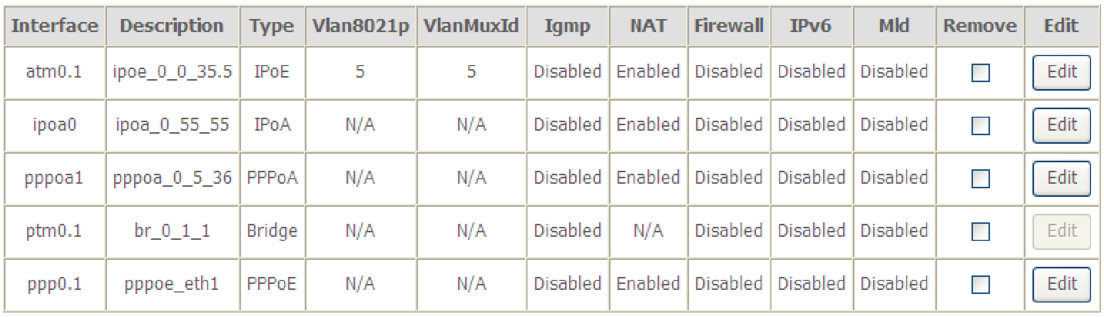
Creating a WAN connection is a two-stage process.

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

The following sections describe each stage in turn.

E1 ~ Layer 2 Interfaces

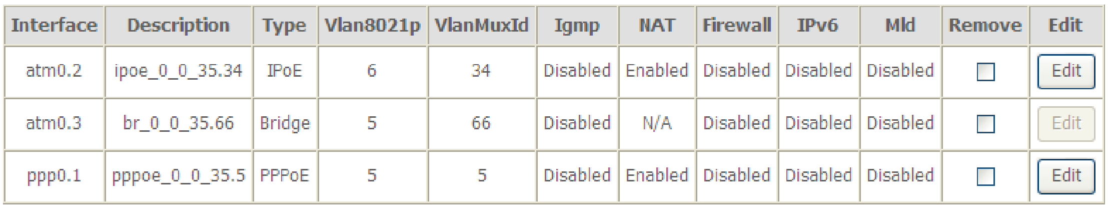
Layer2 interface supports VLAN Mux modes, which allow for multiple connections over a single interface. PPPoE, IPoE, and Bridge are supported while PPPoA and IPoA connections are not.
The figure below shows multiple connections over a single VLAN Mux interface.



Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm0.1	ipoe_0_0_35.5	IPoE	5	5	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
ipoa0	ipoa_0_55_55	IPoA	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
pppoa1	pppoa_0_5_36	PPPoA	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
ptm0.1	br_0_1_1	Bridge	N/A	N/A	Disabled	N/A	Disabled	Disabled	Disabled	□	Edit
ppp0.1	pppoe_eth1	PPPoE	N/A	N/A	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit

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.



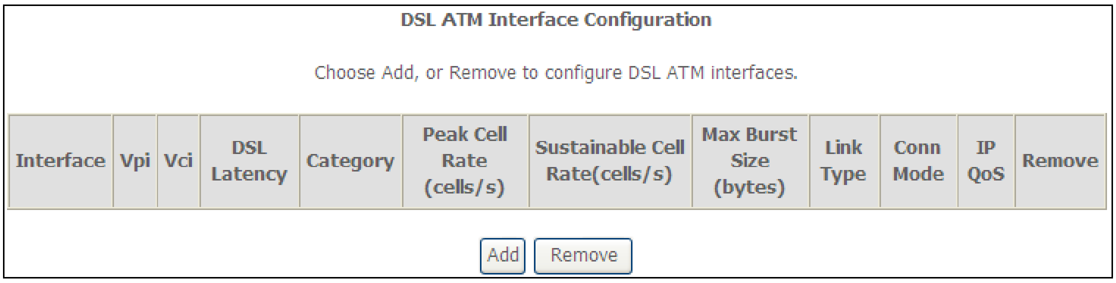
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
atm0.2	ipoe_0_0_35.34	IPoE	6	34	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit
atm0.3	br_0_0_35.66	Bridge	5	66	Disabled	N/A	Disabled	Disabled	Disabled	□	Edit
ppp0.1	pppoe_0_0_35.5	PPPoE	5	5	Disabled	Enabled	Disabled	Disabled	Disabled	□	Edit

E1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE: The AR-5381u 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.

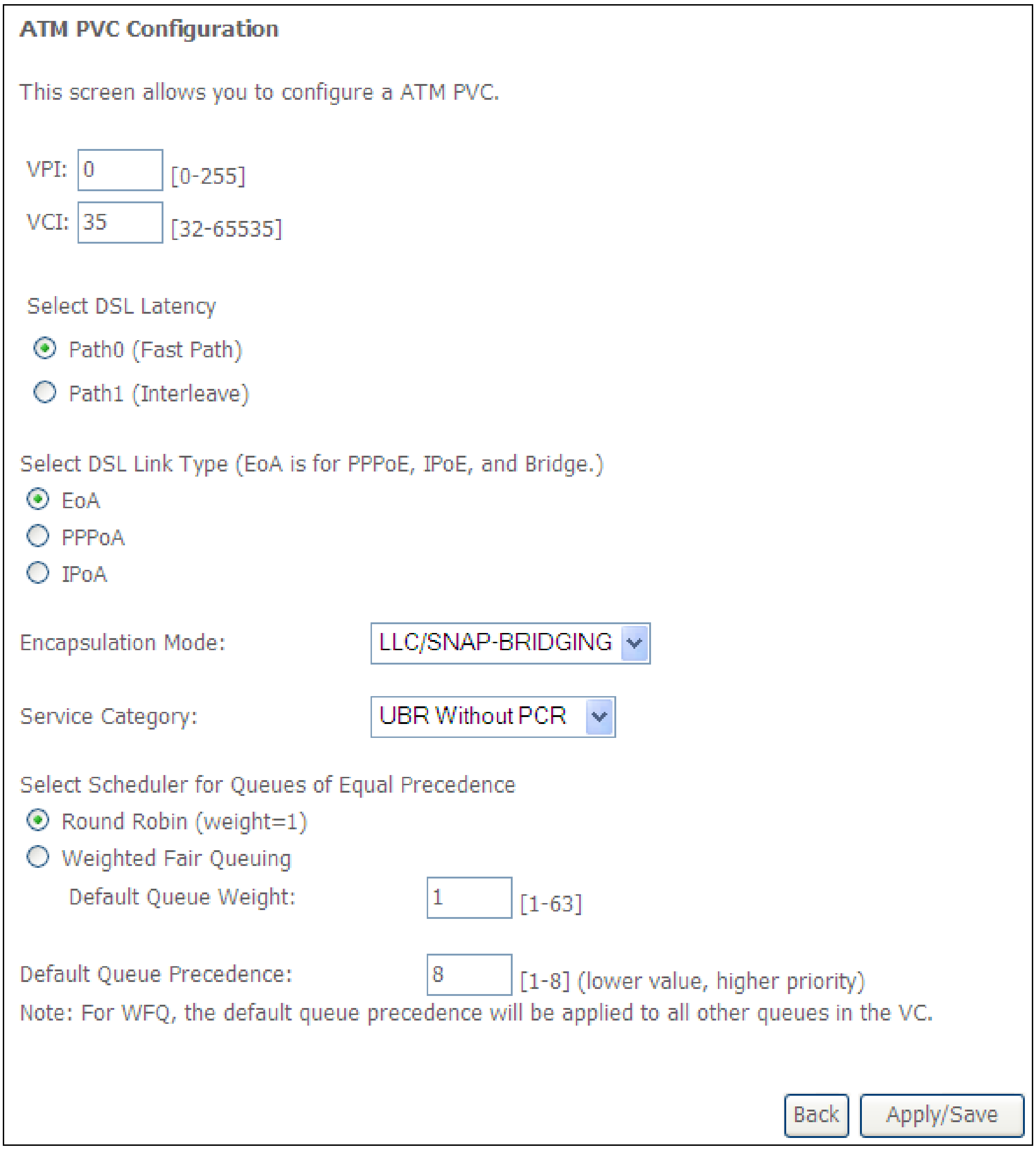
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate (cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size (bytes)	Link Type	Conn Mode	IP QoS	Remove

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} → port ID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	ATM service category
Peak Cell Rate	Maximum allowed traffic rate for the ATM PCR service connection
Sustainable Cell Rate	The average allowable, long-term cell transfer rate on the VBR service connection
Max Burst Size	The maximum allowable burst size of cells that can be transmitted contiguously on the VBR service connection
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
IP QoS	Quality of Service (IP 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 a ATM PVC.

VPI: 0 [0-255]

VCI: 35 [32-65535]

Select DSL Latency

● Path0 (Fast Path)

○ Path1 (Interleave)

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

● EoA

○ PPPoA

○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select Scheduler for Queues of Equal Precedence

● Round Robin (weight=1)

○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

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

Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

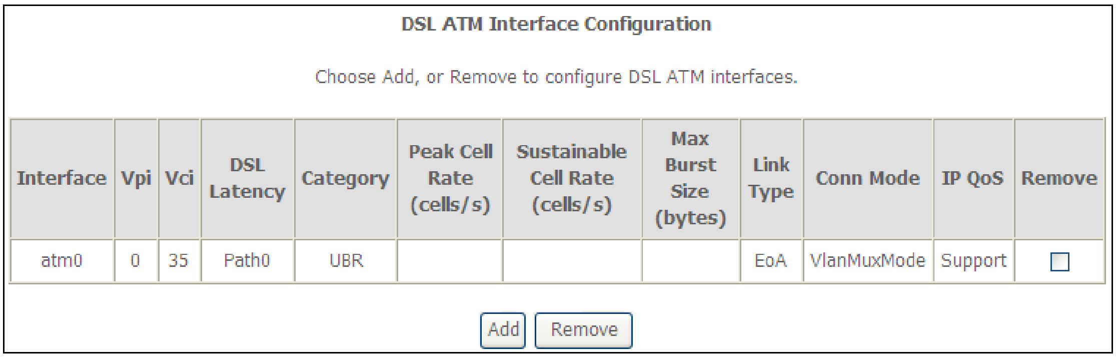
There are many settings here including: VPI/VCI, DSL Latency, DSL Link Type, Encapsulation Mode, Service Category, Connection Mode and Quality of Service.

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	Peak Cell Rate (cells/s)	Sustainable Cell Rate (cells/s)	Max Burst Size (bytes)	Link Type	Conn Mode	IP QoS	Remove
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	□

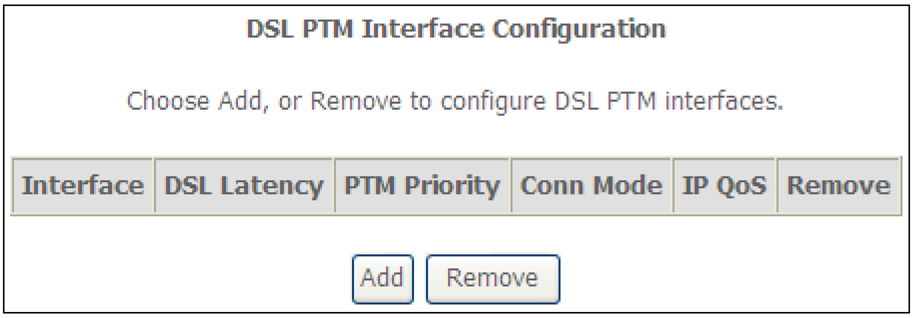
To add a WAN connection go to E2 ~ WAN Connections.

E1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

NOTE: The AR5381u can support two 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.

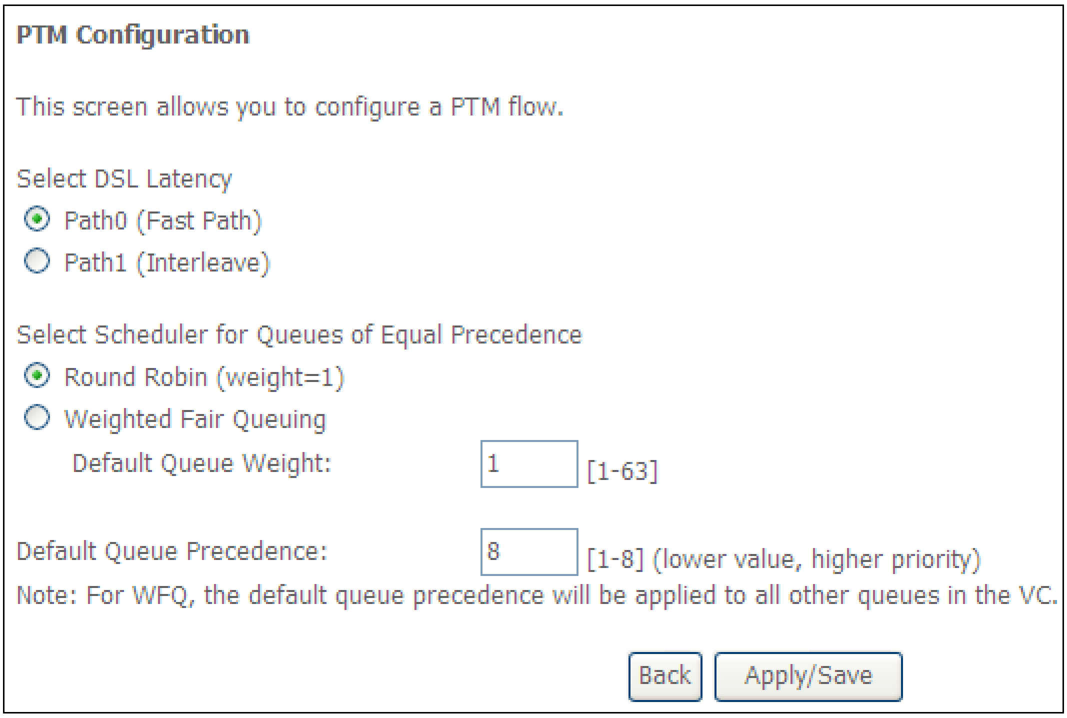
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove

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 flow.

Select DSL Latency

- ● Path0 (Fast Path)
- ○ Path1 (Interleave)

Select Scheduler for Queues of Equal Precedence

- ● Round Robin (weight=1)
- ○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

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

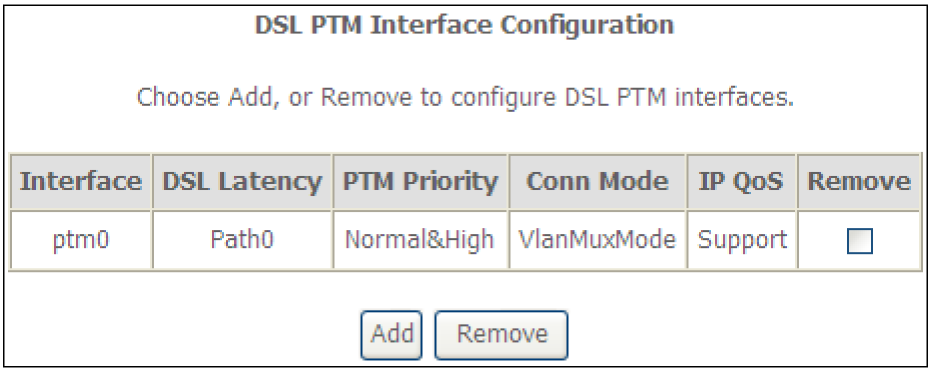
Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

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	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	□

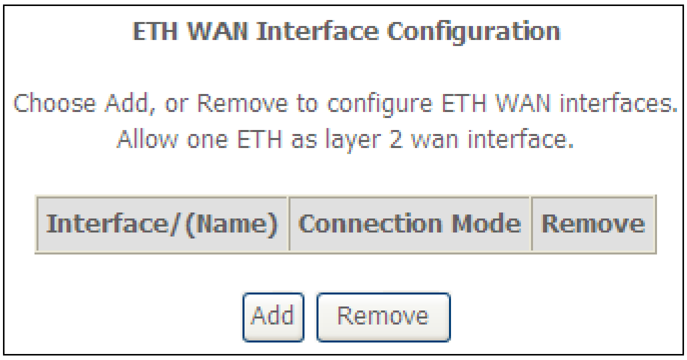
To add a WAN connection go to E2 ~ WAN Connections.

