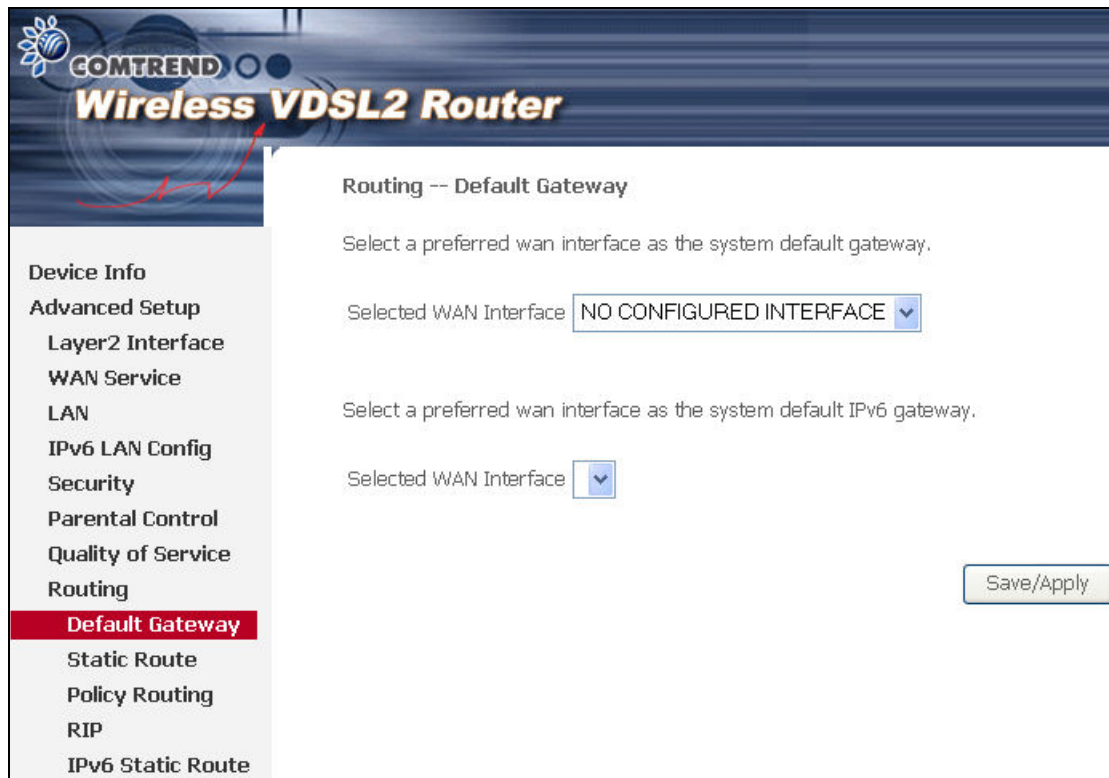


5.9.1 Default Gateway

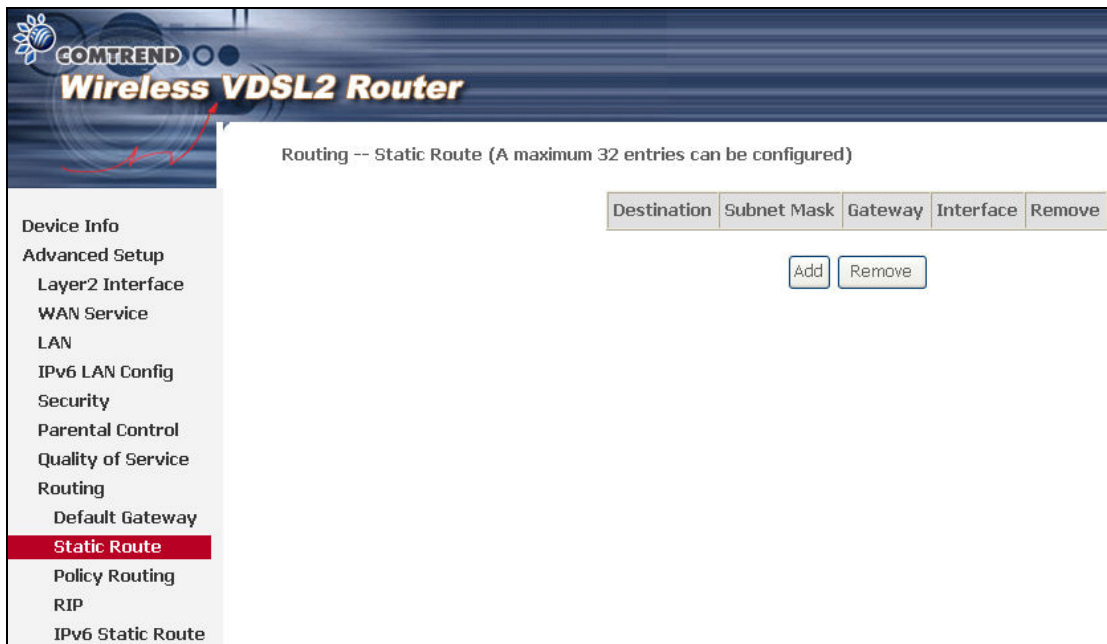
Select WAN Interfaces as default gateways and then click **Save/Apply**.



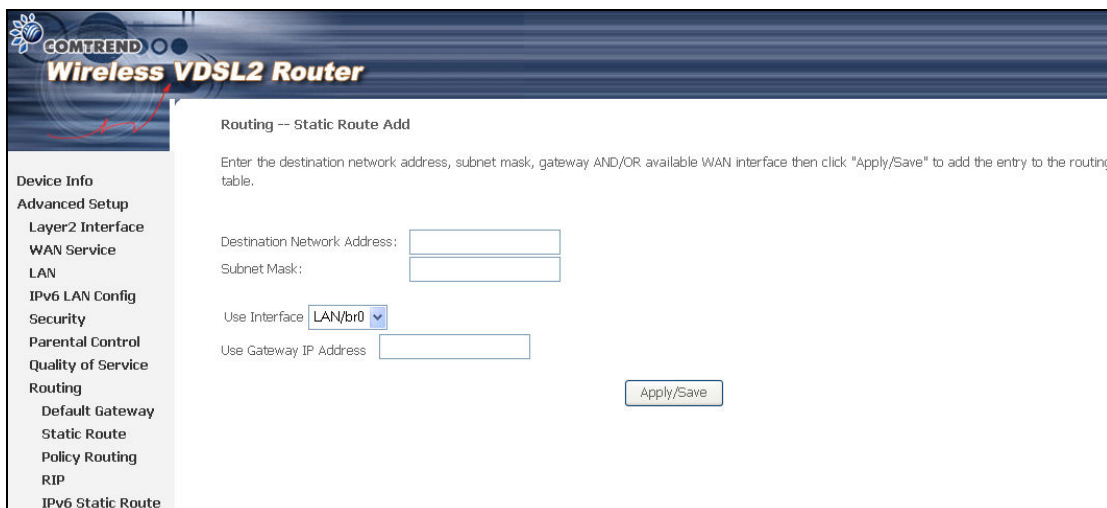
NOTE: After enabling the Automatic Assigned Default Gateway, the device must be rebooted to activate the assigned default gateway.

5.9.2 Static Route

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



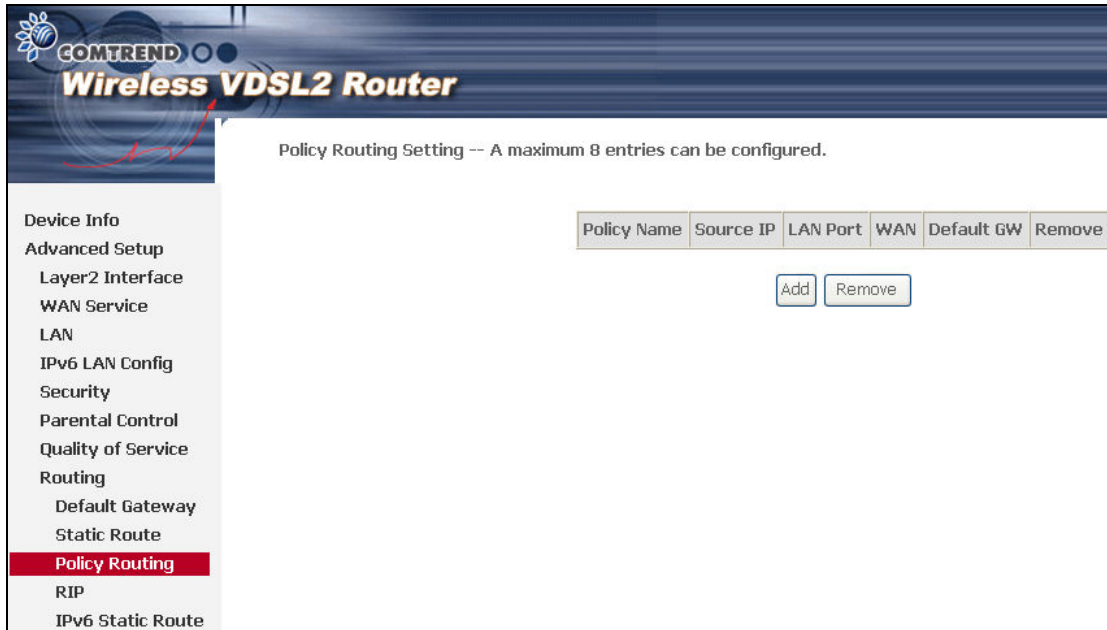
After clicking **Add** the following screen will display.