E1.3 Ethernet WAN Interface

Some models of the AR5381U support a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet WAN interface.

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

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



ETH WAN Interface Configuration

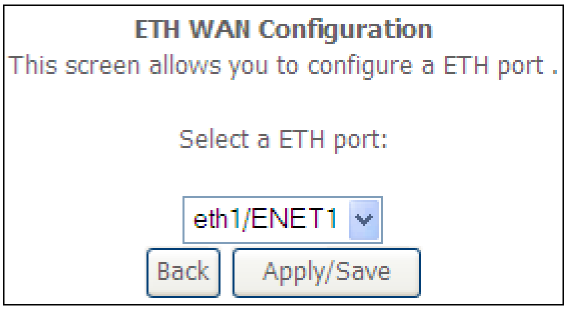
Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove

This table is provided here for ease of reference.

Heading	Description
Interface/ (Name)	ETH WAN Interface
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
Remove	Select the checkbox and click **Remove** to remove the connection.

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



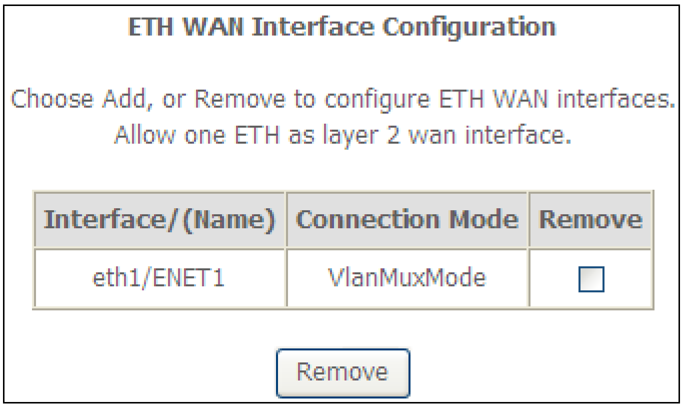
ETH WAN Configuration
This screen allows you to configure a ETH port .

Select a ETH port:

eth1/ENET1

STEP 3: **STEP 4:** Click **Apply/Save** to confirm your choice.

The figure below shows an Ethernet WAN interface configured in VlanMuxMode.



ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove
eth1/ENET1	VlanMuxMode	□

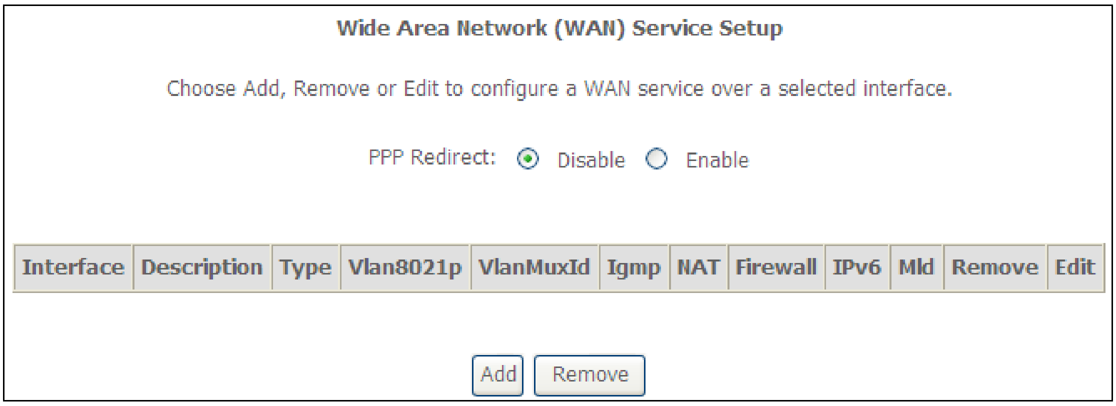
To add a WAN connection go to Appendix E - Connection Setup.

E2 ~ WAN Connections

In Default Mode, the AR5381U supports up to 16 connections.

To setup a WAN connection follow these instructions.

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



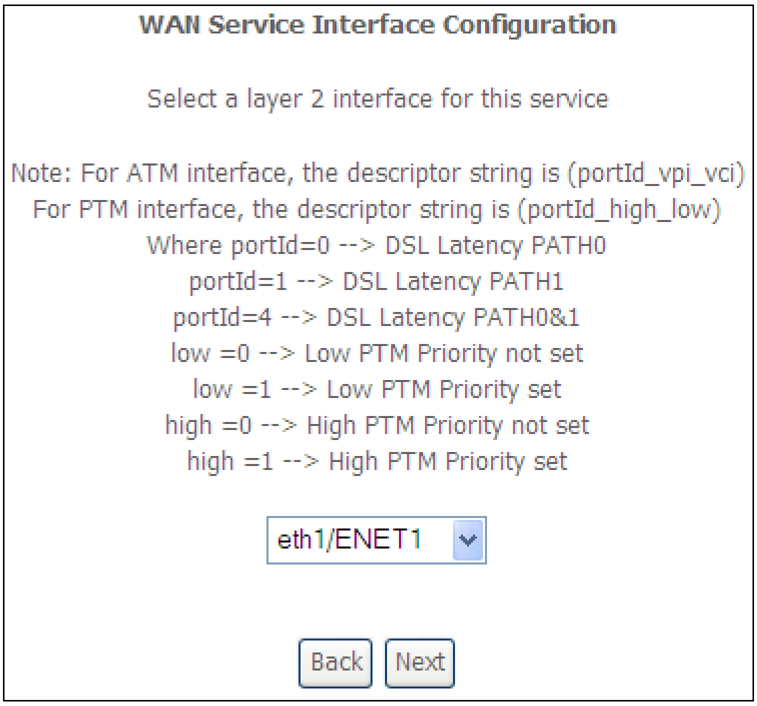
Wide Area Network (WAN) Service Setup

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

PPP Redirect: ● Disable ○ Enable

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

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



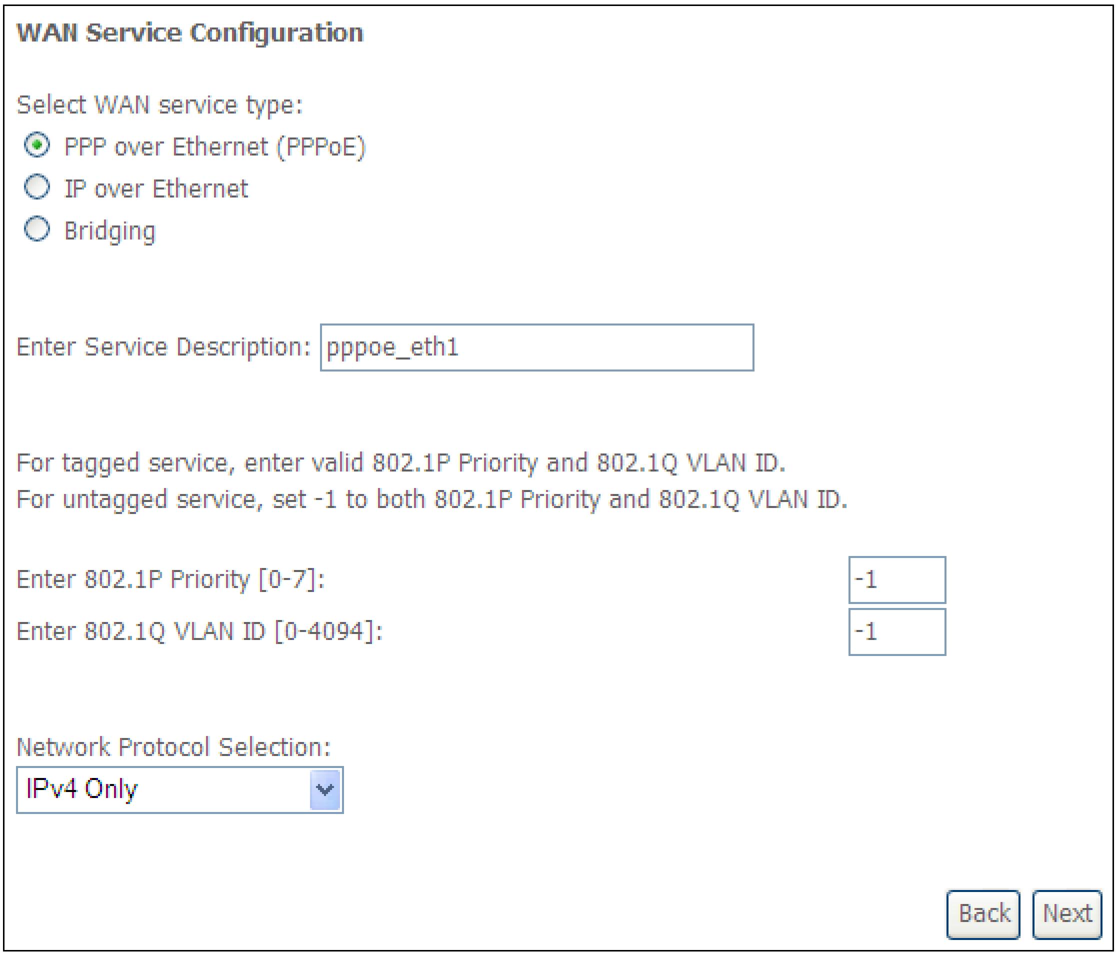
WAN Service Interface Configuration

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

eth1/ENET1

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_eth1

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

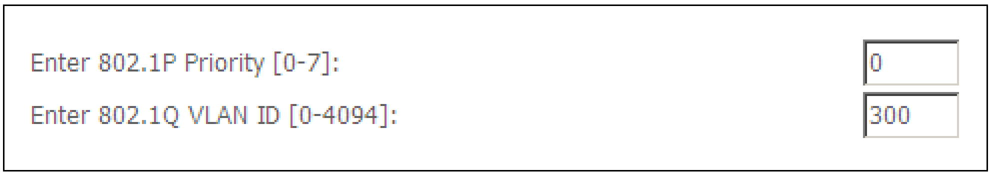
Enter 802.1P Priority [0-7]: -1

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

Network Protocol Selection: IPv4 Only

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, you must enter Priority & VLAN ID tags.



Enter 802.1P Priority [0-7]: 0

Enter 802.1Q VLAN ID [0-4094]: 300

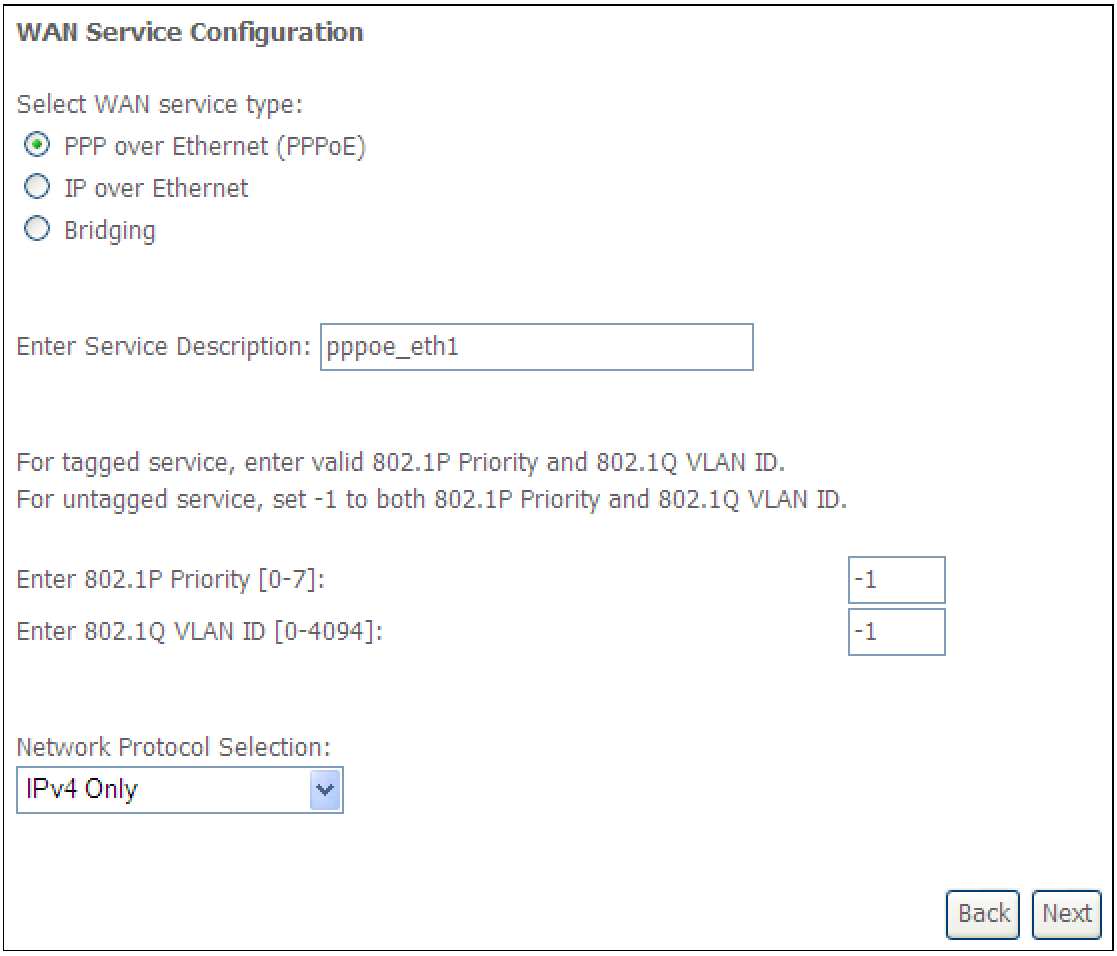
STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) For PPP over ETHERNET (PPPoE), go to page 156.
(2) For IP over ETHERNET (IPoE), go to page 162.
(3) For Bridging, go to page 168.
(4) For PPP over ATM (PPPoA), go to page 170.
(5) For IP over ATM (IPoA), go to page 175.