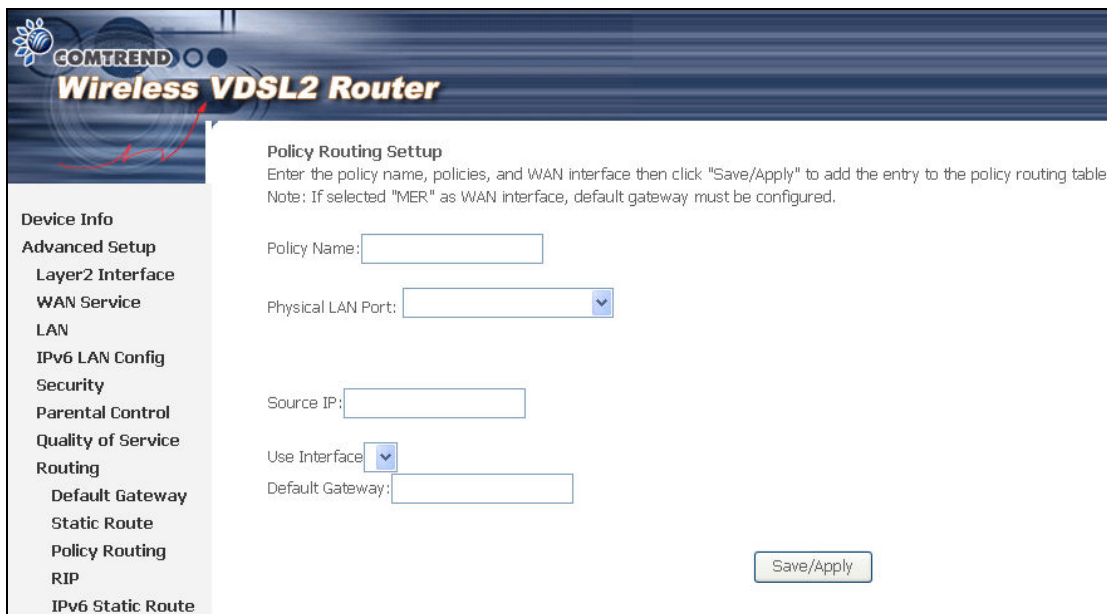
Enter Destination Network Address, Subnet Mask, Gateway IP Address, and/or WAN Interface before clicking **Apply/Save** to add an entry to the routing table.

5.9.3 Policy Routing

This option allows for the configuration of static routes by policy. Click **Add** to create a routing policy or **Remove** to delete one.

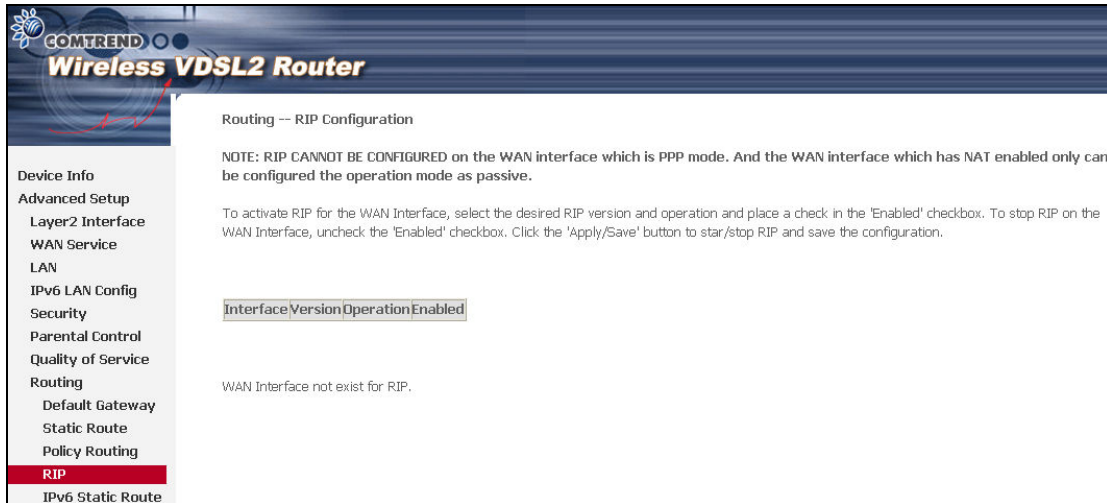


On the following screen, complete the form and click **Save/Apply** to create a policy.



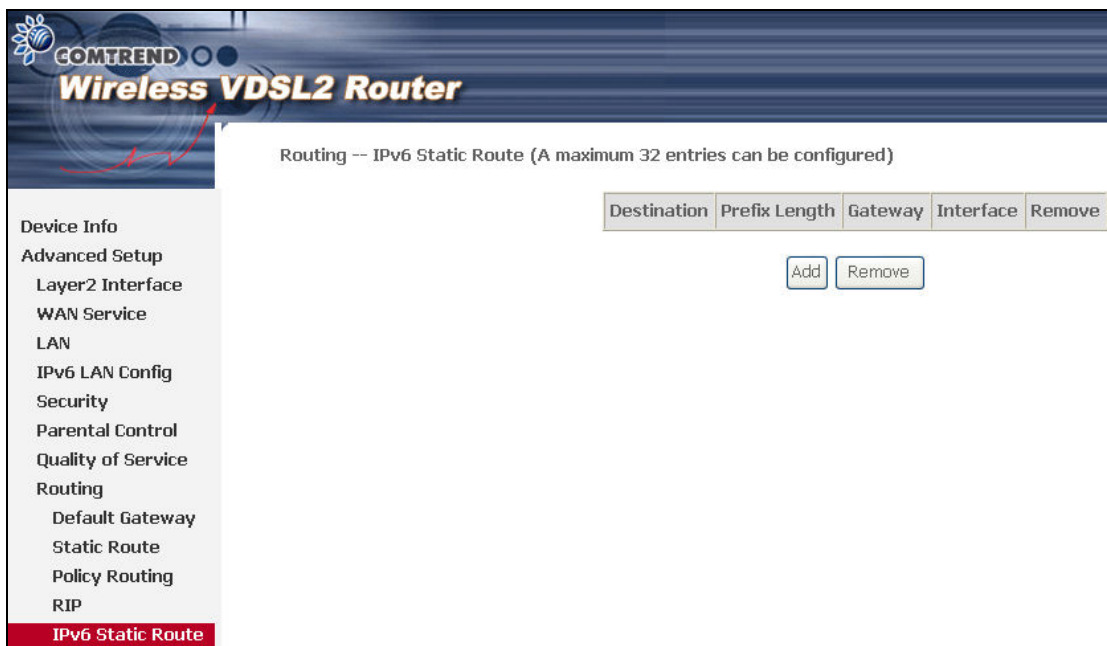
5.9.4 RIP

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



5.9.5 IPv6 Static Route

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



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

COMTREND Wireless VDSL2 Router

Routing -- IPv6 Static Route Add

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

Destination IPv6 Address:

Subnet Prefix Length:

Gateway IPv6 Address:

Interface:

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
IPv6 LAN Config
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
IPv6 Static Route

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

5.10 DNS

5.10.1 DNS Server

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

COMTREND Wireless VDSL2 Router

DNS Server Configuration

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

Obtain DNS info from a WAN interface:
WAN Interface selected:

Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
IPv6 LAN Config
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DNS Entries
DSL

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

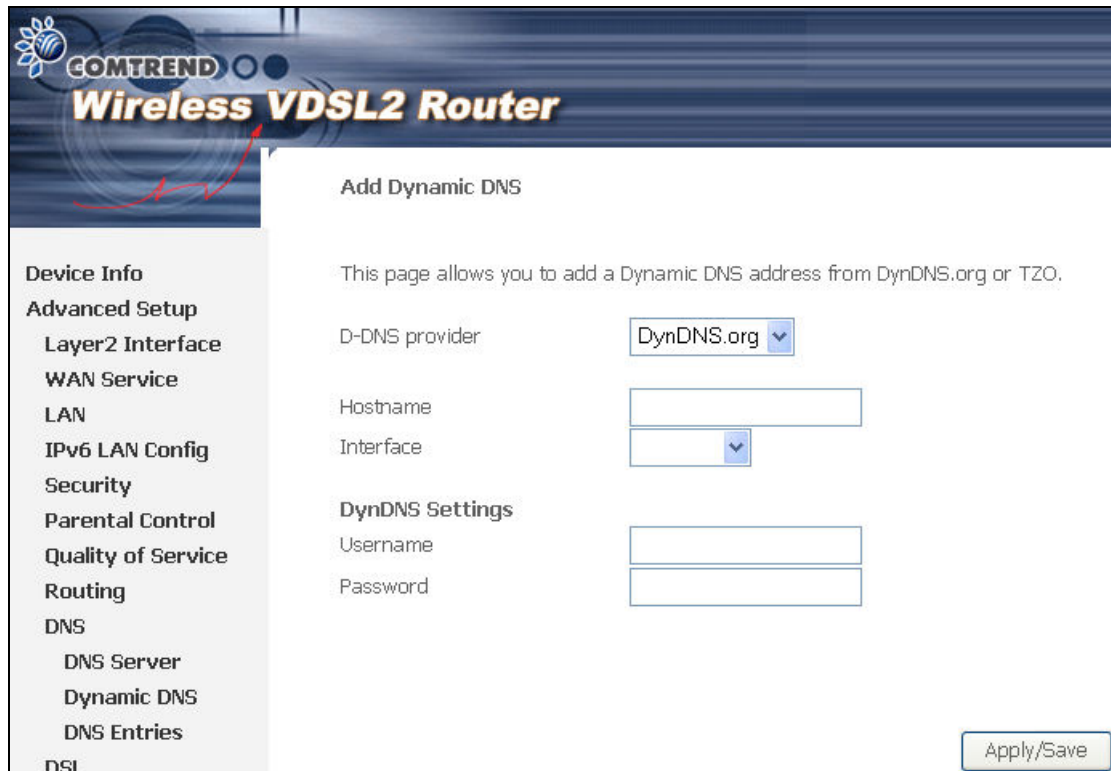
5.10.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static

hostname in any of many domains, allowing the CT-5374 to be more easily accessed from various locations on the Internet.



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



Consult the table below for field descriptions.

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

5.11 DSL

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

COMTREND Wireless VDSL2 Router

DSL Settings

Select the modulation below.

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

Select the profile below.

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

US0

- Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

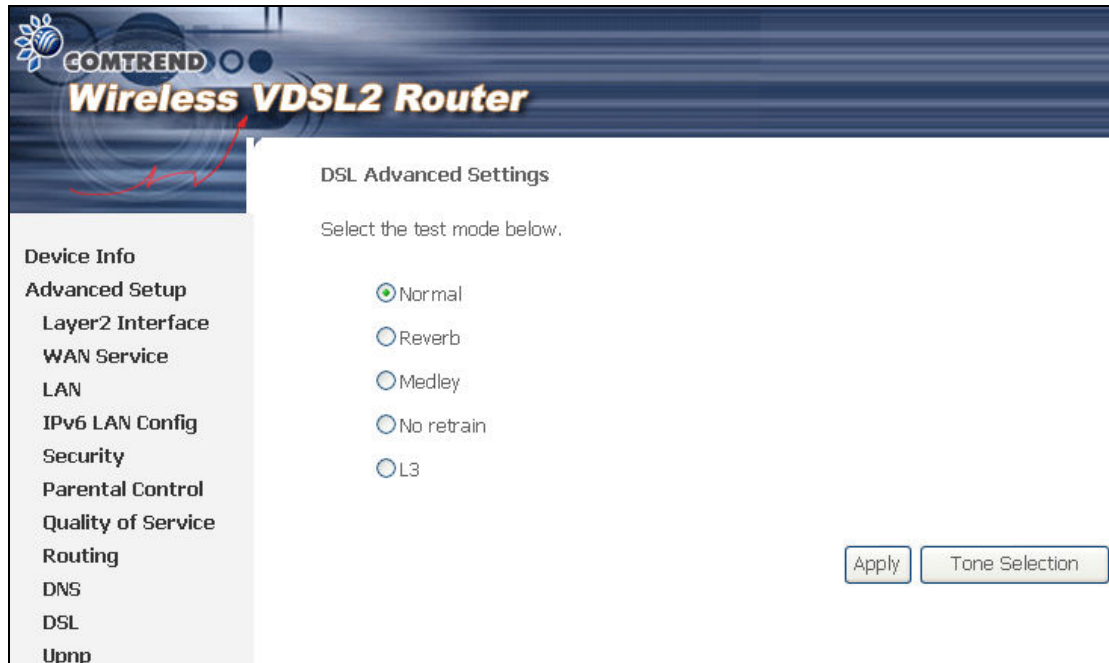
- Bitswap Enable
- SRA Enable

Apply/Save Advanced Settings

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
G.Dmt	Downstream: 12 Mbps Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates
ADSL2+	Downstream: 24 Mbps Upstream: 1.0 Mbps
AnnexM	Downstream: 24 Mbps Upstream: 3.5 Mbps
VDSL2	Downstream: 100 Mbps Upstream: 60 Mbps
Options	Description
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)
Profile Selection	8a-d, 12a-b, 17a, 30a, US0

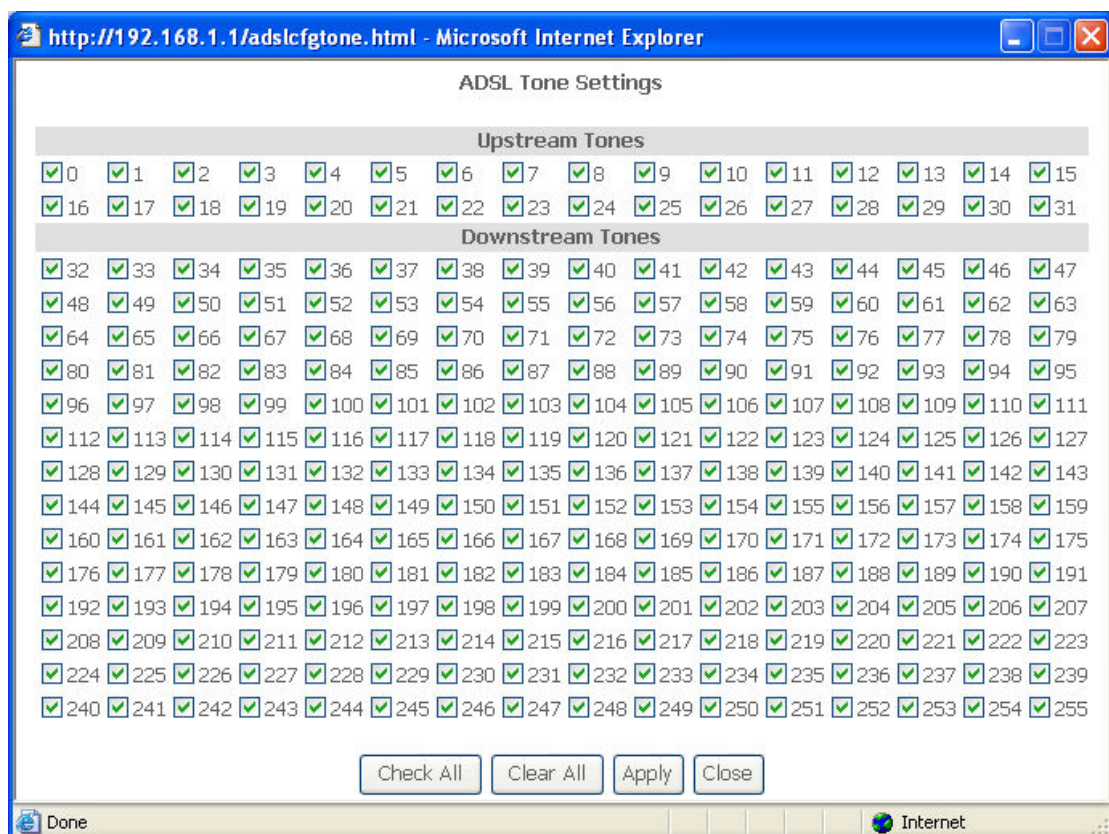
Advanced DSL Settings

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



The screenshot shows the 'DSL Advanced Settings' page of a GOMTREND Wireless VDSL2 Router. On the left is a navigation menu with options: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, IPv6 LAN Config, Security, Parental Control, Quality of Service, Routing, DNS, DSL, and Upnp. The main content area is titled 'DSL Advanced Settings' and contains the instruction 'Select the test mode below.' followed by five radio button options: Normal (selected), Reverb, Medley, No retrain, and L3. At the bottom right are two buttons: 'Apply' and 'Tone Selection'.

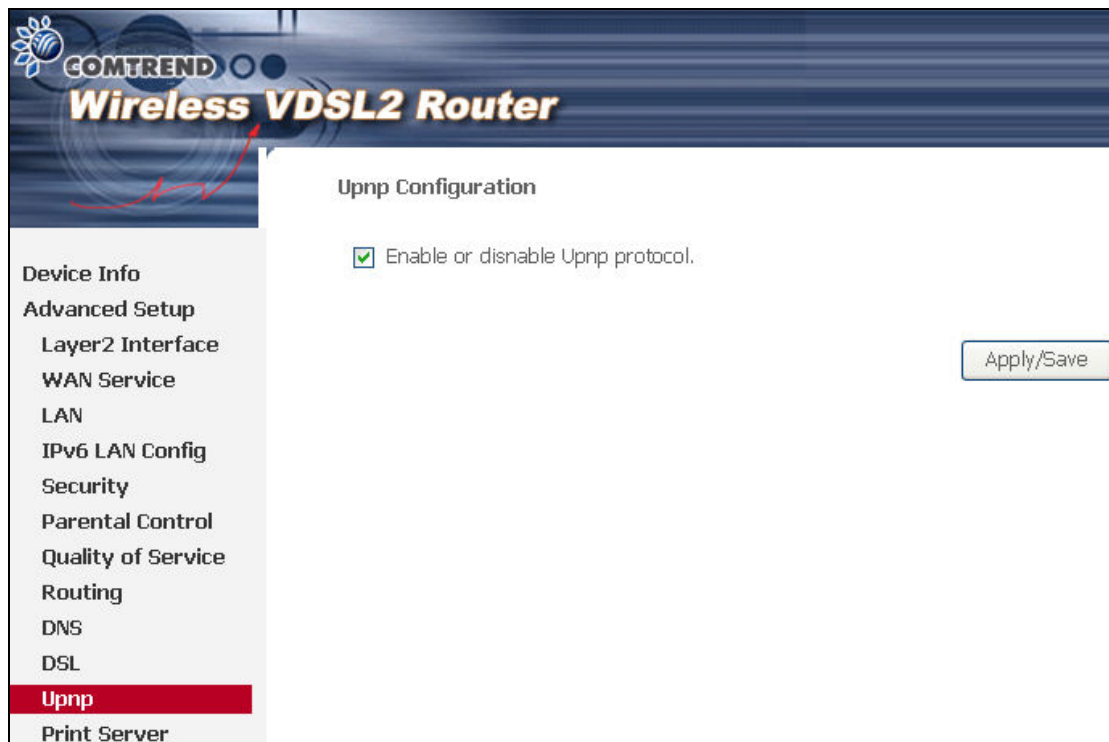
On this screen you select the tones you want activated, then click **Apply** and **Close**.



The screenshot shows a Microsoft Internet Explorer browser window displaying the 'ADSL Tone Settings' page. The address bar shows 'http://192.168.1.1/adslcfgtone.html'. The page title is 'ADSL Tone Settings'. It features two sections: 'Upstream Tones' and 'Downstream Tones'. Each section contains a grid of checkboxes, all of which are checked. The 'Upstream Tones' section includes checkboxes for tones 0 through 31. The 'Downstream Tones' section includes checkboxes for tones 32 through 255. At the bottom of the page are four buttons: 'Check All', 'Clear All', 'Apply', and 'Close'. The browser's status bar at the bottom shows 'Done' and 'Internet'.

5.12 UPnP

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



The screenshot shows the configuration interface for a Comtrend Wireless VDSL2 Router. The page title is "Wireless VDSL2 Router" and the current section is "Upnp Configuration". A sidebar on the left lists various configuration options, with "Upnp" highlighted in red. The main content area contains a single checkbox labeled "Enable or disable Upnp protocol." which is checked. An "Apply/Save" button is located on the right side of the page.

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
IPv6 LAN Config
Security
Parental Control
Quality of Service
Routing
DNS
DSL
Upnp
Print Server

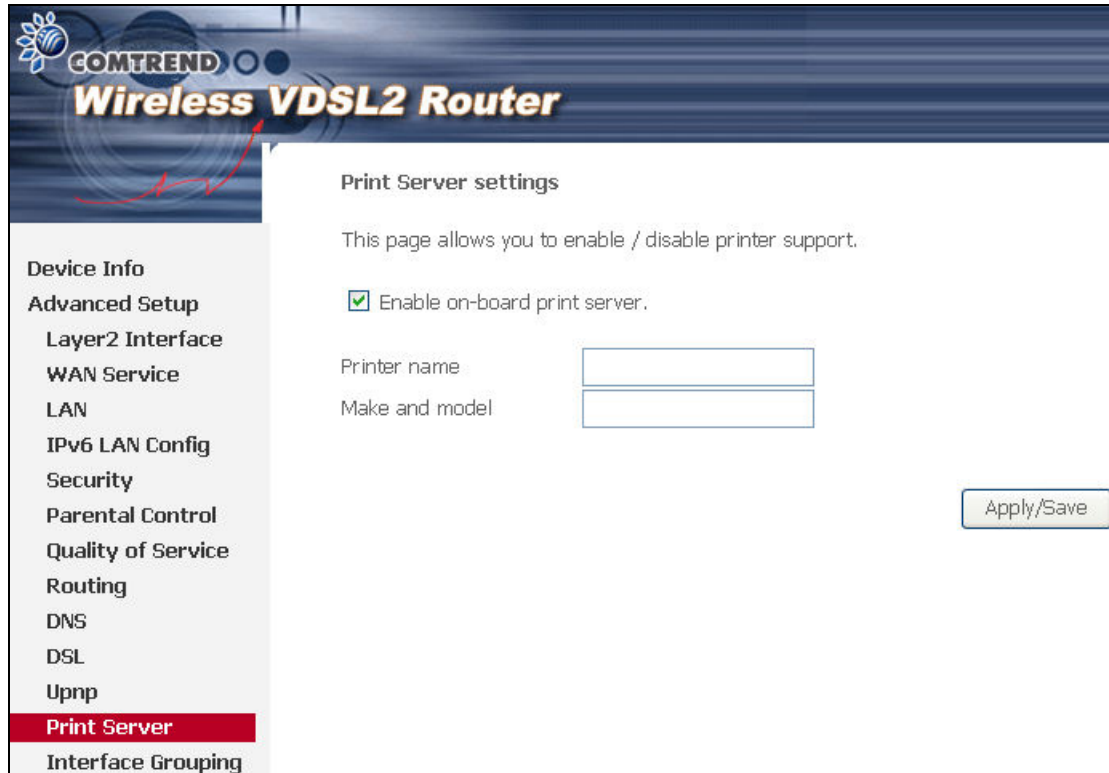
Upnp Configuration

Enable or disable Upnp protocol.