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_eth1

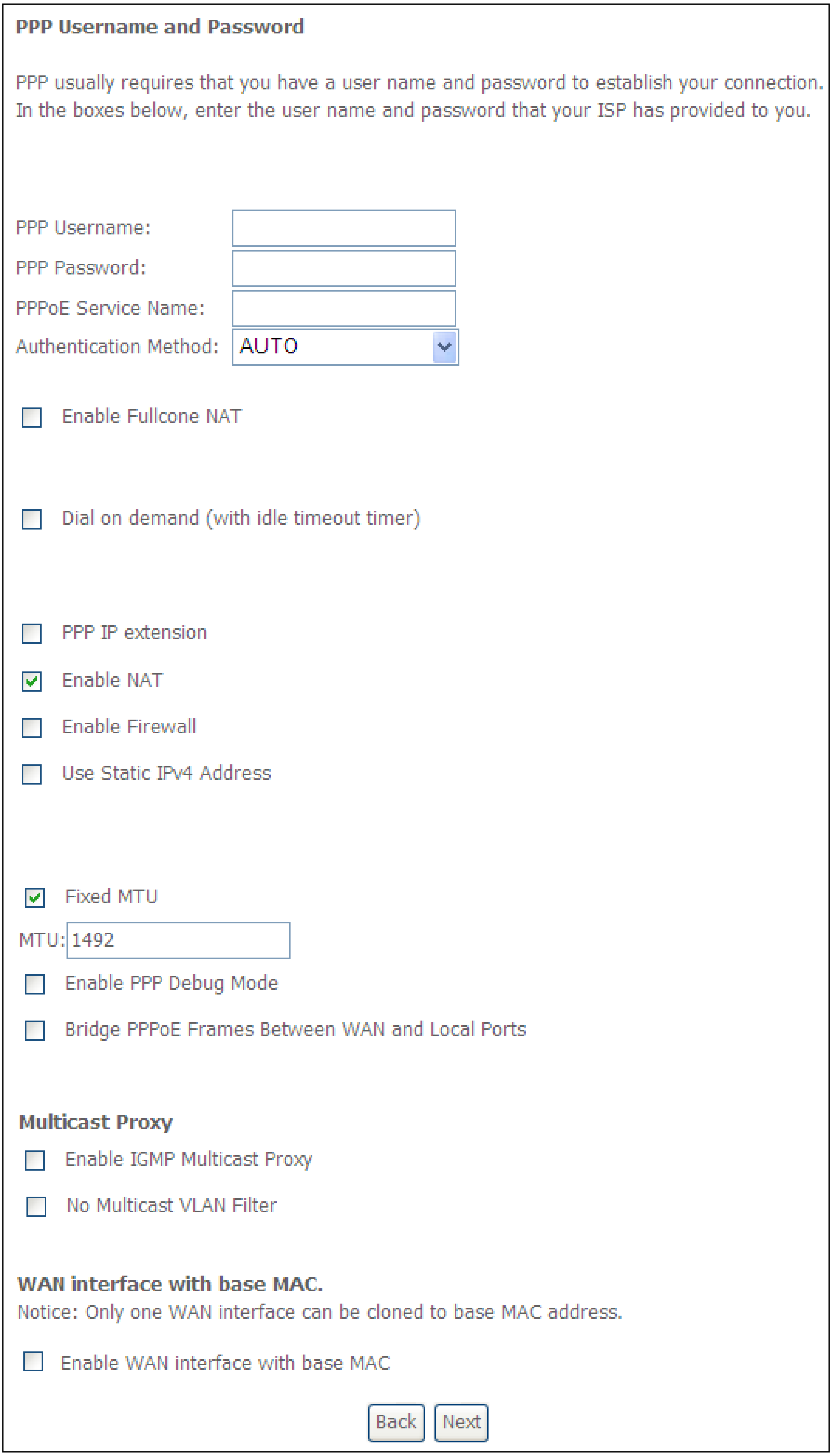
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

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

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

Network Protocol Selection: IPv4 Only

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

☑ Fixed MTU

MTU: 1492

□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

□ No Multicast VLAN Filter

WAN interface with base MAC.

Notice: Only one WAN interface can be cloned to base MAC address.

□ Enable WAN interface with base MAC

The settings shown above are described below.

PPP SETTINGS

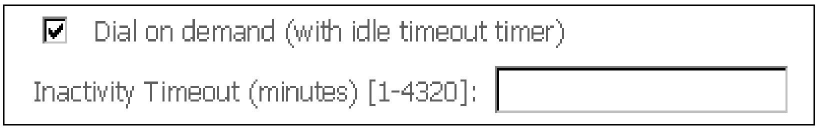
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

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 AR5381U 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

MTU
Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

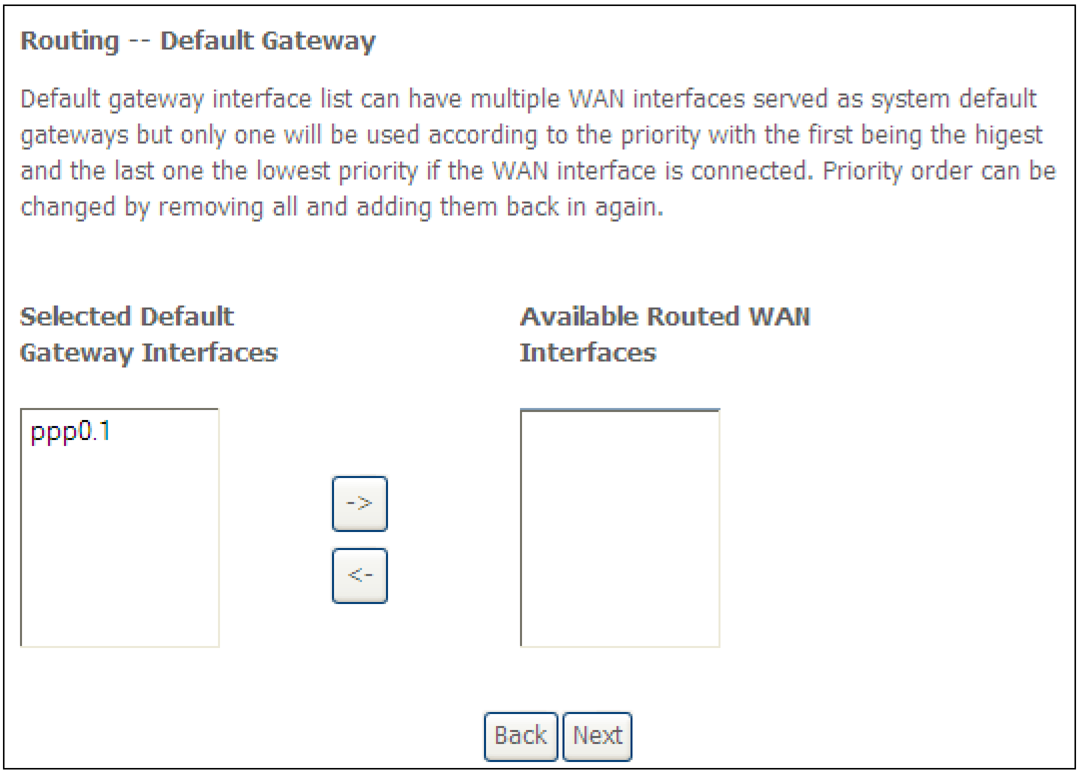
ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

ENABLE IGMP MULTICAST 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.

NO MULTICAST VLAN FILTER
Tick the checkbox ☑ to Enable/Disable multicast VLAN filter.

Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 3: Choose an interface to be the default gateway.



Routing -- Default Gateway

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

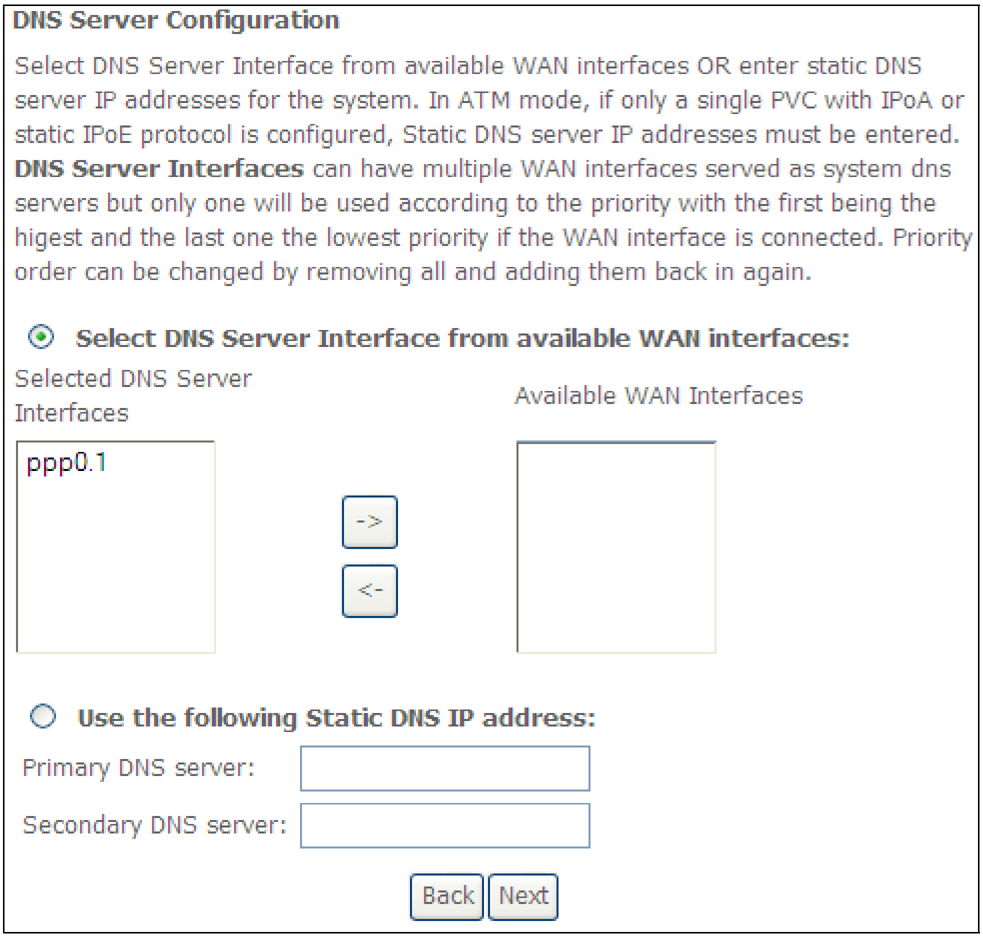
Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

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

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



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: ppp0.1

Available WAN Interfaces:

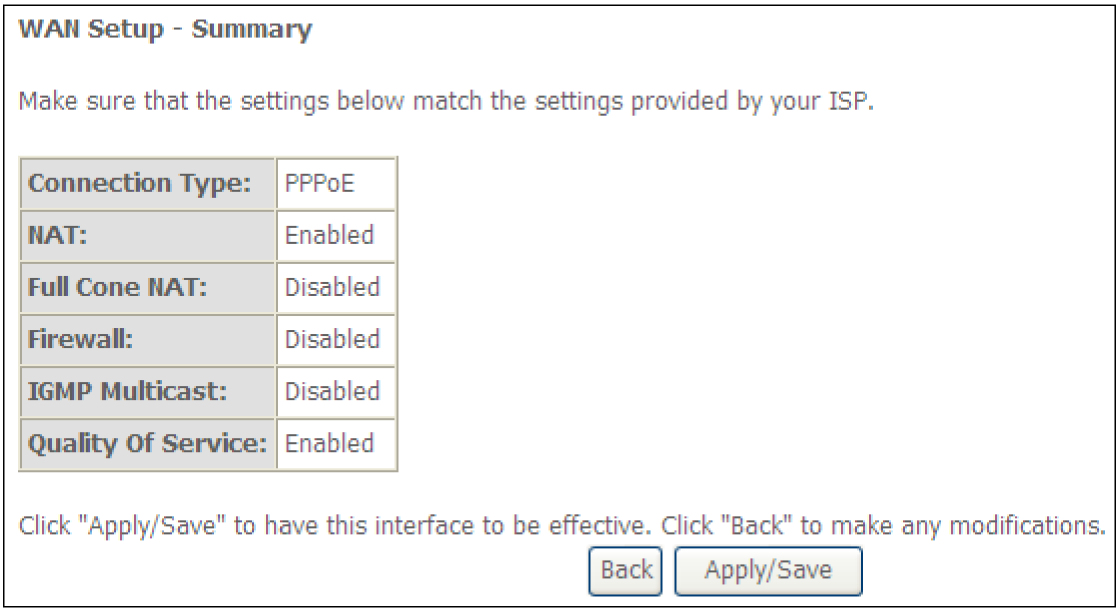
○ **Use the following Static DNS IP address:**

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.

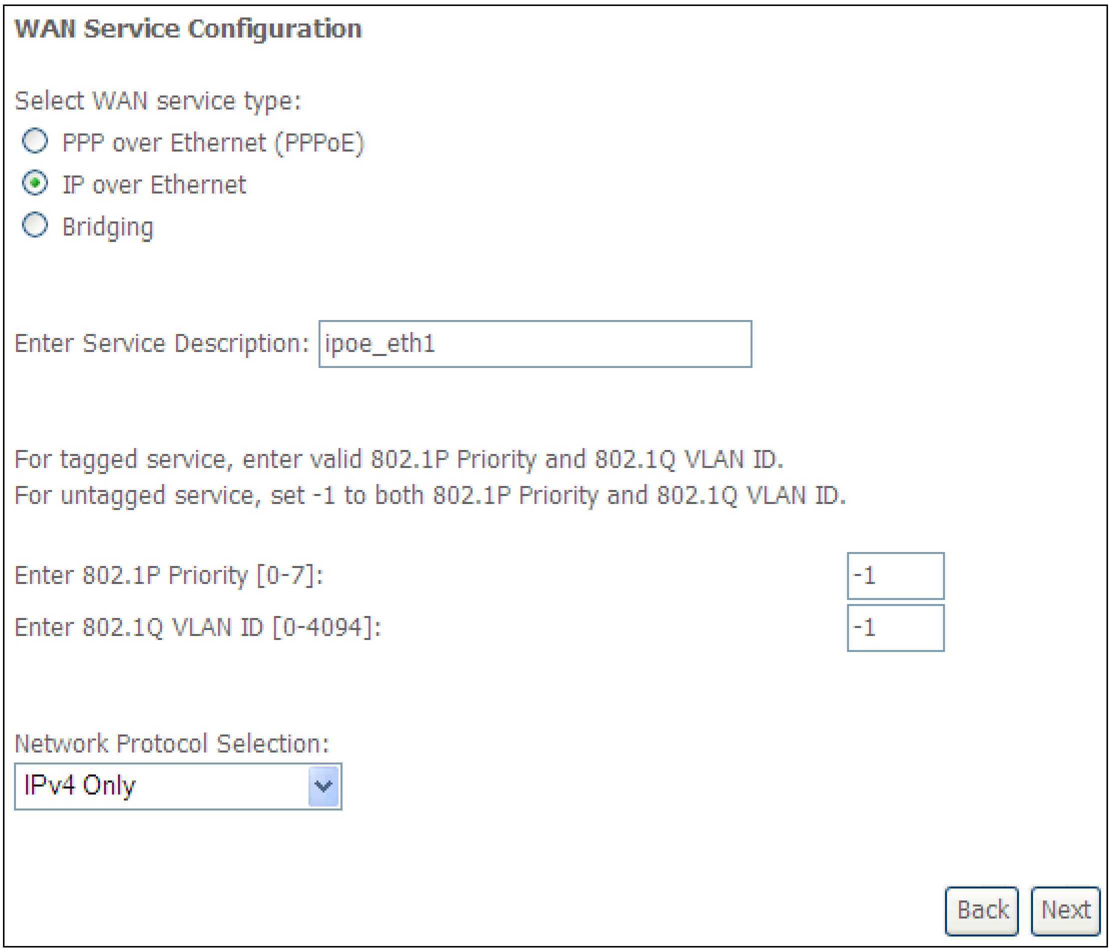
Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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.**