Apply/Save

5.13 Print Server

The CT-5374 can provide printer support through an optional USB2.0 host port. If your device has this port, refer to [Appendix F - Printer Server](#) for detailed setup instructions.



The screenshot displays the web management interface for a Comtrend Wireless VDSL2 Router. The page title is "Print Server settings". A navigation menu on the left includes: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, IPv6 LAN Config, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Upnp, **Print Server** (highlighted), and Interface Grouping. The main content area contains the following text and form elements:

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name

Make and model

5.14 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

COMTREND Wireless VDSL2 Router

Interface Grouping -- A maximum 16 entries can be configured

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

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			ETHWAN	
			ENET1	
			ENET2	
			ENET3	
			ENET4	
			wlan0	
			w10_Guest1	
			w10_Guest2	
			w10_Guest3	

Add Remove

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

COMTREND Wireless VDSL2 Router

Interface grouping Configuration

To create a new interface group:

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

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

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces:

Available LAN Interfaces:

Automatically Add Clients With the following DHCP Vendor IDs:

Apply/Save

Automatically Add Clients With Following DHCP Vendor IDs:

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

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

The Interface Grouping configuration will be:

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

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

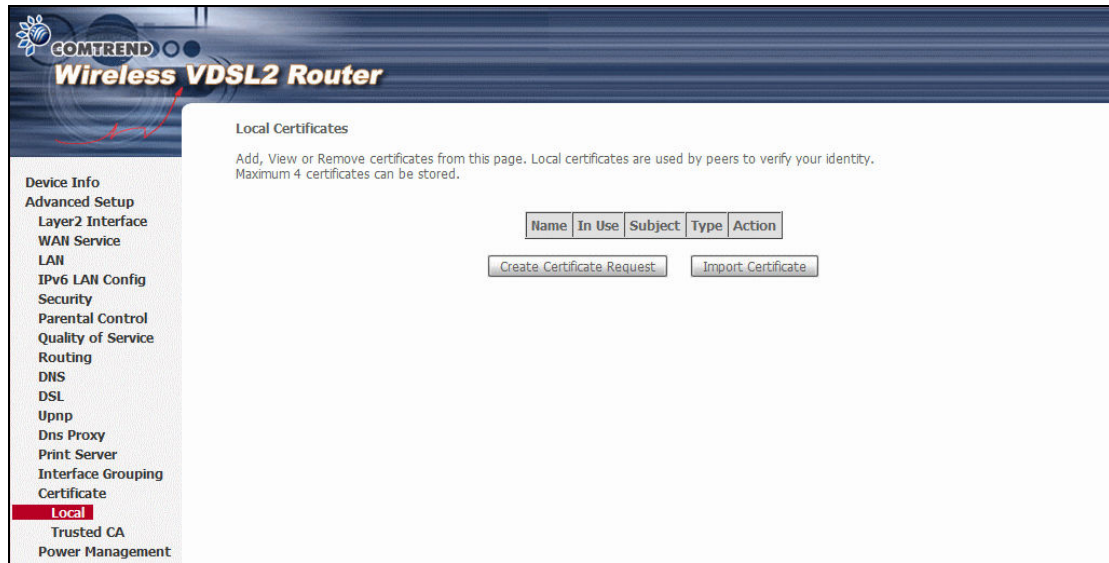
If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

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

5.15 Certificate

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

5.15.1 Local



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.



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.

Field	Description
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.

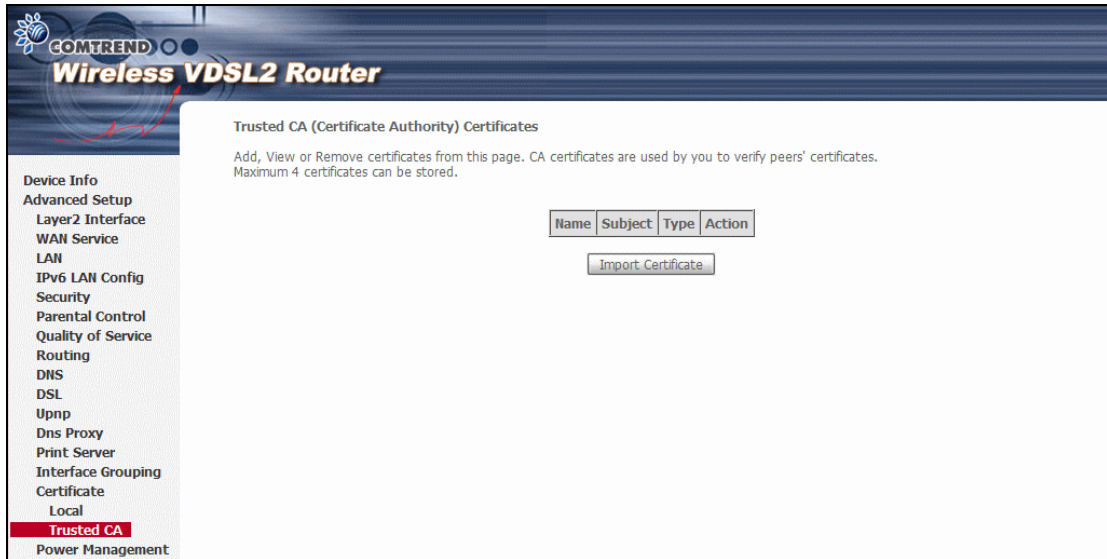
IMPORT CERTIFICATE

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

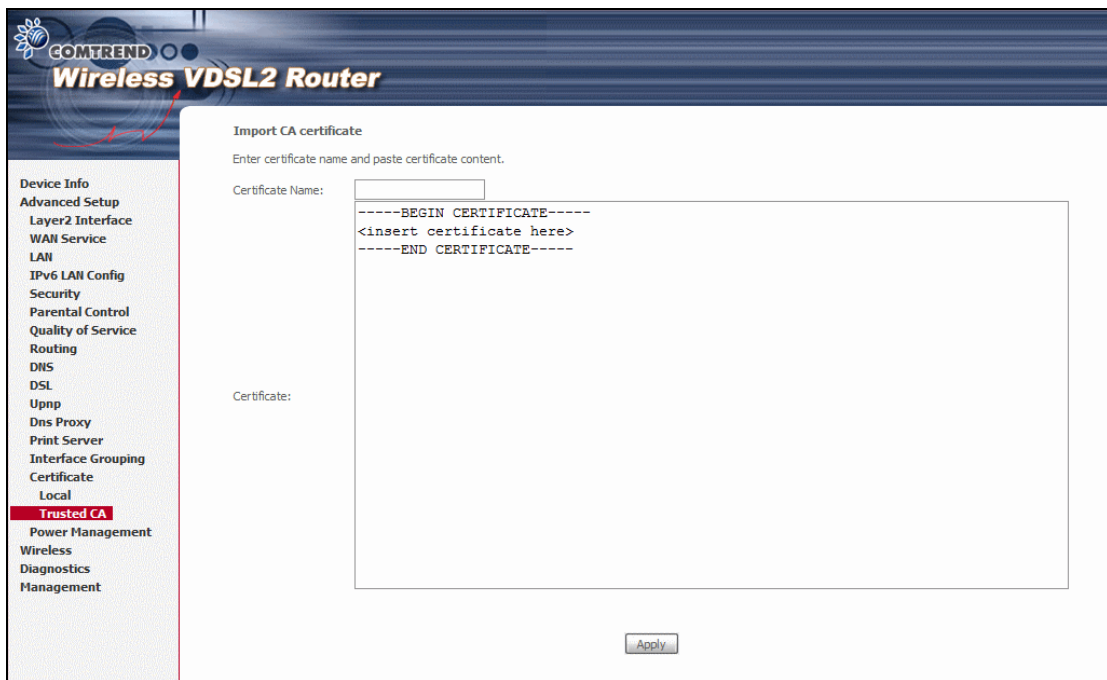
Enter a certificate name and click **Apply** to import the local certificate.

5.15.2 Trusted CA

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



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.



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

5.16 Power Management

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

The screenshot shows the configuration page for a Comtrend Wireless VDSL2 Router, specifically the Power Management section. The page title is "BCM6368 Power Management" and it includes a sub-header: "This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the response."

The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, IPv6 LAN Config, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Uppp, Dns Proxy, Print Server, Interface Grouping, Certificate, **Power Management** (highlighted), Wireless, Diagnostics, and Management.

The main configuration area includes the following sections:

- BCM6368 MIPS CPU Clock:** Radio buttons for 1/8 of full speed, 1/4 of Full speed, 1/2 of full speed, and Full speed (selected). A "full speed" button is visible.
- BCM6368 Linux TP uses r4K Wait instruction when Idle (IMPORTANT : SAVES POWER WHEN ENABLED):** A checkbox for "Enable" is unchecked, and the status is "Disabled".
- DRAM Auto Power Down Mode (IMPORTANT : SAVES POWER WHEN ENABLED):** A checkbox for "Enable" is unchecked, and the status is "Disabled".
- BCM6368 MIPS Voice TP and voice devices (slhc/slac):** A checkbox for "Enable" is checked, and the status is "Enabled".
- 802.11 Wireless:** A checkbox for "Enable Wireless" is checked, and the status is "Enabled".
- BCM6368 Ethernet:** Checkboxes for "Enable PHY0", "Enable PHY1", "Enable PHY2", "Enable PHY3", and "Enable Switch LEDs" are all checked. The status for each is "Enabled".
- BCM6368 USB Hosts Ports:** Checkboxes for "Enable USB Hosts" and "Enable USB Device" are both checked. The status for each is "Enabled".
- BCM6368 (A/V)DSL Link:** A checkbox for "Enable" is checked, and the status is "Enabled".

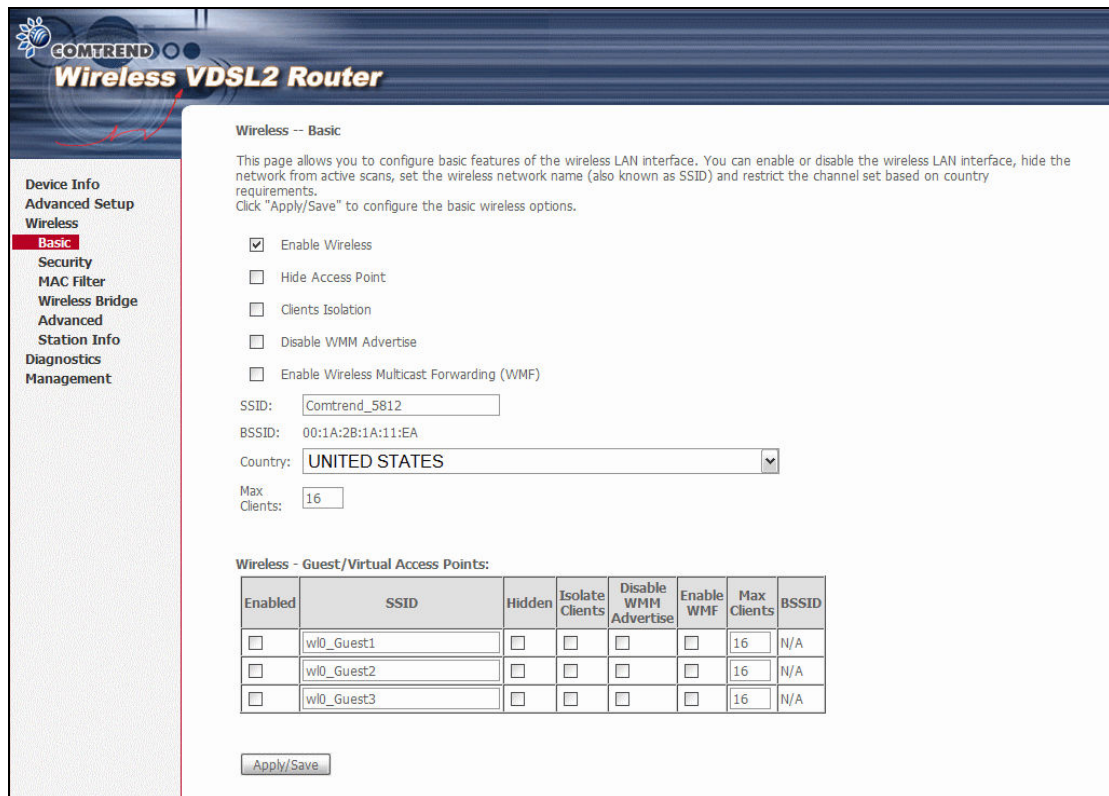
An "Apply" button is located at the bottom right of the configuration area.

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) and restrict the channel set based on country requirements.



Click **Save/Apply** to apply the selected wireless options.

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox <input checked="" type="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.

Option	Description
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 <input checked="" type="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.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	<p>This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes <input checked="" type="checkbox"/> in the Enabled column. To hide a Guest SSID select its checkbox <input checked="" type="checkbox"/> in the Hidden column.</p> <p>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.</p> <p>NOTE: Remote wireless hosts cannot scan Guest SSIDs.</p>

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.

The screenshot shows the configuration page for a Comtrend Wireless VDSL2 Router. The page title is "Wireless -- Security". It contains a sidebar menu on the left with options: Device Info, Advanced Setup, Wireless, Basic, Security (highlighted), MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area has the following sections:

- Wireless -- Security**: A paragraph stating, "This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protected Setup(WPS)".
- WSC Setup**: A form element "Enable WSC" with a dropdown menu set to "Disabled".
- Manual Setup AP**: A paragraph stating, "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." Below this are three form elements:
 - "Select SSID:" with a dropdown menu set to "Comtrend_5812".
 - "Network Authentication:" with a dropdown menu set to "Open".
 - "WEP Encryption:" with a dropdown menu set to "Disabled".
- An "Apply/Save" button at the bottom.

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

Apply/Save

The settings for WPA authentication are shown below.

Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP
WEP Encryption:	Disabled

Save/Apply

The settings for WPA-PSK authentication are shown next.

Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP
WEP Encryption:	Disabled

Apply/Save

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 both a PIN number and a push button, located on the device or accessed through device software. The CT-5374 has both a WPS button on the device and 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".



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 WSC AP Mode. **Configured** is used when the CT-5374 will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the CT-5374.



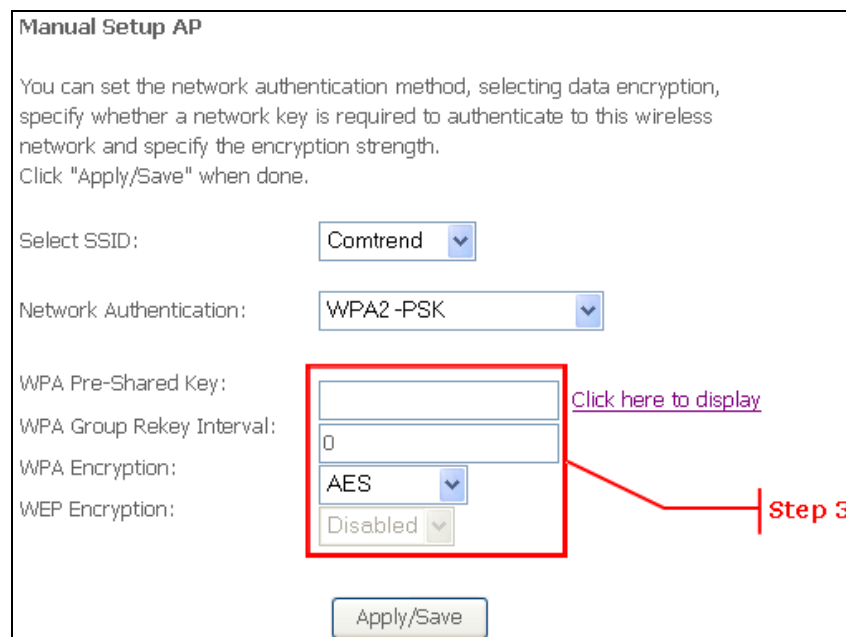
The image shows a dropdown menu for 'Set WSC AP Mode'. The selected option is 'Configured', indicated by a downward arrow on the right side of the box.

NOTES: Your client may or may not have the ability to provide security settings to the CT-5374. If it does not, then you must set the WSC 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 E - WSC External Registrar](#) 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.

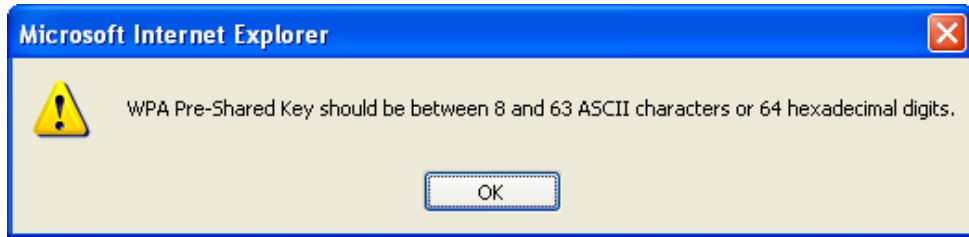


The image shows the 'Manual Setup AP' configuration screen. It includes the following fields and options:

- Select SSID: Comtrend
- Network Authentication: WPA2-PSK
- WPA Pre-Shared Key: [Empty text box]
- WPA Group Rekey Interval: 0
- WPA Encryption: AES
- WEP Encryption: Disabled
- Apply/Save button

A red box highlights the WPA Pre-Shared Key field. A red arrow points from the text 'Step 3' to this field. A purple link 'Click here to display' is positioned to the right of the key field.

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.



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: First method: WPS button

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

Second method: WUI virtual button

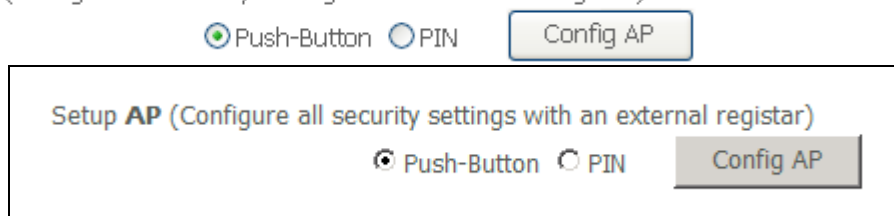
Select the Push-Button radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

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

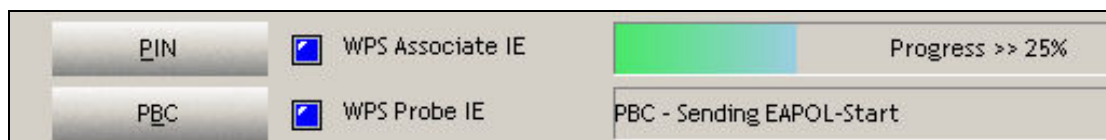


B - For Unconfigured mode, click the Config AP button.

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



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.



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

IIIb. WPS – PIN CONFIGURATION

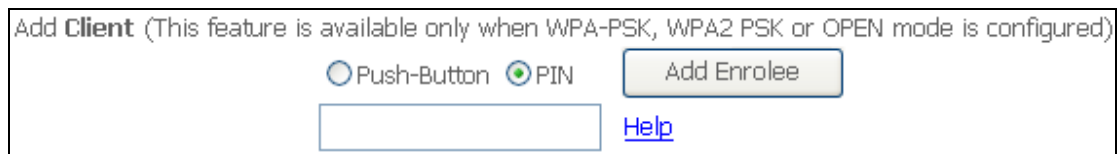
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific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

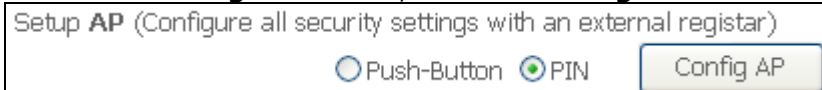
NOTE: Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

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, enter the client PIN in the box provided and then click the **Add Enrollee** button (see below).