WAN Service Configuration

Select WAN service type:

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

Enter Service Description: ipoe_eth1

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

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

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

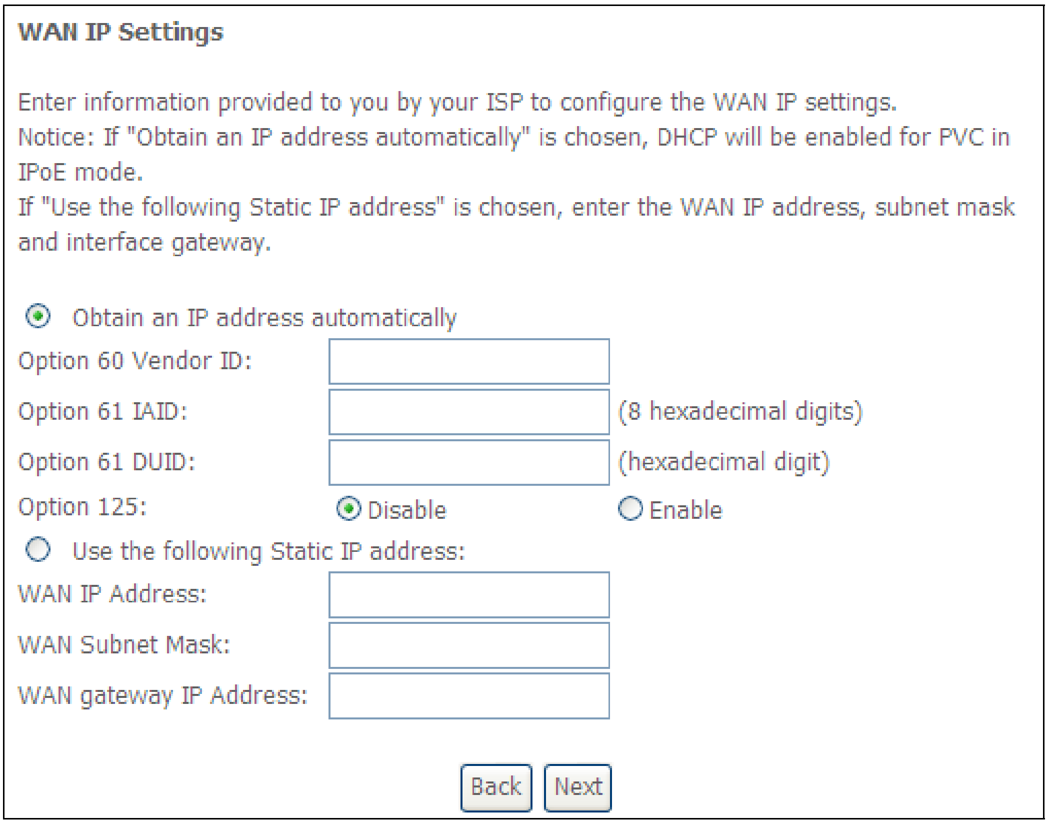
Network Protocol Selection: IPv4 Only

*

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

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

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

● Obtain an IP address automatically

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

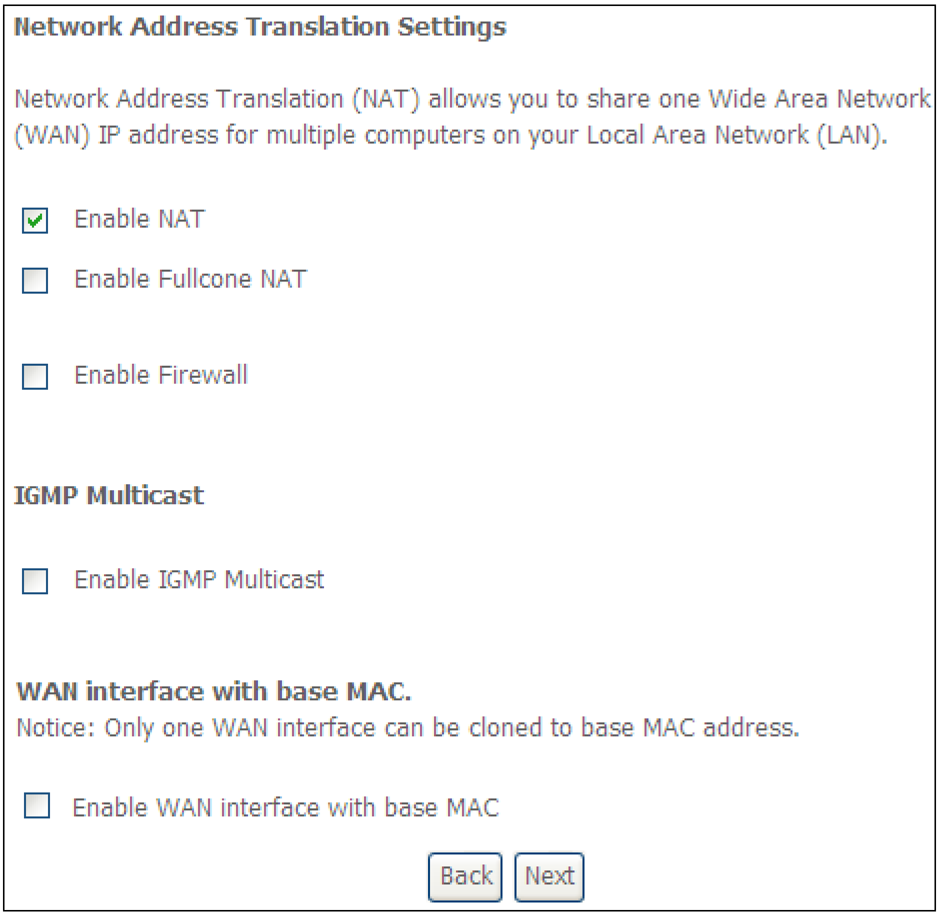
○ Use the following Static IP address:

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.

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 Fullcone NAT

□ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast

WAN interface with base MAC.

Notice: Only one WAN interface can be cloned to base MAC address.

□ Enable WAN interface with base MAC

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.

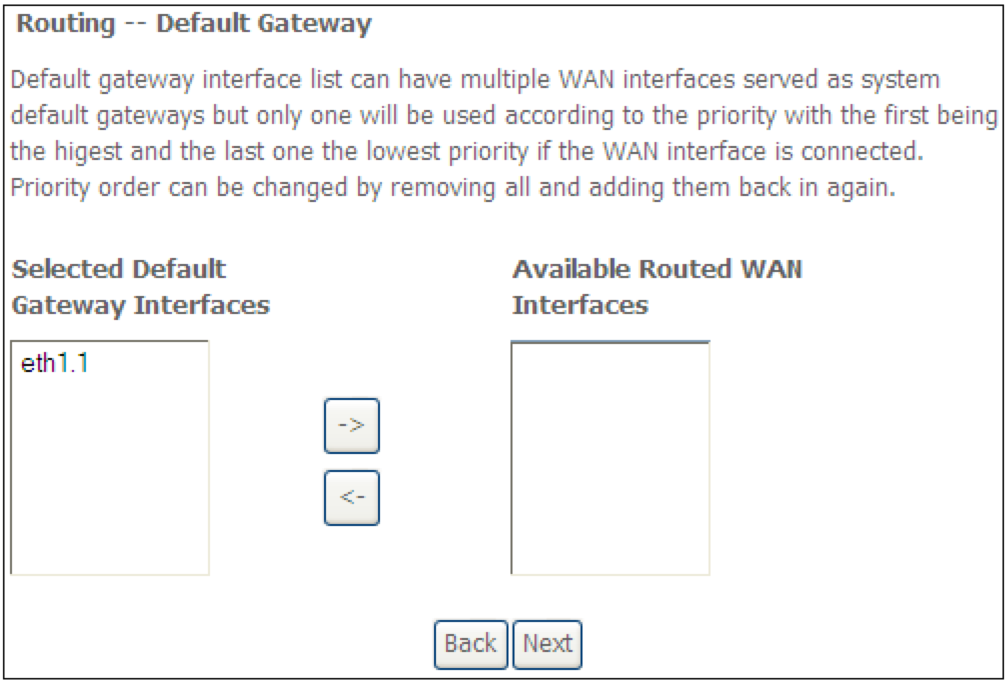
ENABLE IGMP MULTICAST

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 WAN interface with base MAC

Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 4: To choose an interface to be the default gateway.



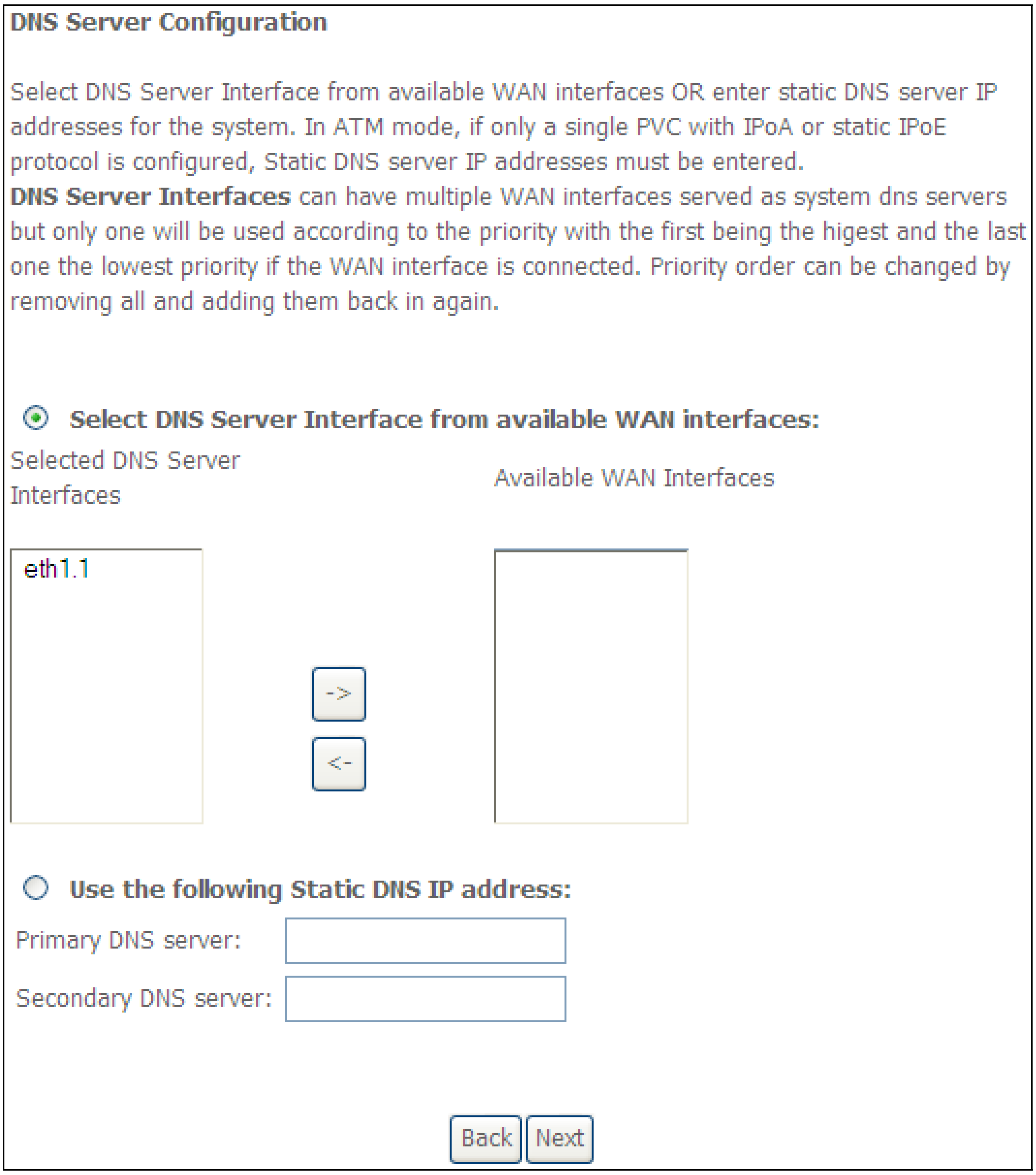
Routing -- Default Gateway

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

Selected Default Gateway Interfaces
eth1.1
->
<-
Available Routed WAN Interfaces
Back
Next

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

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

● **Select DNS Server Interface from available WAN interfaces:**

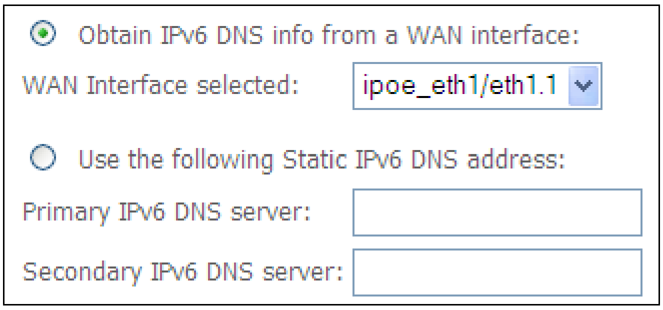
Selected DNS Server Interfaces	Available WAN Interfaces
eth1.1	

○ **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.



● Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: ipoe_eth1/eth1.1

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

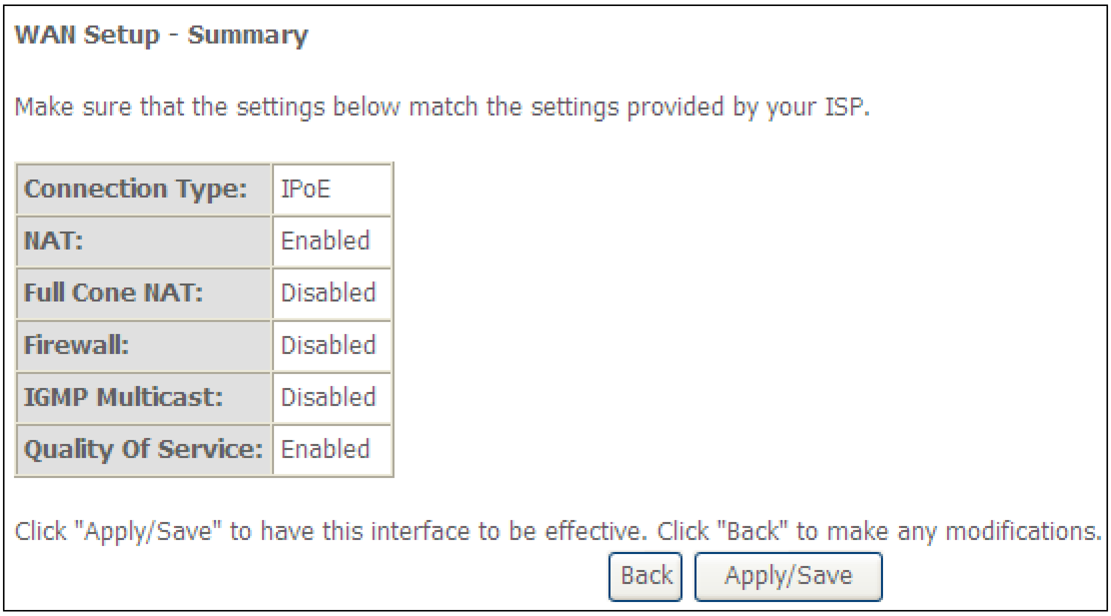
Secondary IPv6 DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

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.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

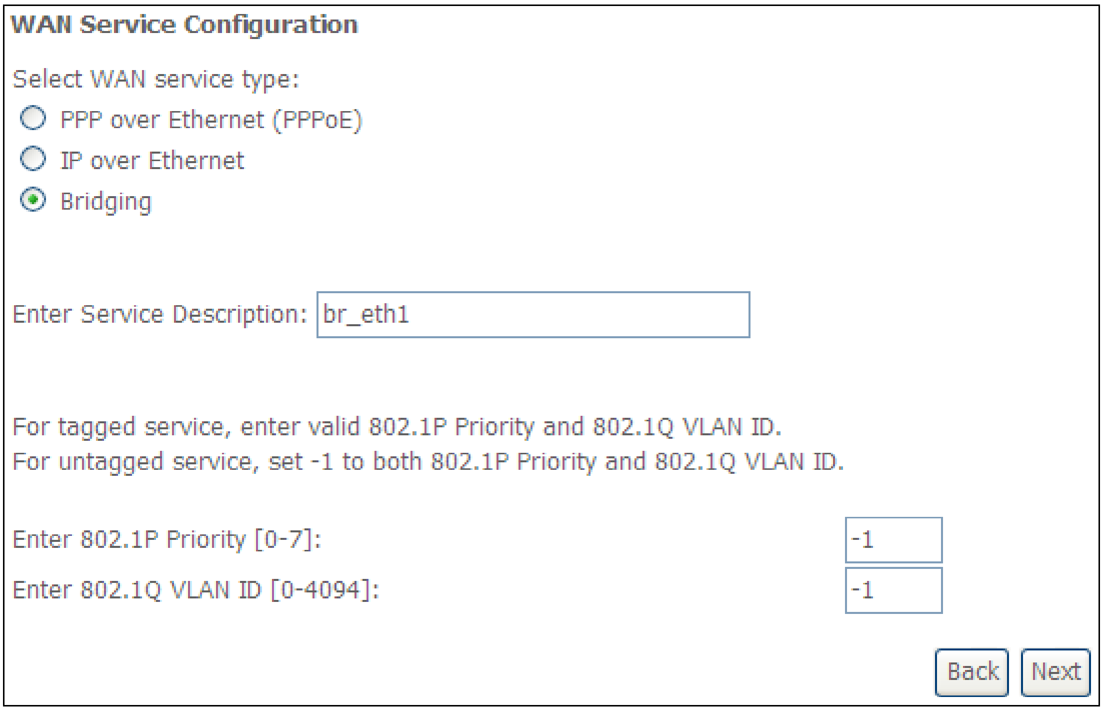
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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**.

E2.3 Bridging

NOTE:	This connection type is not available on the Ethernet WAN interface.

STEP 1: ***Select the Bridging radio button and click **Next**.



WAN Service Configuration

Select WAN service type:

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

Enter Service Description: br_eth1

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

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

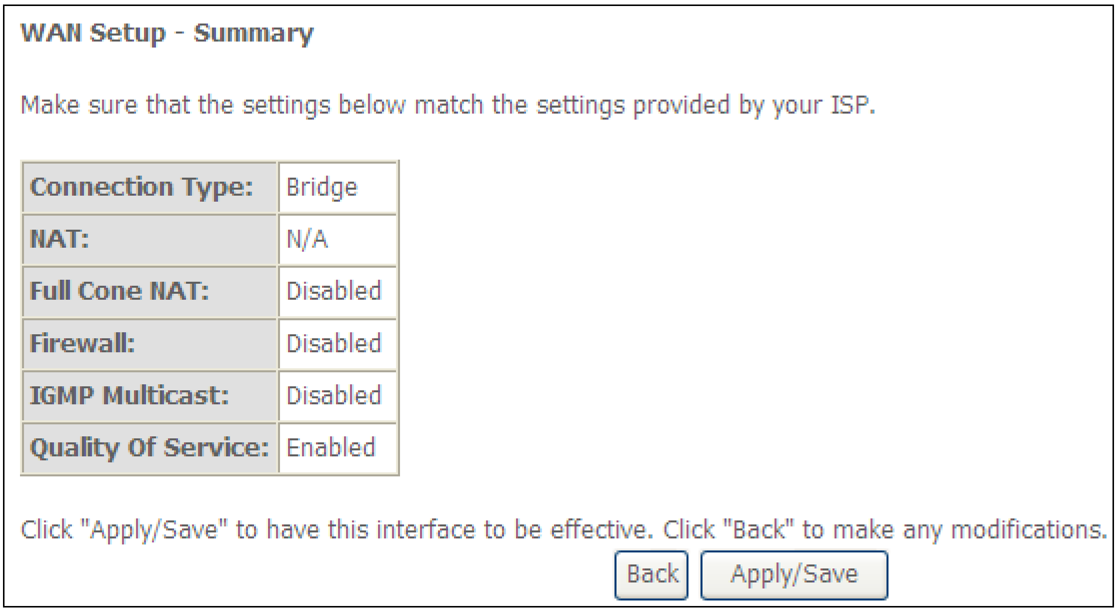
Enter 802.1Q VLAN ID [0-4094]: -1

*****

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

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

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.

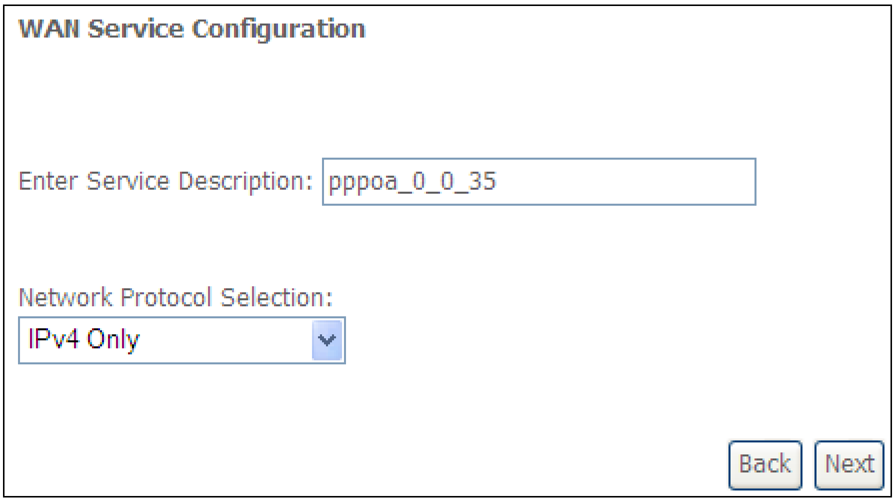
Connection Type:	Bridge
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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**.

NOTE: If this bridge connection is your only WAN service, the AR5381U will be inaccessible for remote management or technical support from the WAN.

E2.4 PPP over ATM (PPPoA)



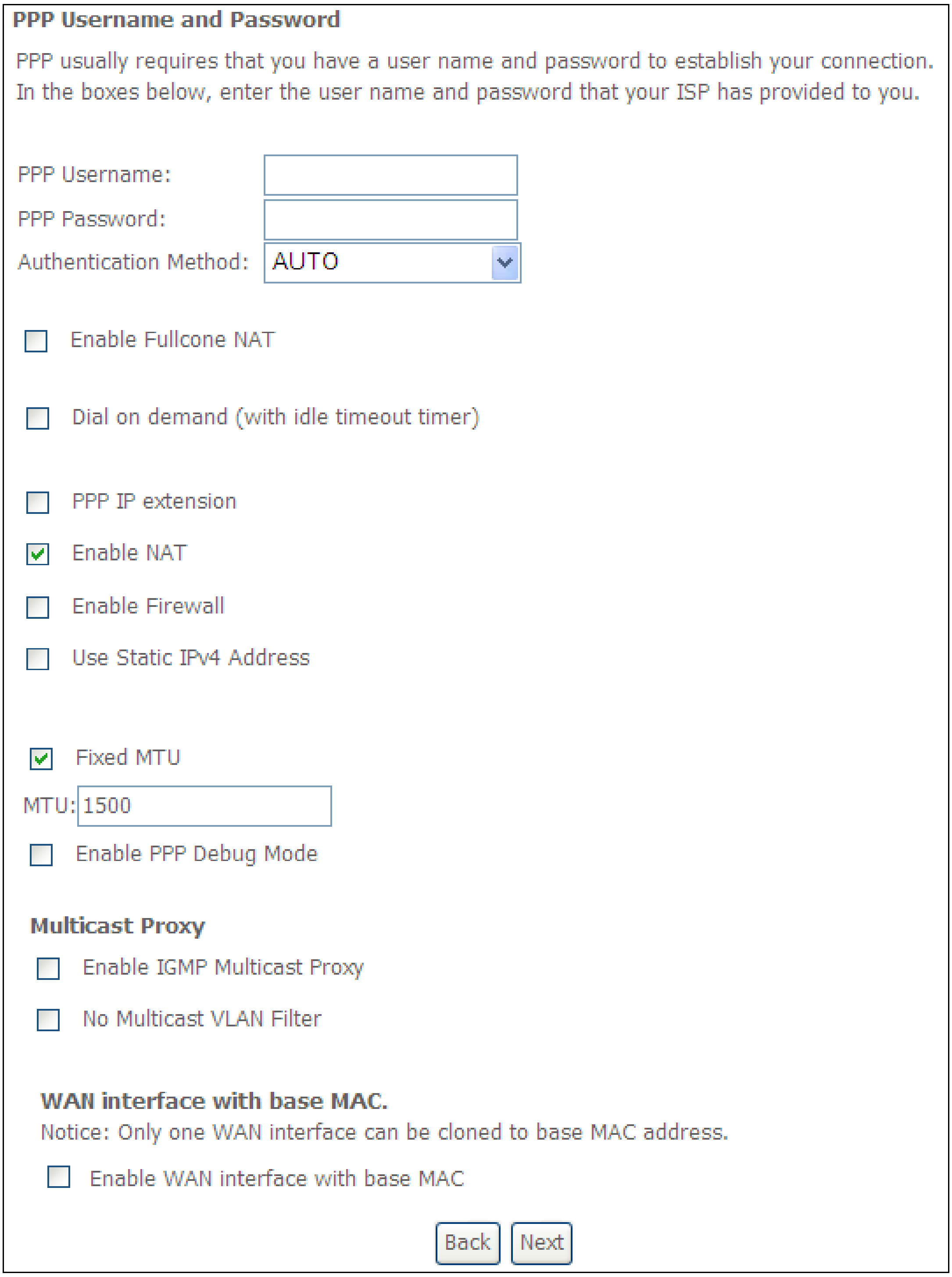
WAN Service Configuration

Enter Service Description: pppoa_0_0_35

Network Protocol Selection: IPv4 Only

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

☑ Fixed MTU

MTU: 1500

□ Enable PPP Debug Mode

Multicast Proxy

□ Enable IGMP Multicast Proxy

□ No Multicast VLAN Filter

WAN interface with base MAC.

Notice: Only one WAN interface can be cloned to base MAC address.

□ Enable WAN interface with base MAC

PPP SETTINGS

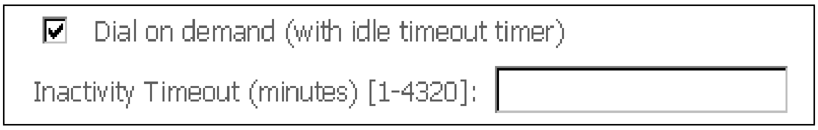
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

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 AR5381U 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.

Fixed MTU

Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

ENABLE PPP DEBUG MODE

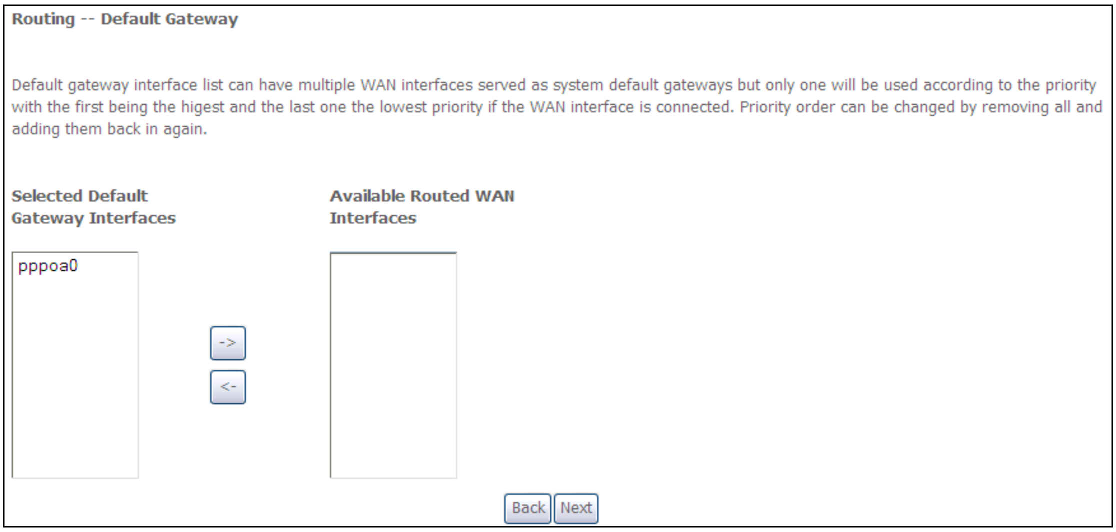
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

ENABLE IGMP MULTICAST Proxy
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.

NO MULTICAST VLAN FILTER
Tick the checkbox ☑ to have the multicast packets bypass the VLAN filter.

Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 3: Choose an interface to be the default gateway.