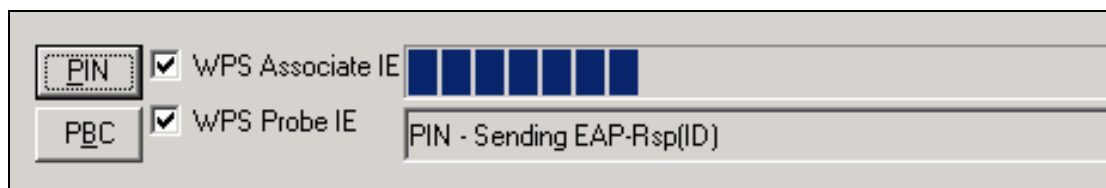


B - For Unconfigured mode, click the **Config AP** button.



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.

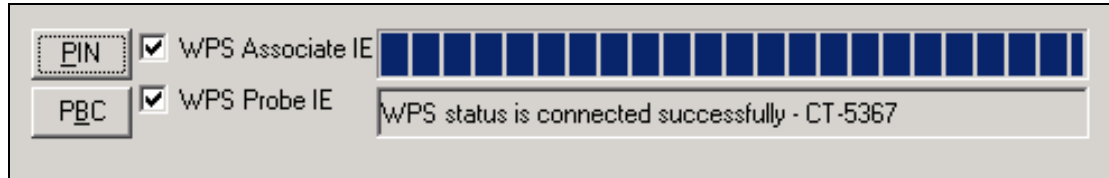
The figure below provides an example of a WPS client PIN function in-progress.



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.



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.

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**.

6.4 Wireless Bridge

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

The screenshot shows the configuration page for the Wireless Bridge feature on a Comtrend Wireless VDSL2 Router. The page title is "Wireless -- Bridge". The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, **Wireless Bridge** (highlighted), Advanced, Station Info, Diagnostics, and Management. The main content area contains the following text and form elements:

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.

Form fields:

- AP Mode:
- Bridge Restrict:
- Remote Bridges MAC Address:
-

Buttons: Refresh, Apply/Save

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

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: 1 Current: 1
 Auto Channel Timer (min): 0
 802.11n/EWC: Auto
 Bandwidth: 20MHz in 2.4G Band and 40MHz in 5G Band Current: 20MHz
 Control Sideband: Lower Current: None
 802.11n Rate: Auto
 802.11n Protection: Auto
 Support 802.11n Client Only: Off
 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

Apply/Save

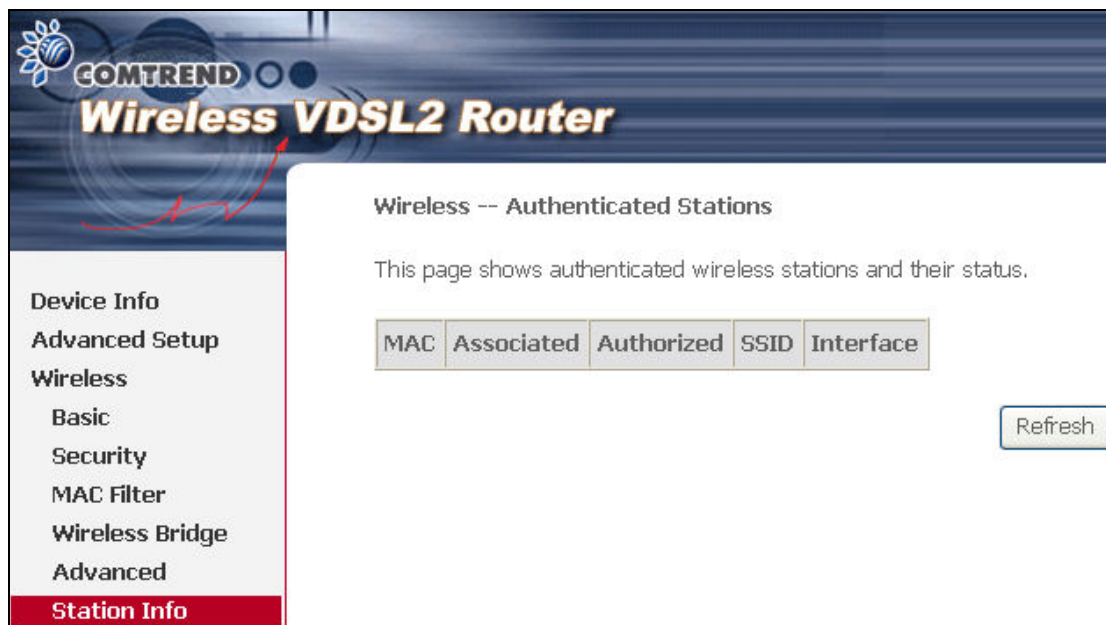
Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, 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.

Field	Description
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.
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.
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.

Field	Description
Xpress™ 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 Station Info

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



COMTREND
Wireless VDSL2 Router

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

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

Refresh

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

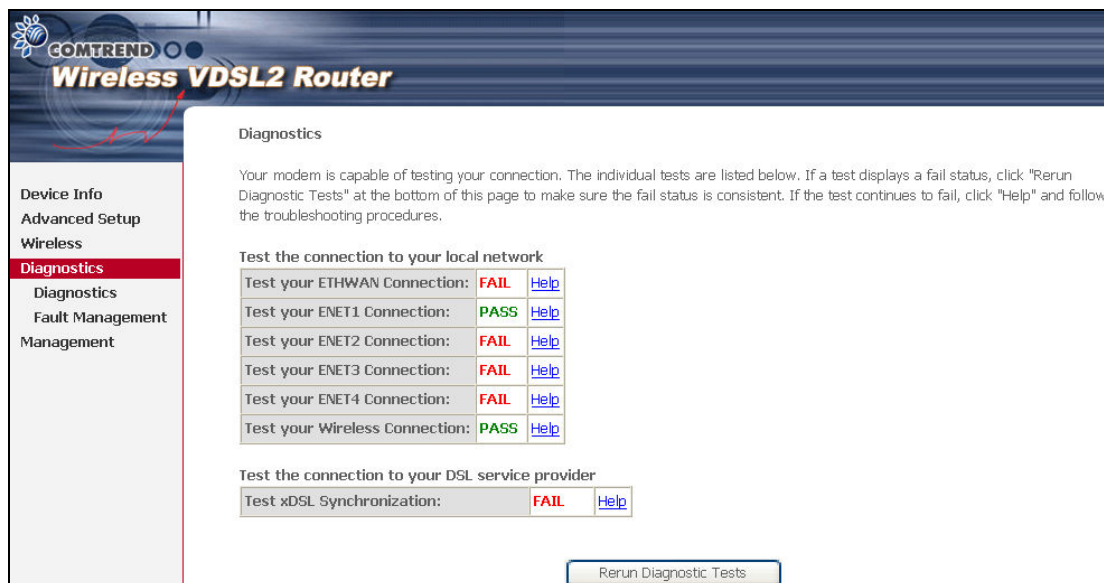
MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Consult the table below for descriptions of each column heading.

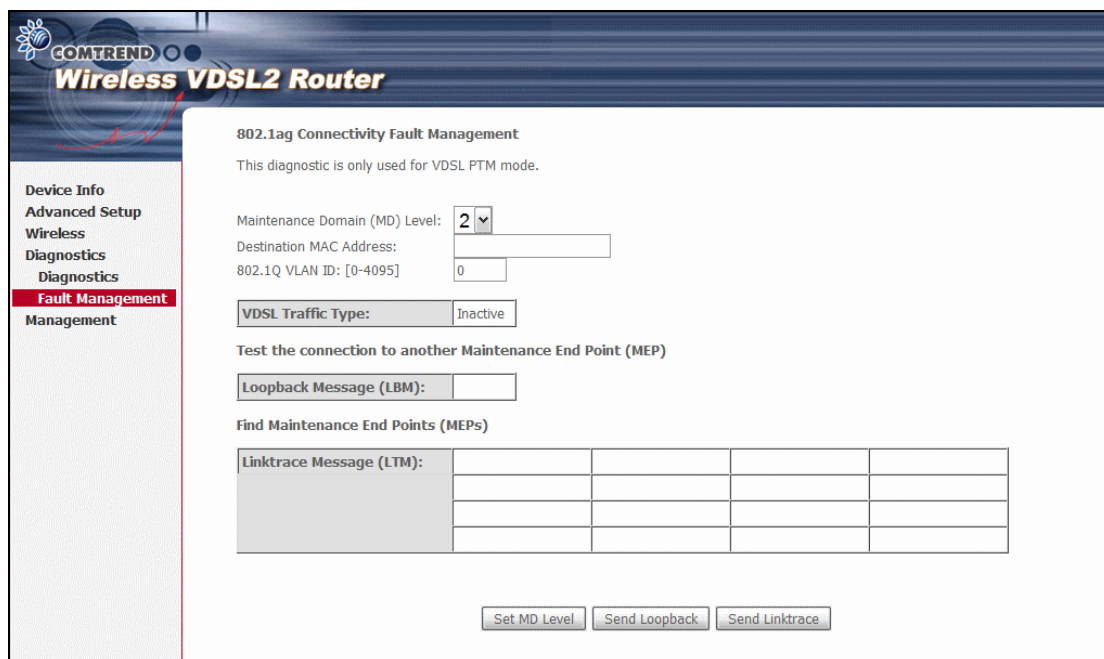
Heading	Description
MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized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

Chapter 7 Diagnostics

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



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



Chapter 8 Management

Click on the link to jump to a specific section:

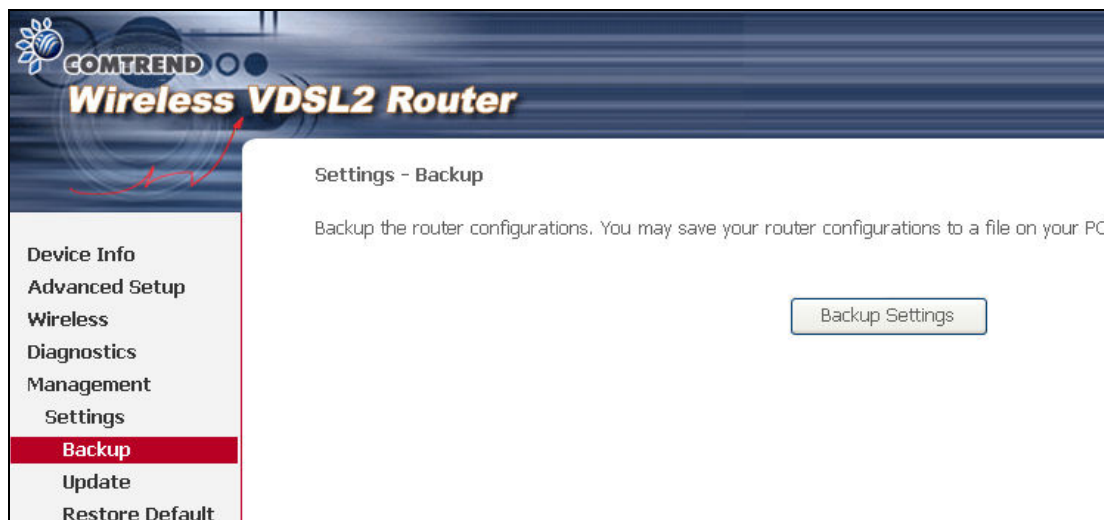
8.1 Settings	8.5 TR-069 Client
8.2 System Log	8.6 Access Control
8.3 SNMP Agent	8.7 Update Software
8.4 Internet Time	8.8 Reboot

8.1 Settings

This includes [8.1.1 Backup](#) Settings, [8.1.2 Update](#) Settings, and [8.1.3 Restore](#) Default screens.