Routing -- Default Gateway

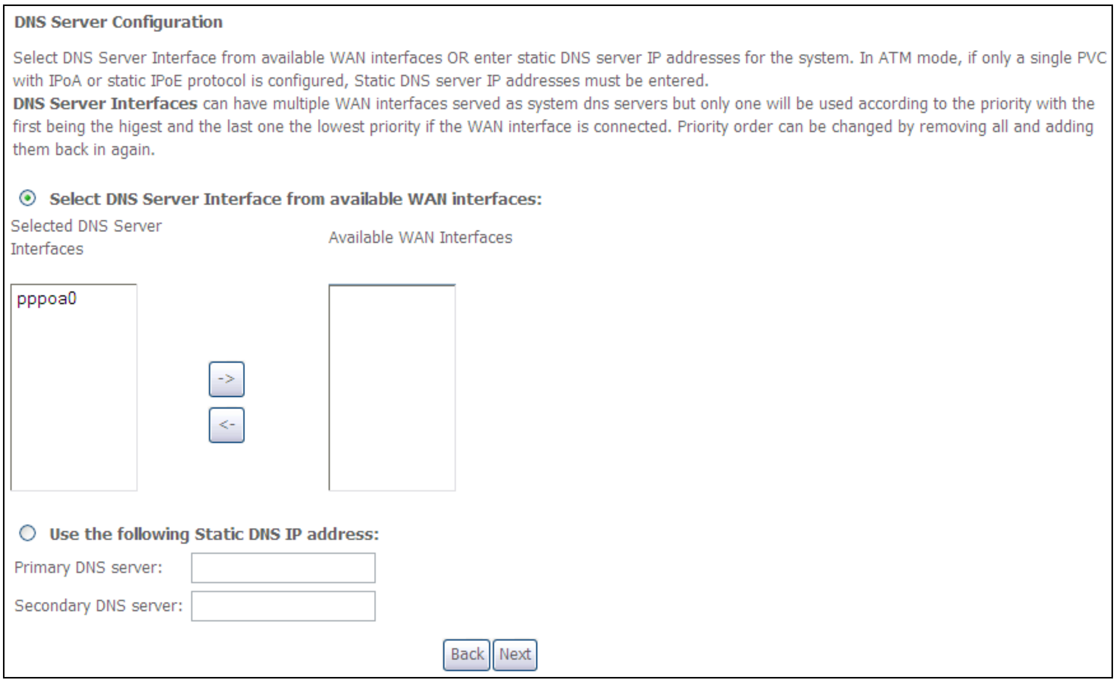
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and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

Selected Default Gateway Interfaces: pppoa0

Available Routed WAN Interfaces

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

STEP 4: Choose an interface to be the default gateway.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: pppoa0

Available WAN Interfaces

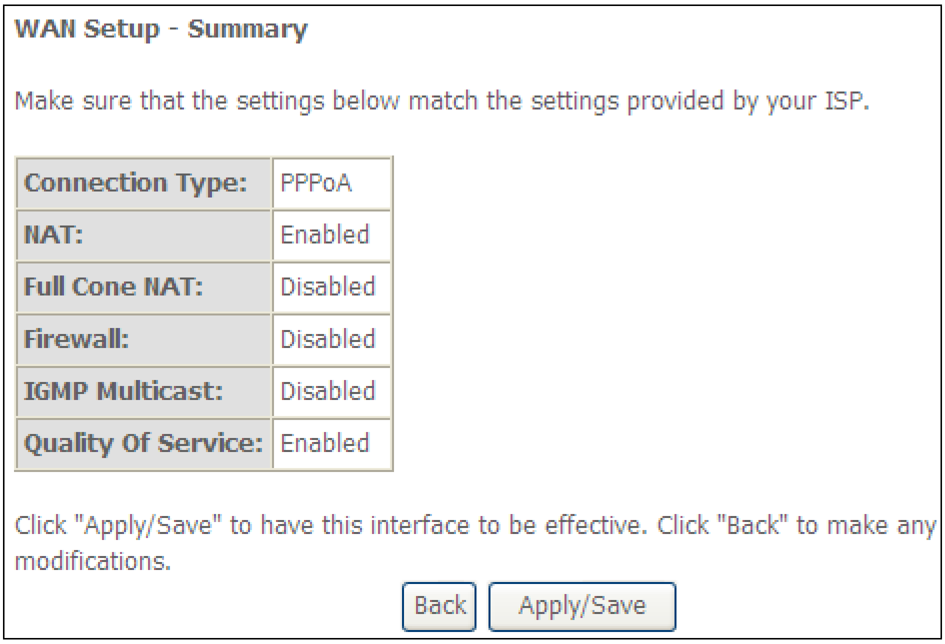
○ **Use the following Static DNS IP address:**

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

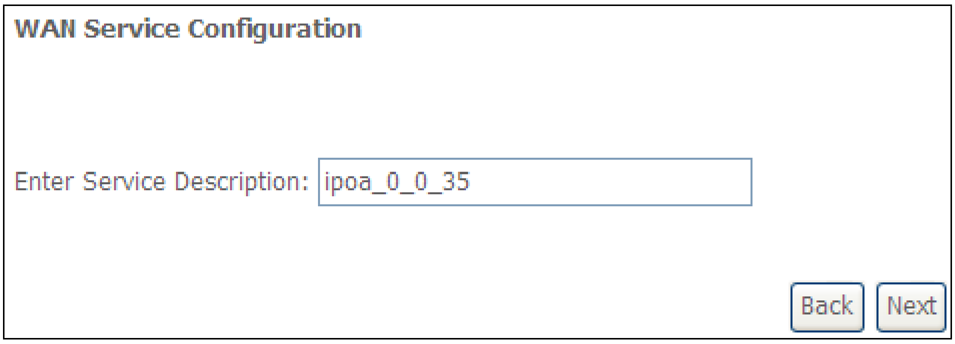
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
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**.

E2.5 IP over ATM (IPoA)

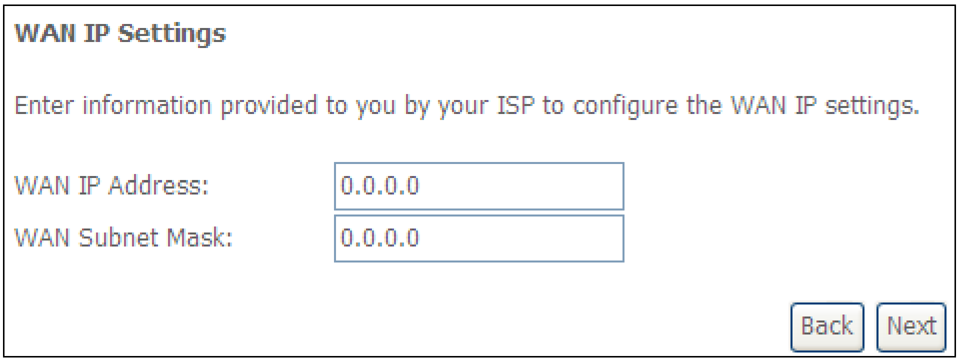


WAN Service Configuration

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.



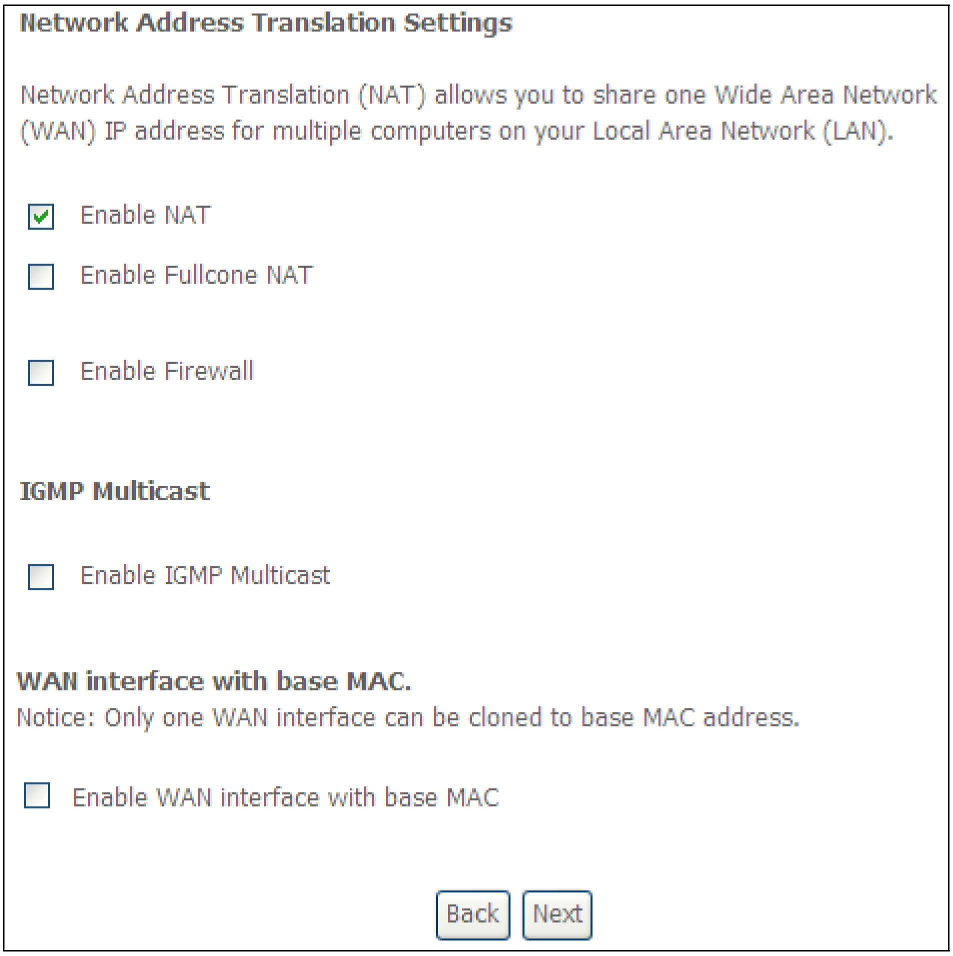
WAN IP Settings

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 Fullcone NAT

□ Enable Firewall

IGMP Multicast

□ Enable IGMP Multicast

WAN interface with base MAC.

Notice: Only one WAN interface can be cloned to base MAC address.

□ Enable WAN interface with base MAC

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.

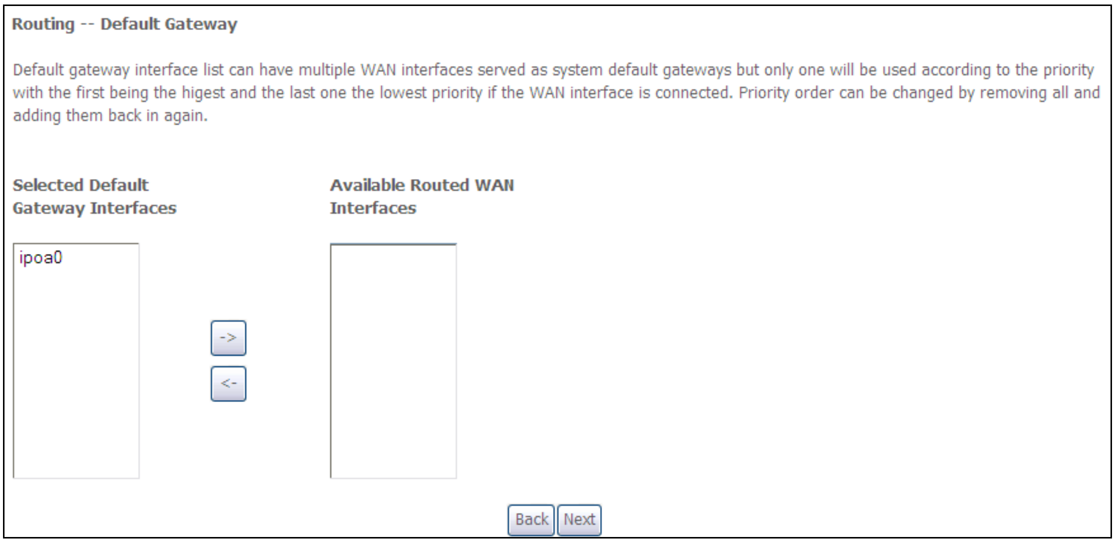
ENABLE IGMP MULTICAST

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 WAN interface with base MAC

Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 4: Choose an interface to be the default gateway.



Routing -- Default Gateway

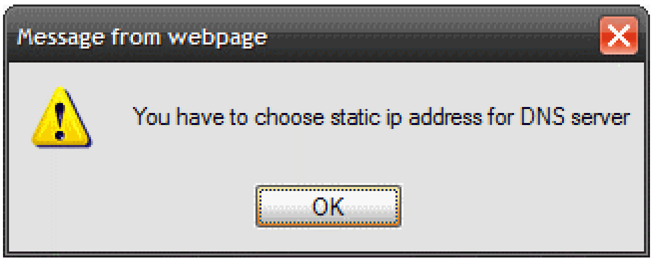
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and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

Selected Default Gateway Interfaces: ipoa0

Available Routed WAN Interfaces:

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

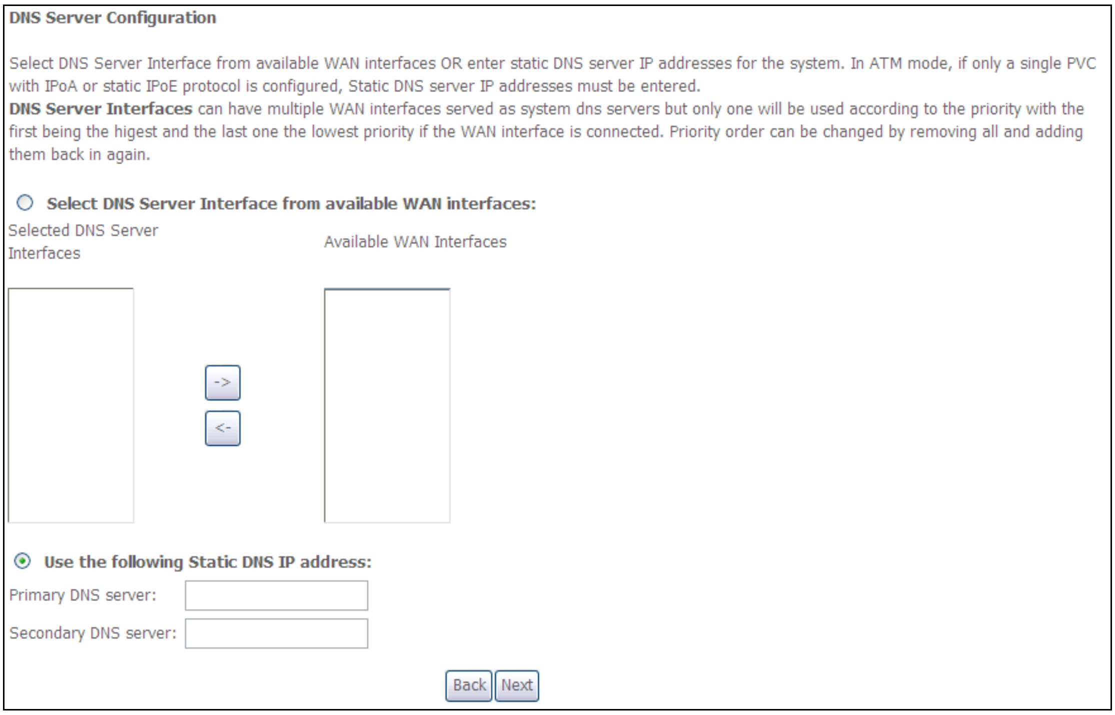
NOTE: If the DHCP server is not enabled on another WAN interface then the following notification will be shown before the next screen.