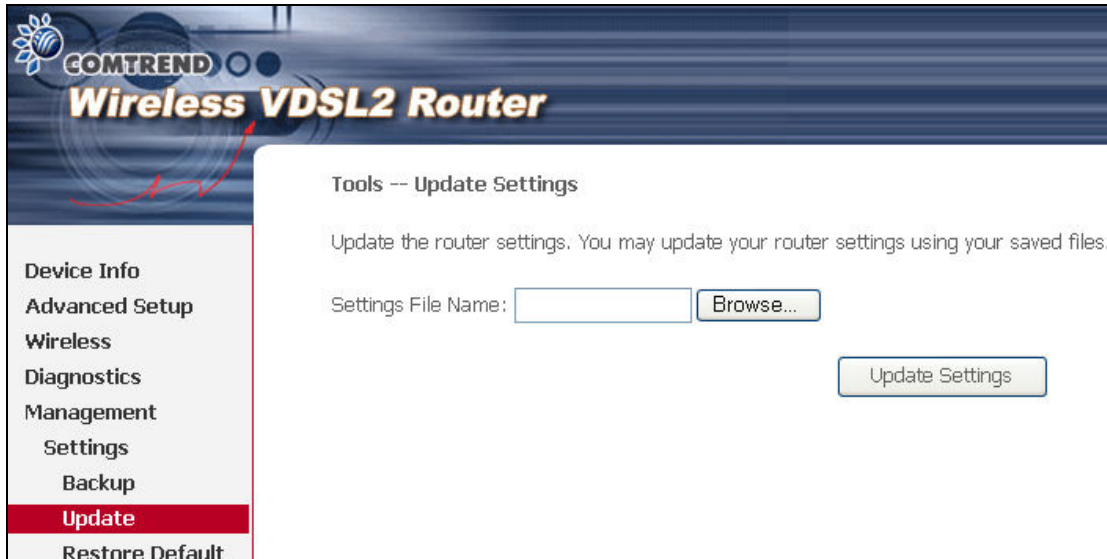
8.1.1 Backup Settings

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.



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.

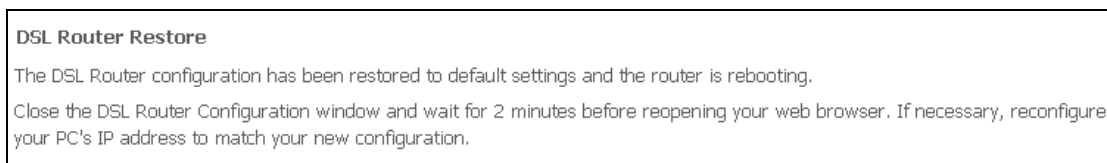


8.1.3 Restore Default

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



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



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.

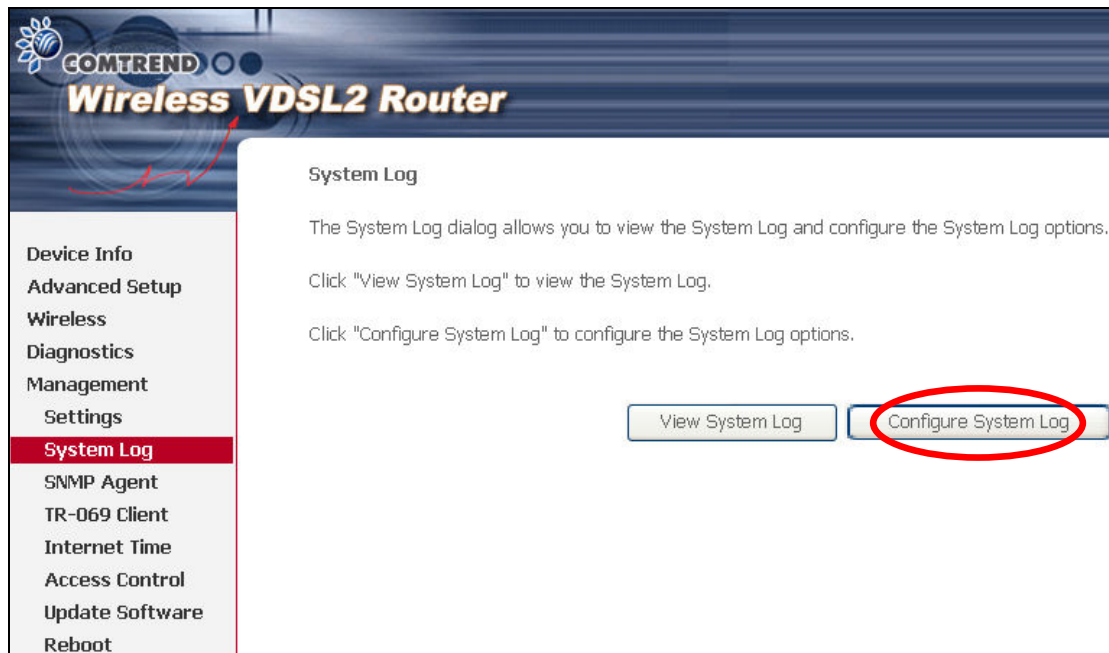
NOTE: This entry has the same effect as the **Reset** button. The CT-5374 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

8.2 System Log

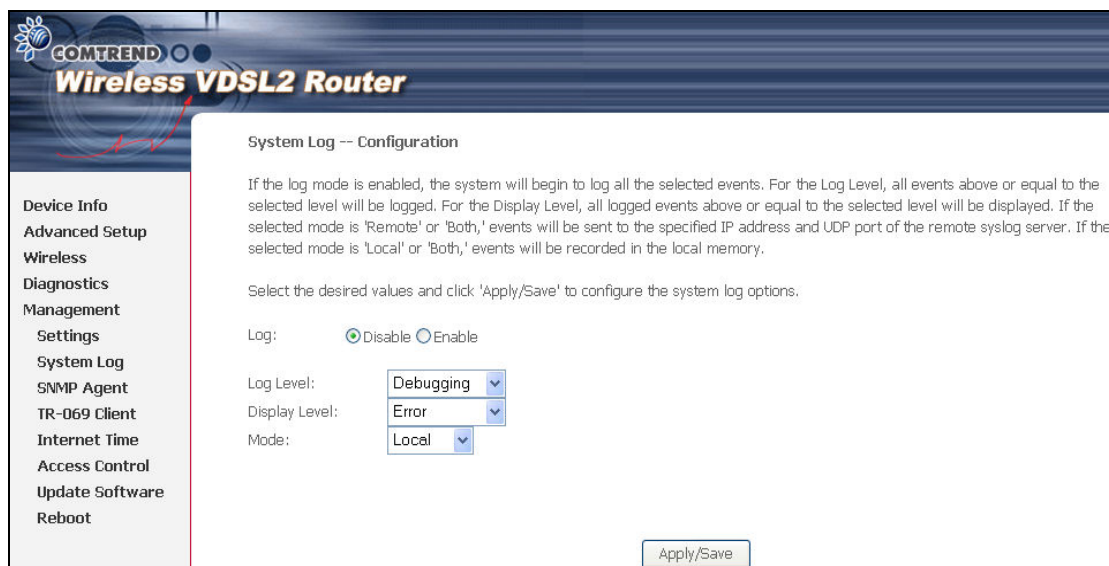
This function allows a system log to be kept and viewed upon request.

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

STEP 1: Click **Configure System Log**, as shown below (circled in **Red**).



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



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

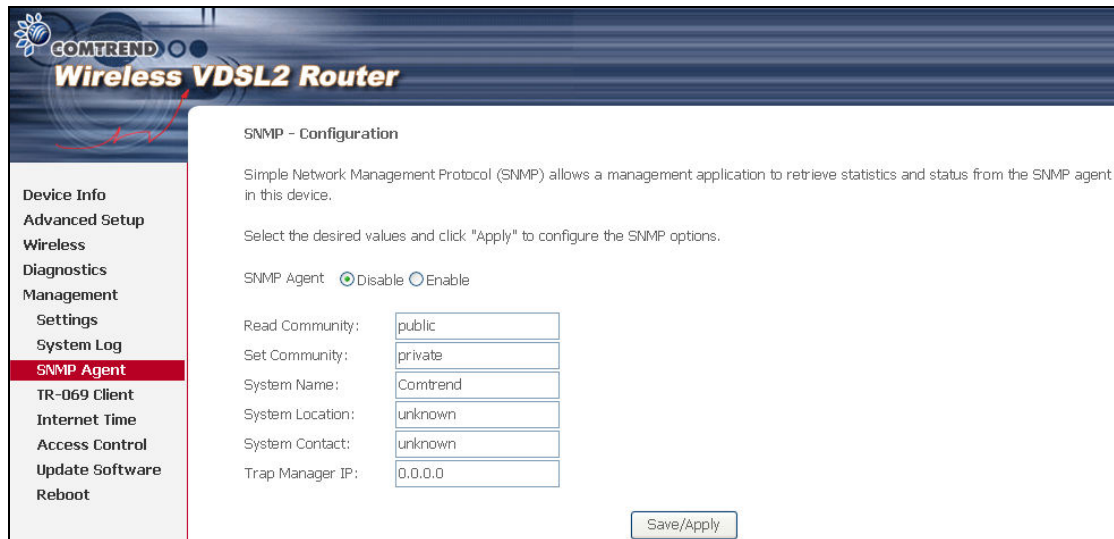
Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the Enable radio button and then click Apply/Save .
Log Level	<p>Allows you to configure the event level and filter out unwanted 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 CT-5374 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.</p> <p>The log levels are defined as follows:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
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.