Message from webpage

You have to choose static ip address for DNS server

STEP 5: Choose an interface to be the default gateway.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

○ **Select DNS Server Interface from available WAN interfaces:**

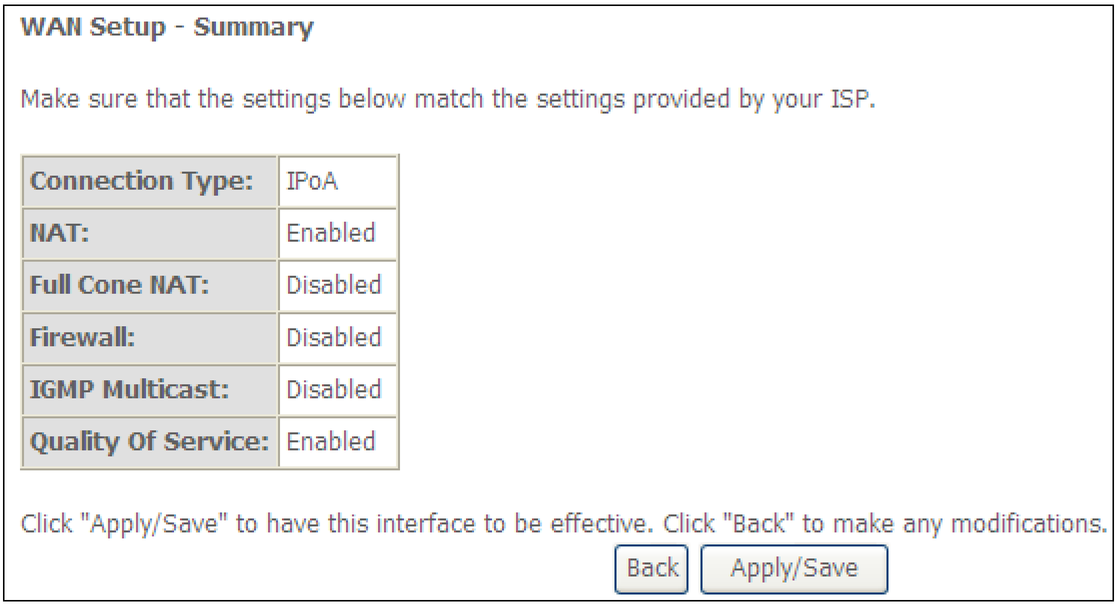
● **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

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

STEP 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.

Connection Type:	IPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
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**.

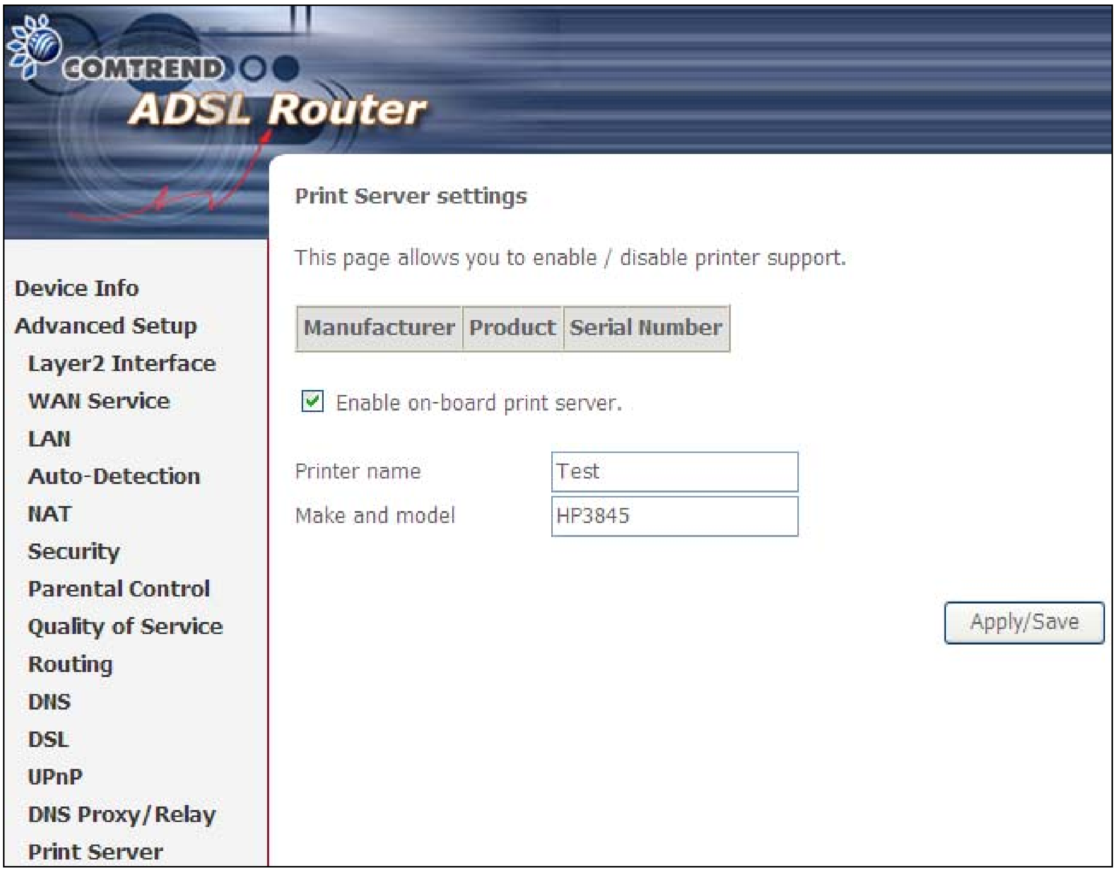
Appendix F - Printer Server

These steps explain the procedure for enabling the Printer Server.

NOTE:	This function only applies to models with an USB host port.

STEP 1: Enable Print Server from Web User Interface. Select Enable on-board print server checkbox ☑ and enter Printer name and Make and model

NOTE:	The **Printer name** can be any text string up to 40 characters. The **Make and model** can be any text string up to 128 characters.



Print Server settings

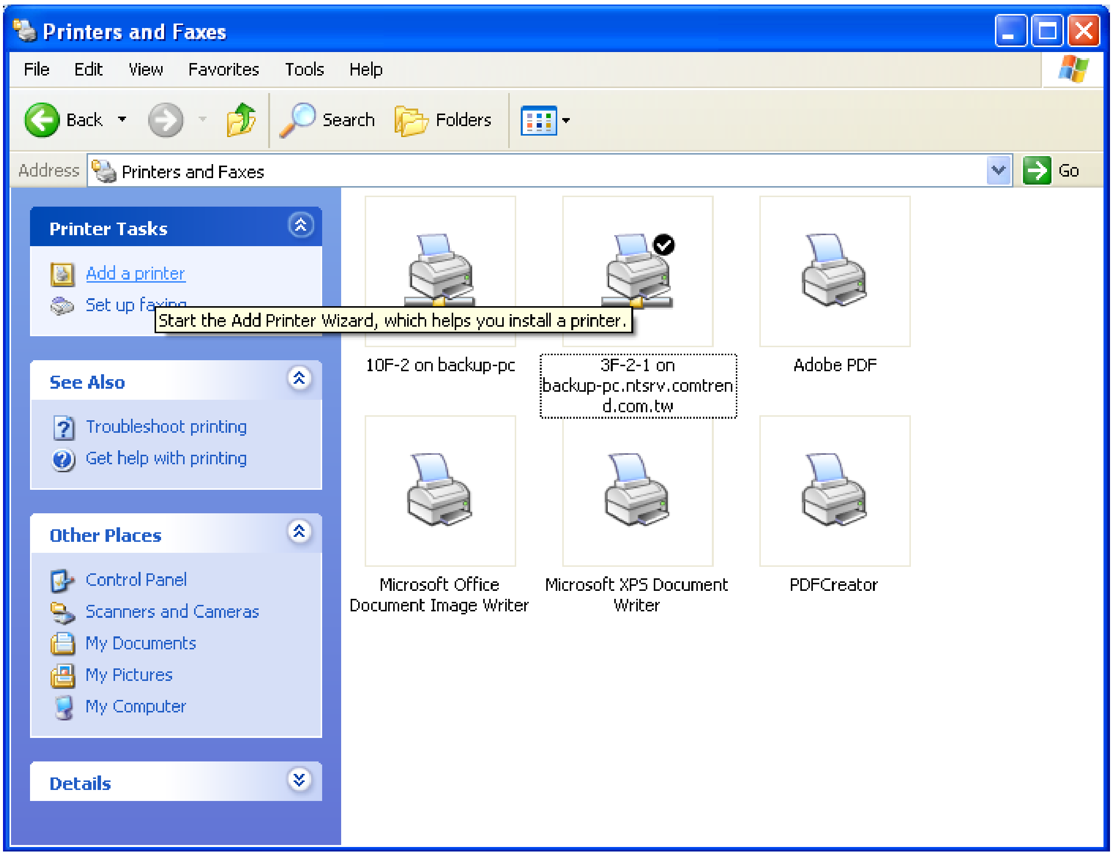
This page allows you to enable / disable printer support.

Manufacturer	Product	Serial Number

☑ Enable on-board print server.

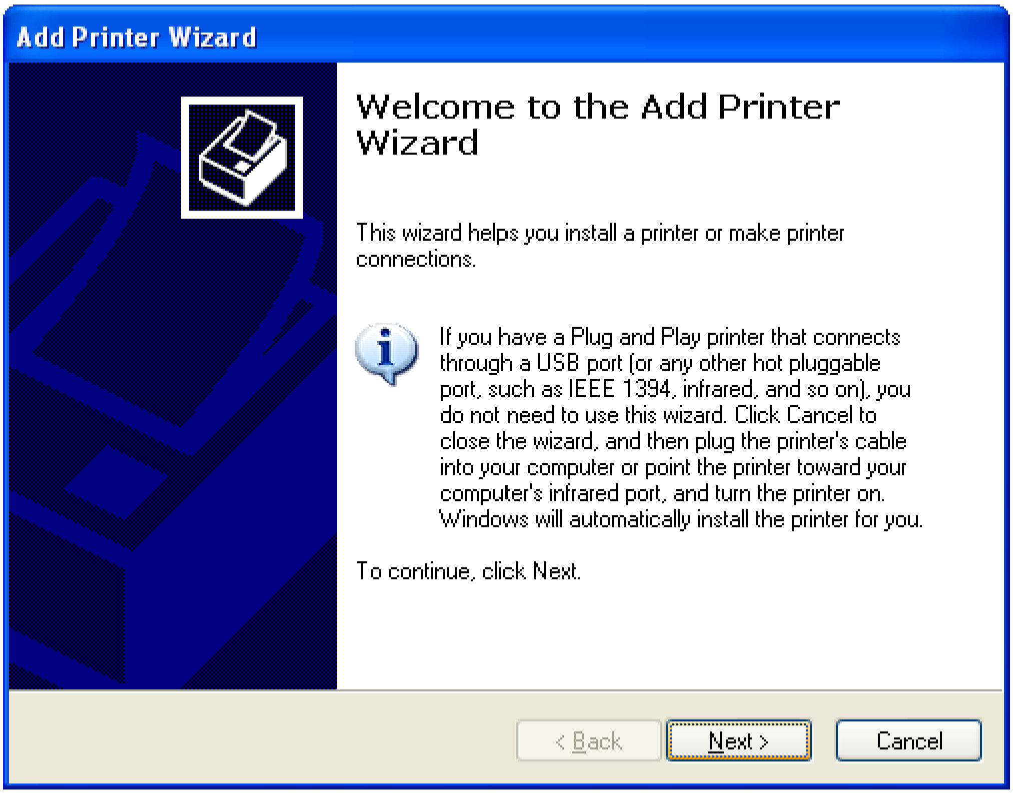
Printer name	Test
Make and model	HP3845

STEP 2: Go to the **Printers and Faxes** application in the **Control Panel** and select the **Add a printer** function (as located on the side menu below).



Start the Add Printer Wizard, which helps you install a printer.

STEP 3: Click **Next** to continue when you see the dialog box below.



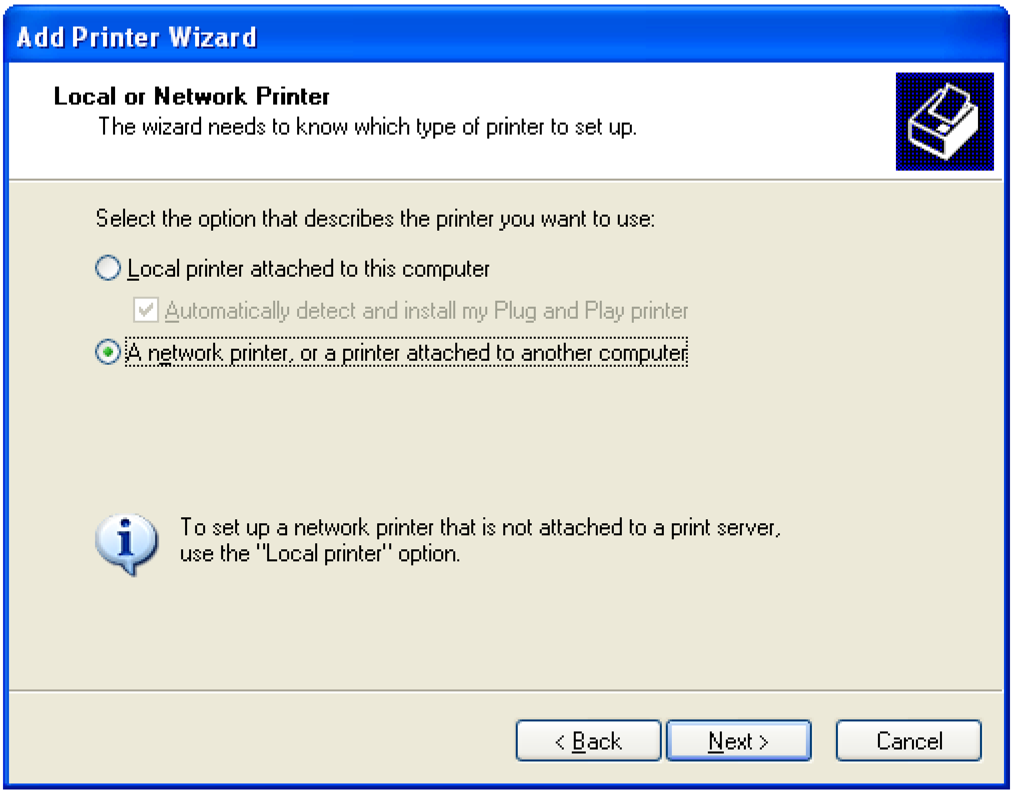
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

STEP 4: Select **Network Printer** and click **Next**.



Local or Network Printer
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

○ Local printer attached to this computer

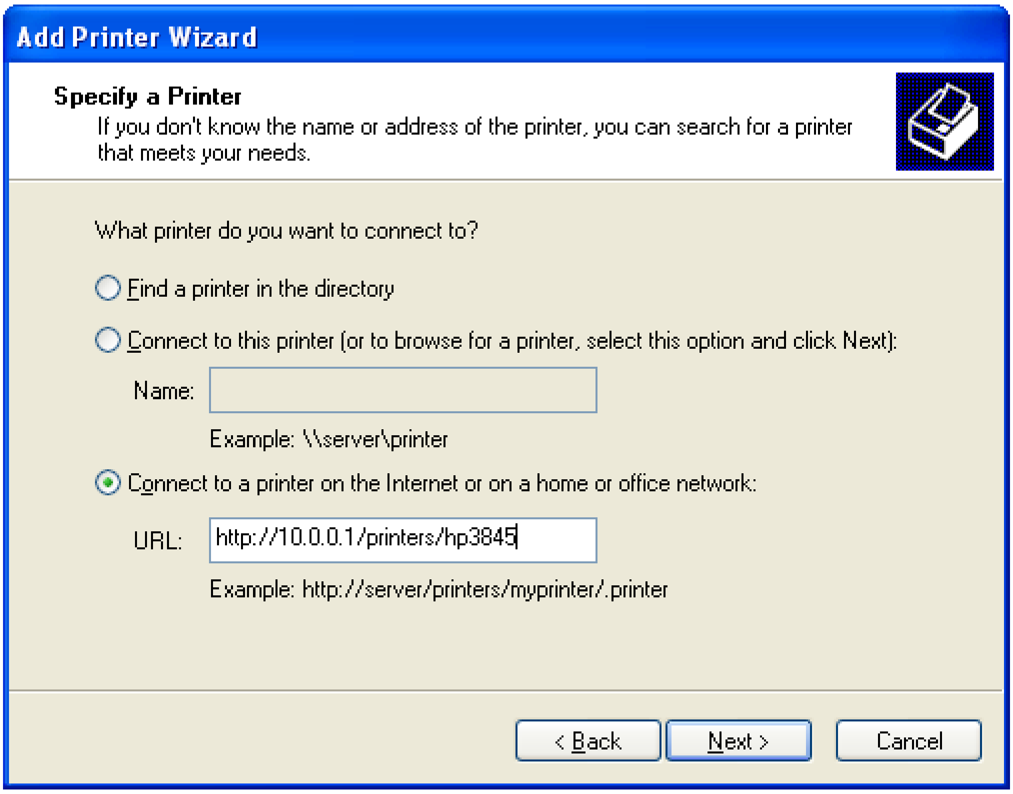
☑ Automatically detect and install my Plug and Play printer

● A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

STEP 5: Select Connect to a printer on the Internet and enter your printer link. (e.g. http://192.168.1.1:631/printers/hp3845) and click **Next**.

NOTE: The printer name must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.



Add Printer Wizard

Specify a Printer

If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

○ Find a printer in the directory

○ Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

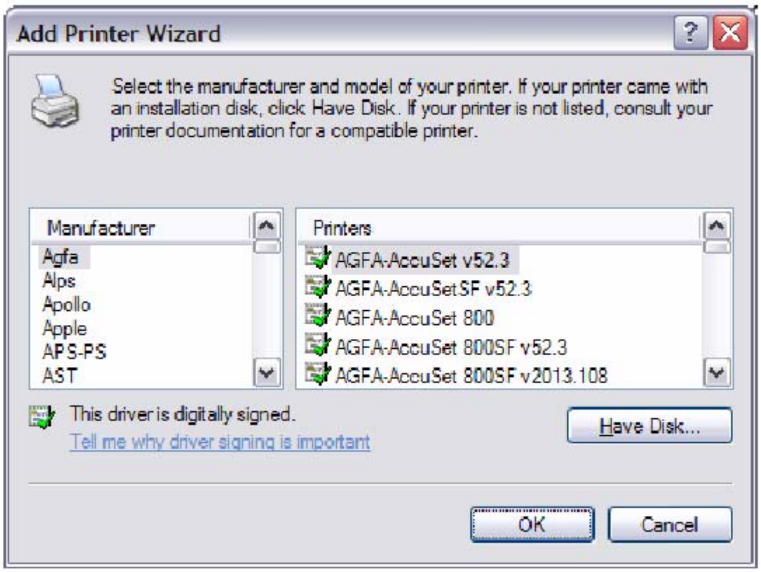
Example: \\server\printer

● Connect to a printer on the Internet or on a home or office network:

URL: http://10.0.0.1/printers/hp3845

Example: http://server/printers/myprinter/.printer

STEP 6: Click **Have Disk** and insert the printer driver CD.



Add Printer Wizard

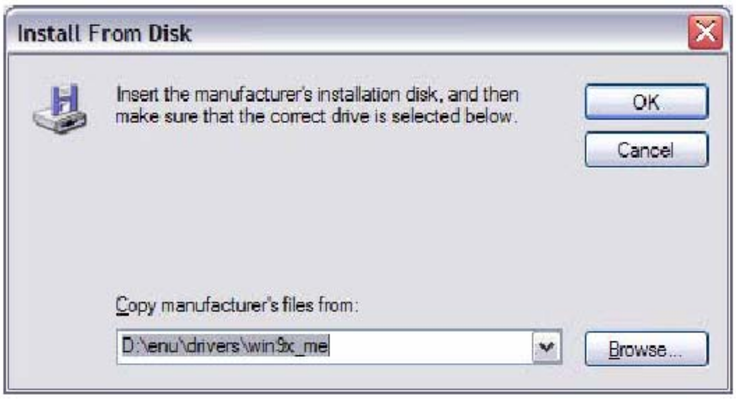
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer	Printers
Agfa	AGFA-AccuSet v52.3
Alps	AGFA-AccuSet SF v52.3
Apollo	AGFA-AccuSet 800
Apple	AGFA-AccuSet 800SF v52.3
APS-PS	AGFA-AccuSet 800SF v2013.108
AST	

This driver is digitally signed.

Tell me why driver signing is important

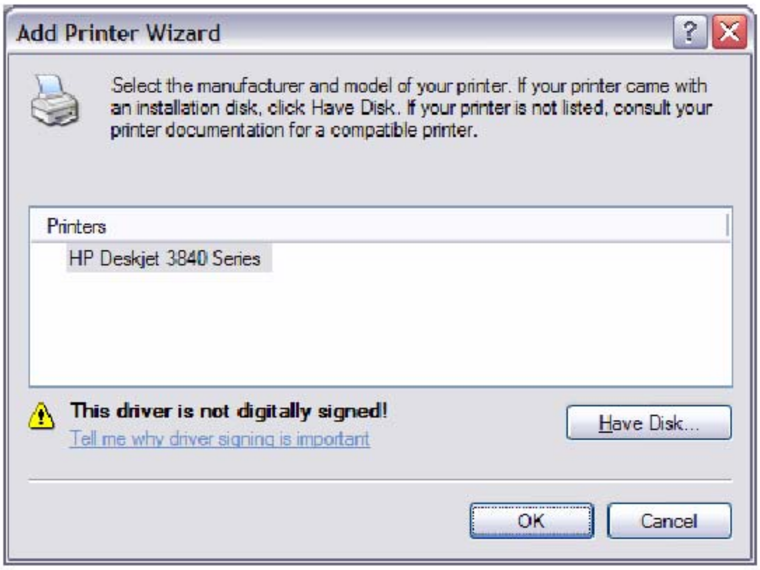
STEP 7: Select driver file directory on CD-ROM and click **OK**.



Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:
D:\enu\drivers\win9x_me

STEP 8: Once the printer name appears, click **OK**.

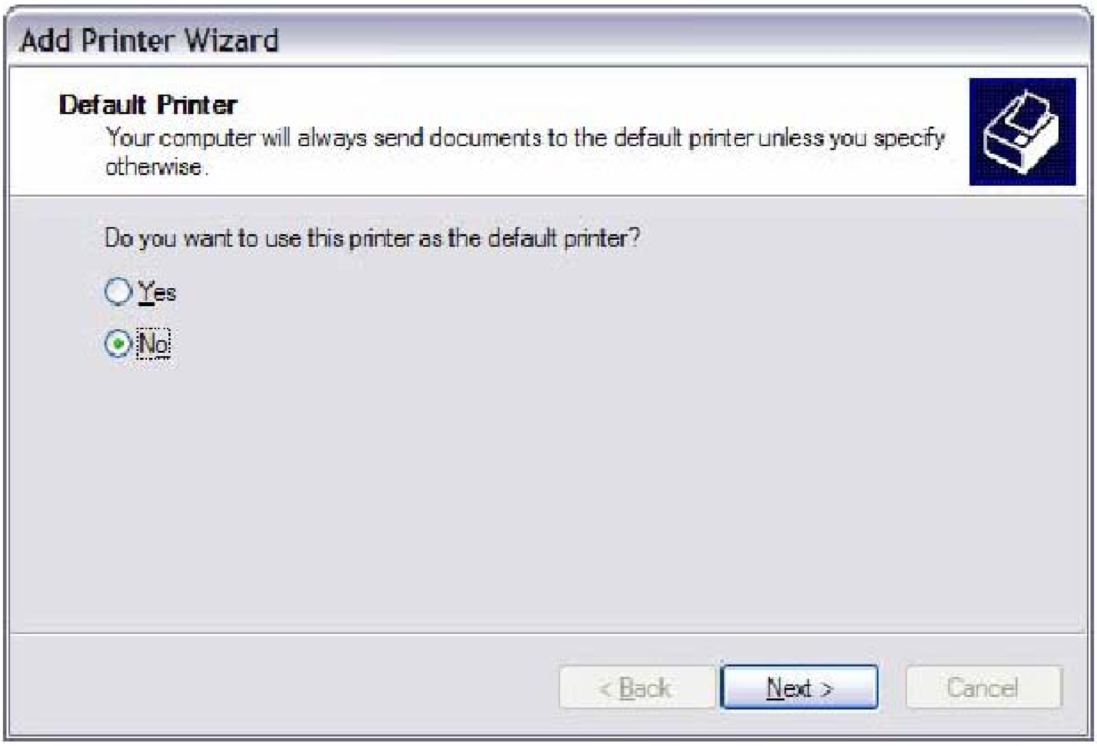


Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Printers
HP Deskjet 3840 Series

This driver is not digitally signed!
Tell me why driver signing is important

STEP 9: Choose **Yes** or **No** for default printer setting and click **Next.**



Add Printer Wizard

Default Printer

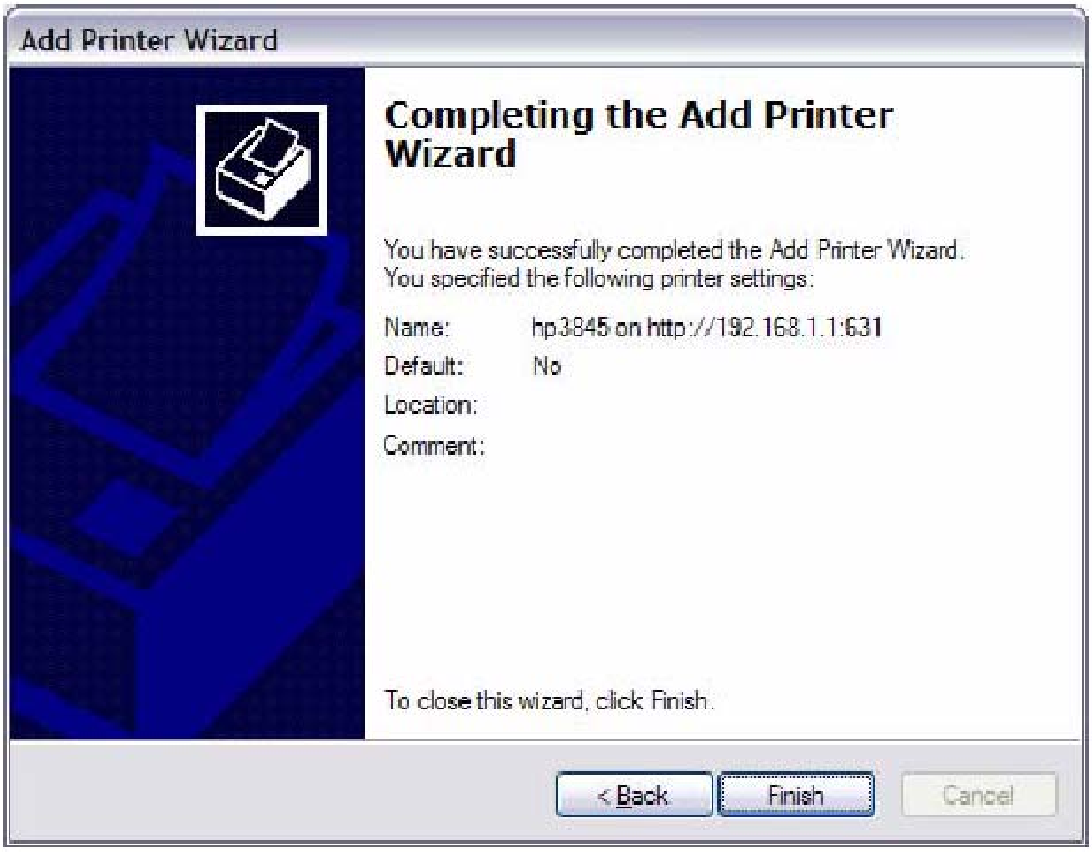
Your computer will always send documents to the default printer unless you specify otherwise.

Do you want to use this printer as the default printer?

○ Yes

● No

STEP 10: Click Finish.



Add Printer Wizard

Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard. You specified the following printer settings:

Name: hp3845 on http://192.168.1.1:631

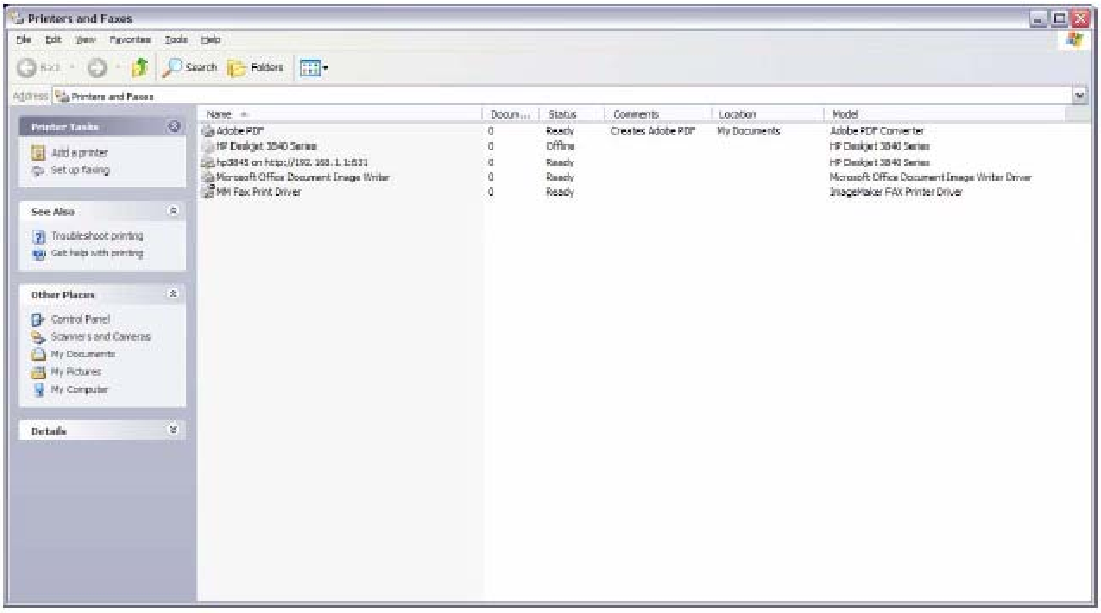
Default: No

Location:

Comment:

To close this wizard, click Finish.

STEP 11: Check the status of printer from Windows Control Panel, printer window. Status should show as **Ready**.



Name	Docum...	Status	Comments	Location	Model
Adobe PDF	0	Ready	Creates Adobe PDF	My Documents	Adobe PDF Converter
HP Deskjet 3840 Series	0	Offline			HP Deskjet 3840 Series
hp3845 on http://192.168.1.1:631	0	Ready			HP Deskjet 3840 Series
Microsoft Office Document Image Writer	0	Ready			Microsoft Office Document Image Writer Driver
MM Fax Print Driver	0	Ready			ImageMaker FAX Printer Driver