The screenshot shows the configuration page for the SNMP Agent on a Comtrend Wireless VDSL2 Router. The page has a dark blue header with the Comtrend logo and the text "Wireless VDSL2 Router". On the left side, there is a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, **SNMP Agent** (highlighted in red), TR-069 Client, Internet Time, Access Control, Update Software, and Reboot. The main content area is titled "SNMP - Configuration" and contains the following text: "Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device." and "Select the desired values and click 'Apply' to configure the SNMP options." Below this text, there are two radio buttons for "SNMP Agent": "Disable" (selected) and "Enable". There are also five text input fields: "Read Community:" with the value "public", "Set Community:" with the value "private", "System Name:" with the value "Comtrend", "System Location:" with the value "unknown", and "System Contact:" with the value "unknown". At the bottom right of the configuration area, there is a "Trap Manager IP:" field with the value "0.0.0.0" and a "Save/Apply" button.

COMTREND
Wireless VDSL2 Router

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.

The table below is provided for ease of reference.

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

Option	Description
Display SOAP messages on serial console	Enable/Disable SOAP messages on serial console. This option is used for advanced troubleshooting of the device.
Connection Request	
Authorization	Tick the checkbox <input checked="" type="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 CT-5374.

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

8.5 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**.

The screenshot shows the configuration interface for a COMTREND Wireless VDSL2 Router. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings (highlighted), System Log, SNMP Agent, TR-069 Client, Internet Time (highlighted), Access Control, Update Software, and Reboot. The main content area is titled "Time settings" and includes the following configuration options:

- A checkbox labeled "Automatically synchronize with Internet time servers" which is checked.
- Five NTP time server fields:
 - 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
- An "Apply/Save" button at the bottom right.

NOTE: Internet Time must be activated to use [5.7 Parental Control](#) (page 43). 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 Passwords

This screen is used to configure the user account access passwords for the device. Access to the CT-5374 is controlled through the following three user accounts:

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

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

The screenshot shows the 'Access Control -- Passwords' configuration page. The left sidebar contains a menu with options: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, TR-069 Client, Internet Time, Access Control, Passwords (highlighted), Update Software, and Reboot. The main content area is titled 'Access Control -- Passwords' and contains the following text: 'Access to your router is controlled through three user accounts: root, support, and user.' It then lists the roles for 'root', 'support', and 'user'. Below this, it instructs the user to enter up to 16 characters for the passwords, with a note that spaces are not allowed. There are four input fields: 'Username' (a dropdown menu), 'Old Password', 'New Password', and 'Confirm Password'. An 'Apply/Save' button is located at the bottom right of the form.

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

8.7 Update Software

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

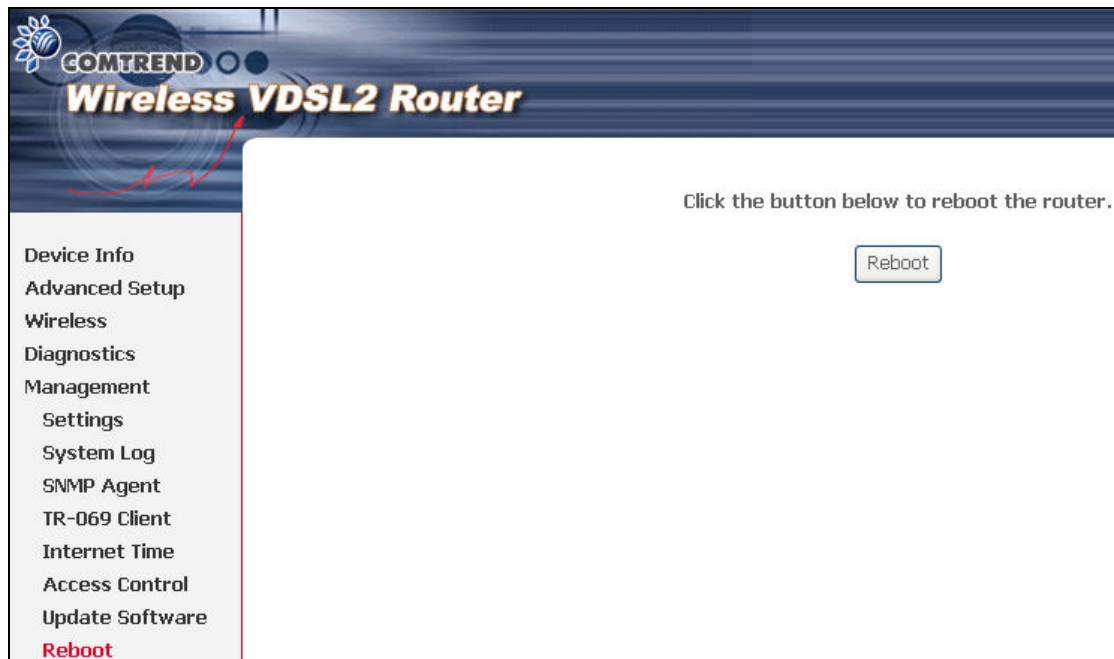
The screenshot shows the 'Tools -- Update Software' configuration page. The left sidebar contains a menu with options: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, TR-069 Client, Internet Time, Access Control, Update Software (highlighted), and Reboot. The main content area is titled 'Tools -- Update Software' and contains three steps: '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.', and 'Step 3: Click the "Update Software" button once to upload the new image file.' A note states: 'NOTE: The update process takes about 2 minutes to complete, and your router will reboot.' There is a 'Software File Name:' label followed by an input field and a 'Browse...' button. An 'Update Software' button is located at the bottom right of the form.

- 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**.



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

Appendix A - Firewall

STATEFUL PACKET INSPECTION

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

DENIAL OF SERVICE ATTACK

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

TCP/IP/PORT/INTERFACE FILTER

These rules help in the filtering of traffic at the Network layer (i.e. Layer 3).

When a Routing interface is created, **Enable Firewall** must be checked.

Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER

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

Example 1:

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

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

Example 2:

Filter Name	: Out_Filter2
Protocol	: UDP
Source IP Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 5060:6060
Dest. IP Address	: 172.16.13.4
Dest. Subnet Mask	: 255.255.255.0
Dest. Port	: 6060:7070

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

INCOMING IP FILTER

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

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

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

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

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

MAC LAYER FILTER

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

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

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

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

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

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the CT-5374, as per chosen days of the week and the chosen times.

Example: User Name : FilterJohn
 Browser's MAC Address : 00:25:46:78:63:21
 Days of the Week : Mon, Wed, Fri
 Start Blocking Time : 14:00
 End Blocking Time : 18:00

With this rule, a LAN device with MAC Address of 00:25:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix B - Pin Assignments

ETHERNET Ports (RJ45)

ETHERNET LAN Ports (10/100Base-T)

Pin	Signal name	Signal definition
1	TXP	Transmit data (positive lead)
2	TXN	Transmit data (negative lead)
3	RXP	Receive data (positive lead)
4	NC	Not used
5	NC	Not used
6	RXN	Receive data (negative lead)
7	NC	Not used
8	NC	Not used

Table 1

Signals for ETHERNET WAN port (10/1001000Base-T)

Pin	Signal name	Signal definition
1	TRD+(0)	Transmit/Receive data 0 (positive lead)
2	TRD-(0)	Transmit/Receive data 0 (negative lead)
3	TRD+(1)	Transmit/Receive data 1 (positive lead)
4	TRD+(2)	Transmit/Receive data 2 (positive lead)
5	TRD-(2)	Transmit/Receive data 2 (negative lead)
6	TRD-(1)	Transmit/Receive data 1 (negative lead)
7	TRD+(3)	Transmit/Receive data 3 (positive lead)
8	TRD-(3)	Transmit/Receive data 3 (negative lead)

Table 2

Appendix C - Specifications

Hardware Interface

- RJ-11 X 1 for ADSL2+/VDSL2
- RJ-45 X 4 for LAN (10/100 Base-T auto-sense)
- RJ-45X 1 for ETH WAN, (10/100/1000 BaseT auto-sense)
- Reset Button X 1
- WPS Button X 1
- Wi-Fi On/Off Button X 1
- Wi-Fi Antennas X 2
- Power Switch X 1
- USB Host X 1

WAN Interface

- ADSL2+ Downstream : 24 Mbps Upstream : 1.3 Mbps
- ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, AnnexM
- VDSL2 Downstream : 100 Mbps Upstream : 60 Mbps
- ITU-T G.993.2 (supporting profile 8a, 8b, 8c, 8d, 12a, 12b, 17a)

LAN Interface

- Standard IEEE 802.3, IEEE 802.3u
- MDI/MDX support Yes
- Multiple Subnets on LAN

Wireless Interface

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
- 11 Channels (US, Canada)/ 13 Channels (Europe)/ 14 Channels (Japan)
- Up to 300Mbps data rate
- Multiple BSSID
- MAC address filtering, WDS, WEP, WPA, WPA2, IEEE 802.1x
- 10,25,50,100mW@22MHz channel bandwidth output power level can be selected according to the environment
- Optional Afterburner mode (Turbo mode)***

ATM Attributes

- RFC 2684 (RFC 1483) Bridge/Route;
- RFC 2516 (PPPoE); RFC 2364 (PPPoA); RFC 1577 (IPoA)
- Support up to 16 PVCs
- AAL type AAL5
- ATM service class UBR/CBR/VBR-rt/VBR-nrt
- ATM UNI support UNI 3.1/4.0
- OAM F4/F5

PTM Attributes

- Dual Latency.....Yes

Management

- Compliant with TR-069/TR-098/TR-104/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, Packet and MAC address filtering, SSH,
- VPN termination
- Three level login: local admin, local user and remote technical support access

QoS

- Packet level QoS classification rules,
- Priority queuing using ATM TX queues,
- IP TOS/Precedence,
- 802.1p marking,
- DiffServ DSCP marking
- Src/dest MAC addresses classification

Firewall/Filtering

- Stateful Inspection Firewall
- Stateless Packet Filter
- Day-time Parental Control
- URI/URL filtering
- 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 Layer Gateway (ALG)

SIP, H.323, Yahoo messenger, ICQ, RealPlayer, Net2Phone, NetMeeting, MSN, X-box, Microsoft DirectX games and 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.....205 mm (W) x 48 mm (H) x 145 mm (D)

Kit Weight

(1*CT-5374, 1*RJ14 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM) = 1.0 kg

NOTE: Specifications are subject to change without notice
--

Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

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

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

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

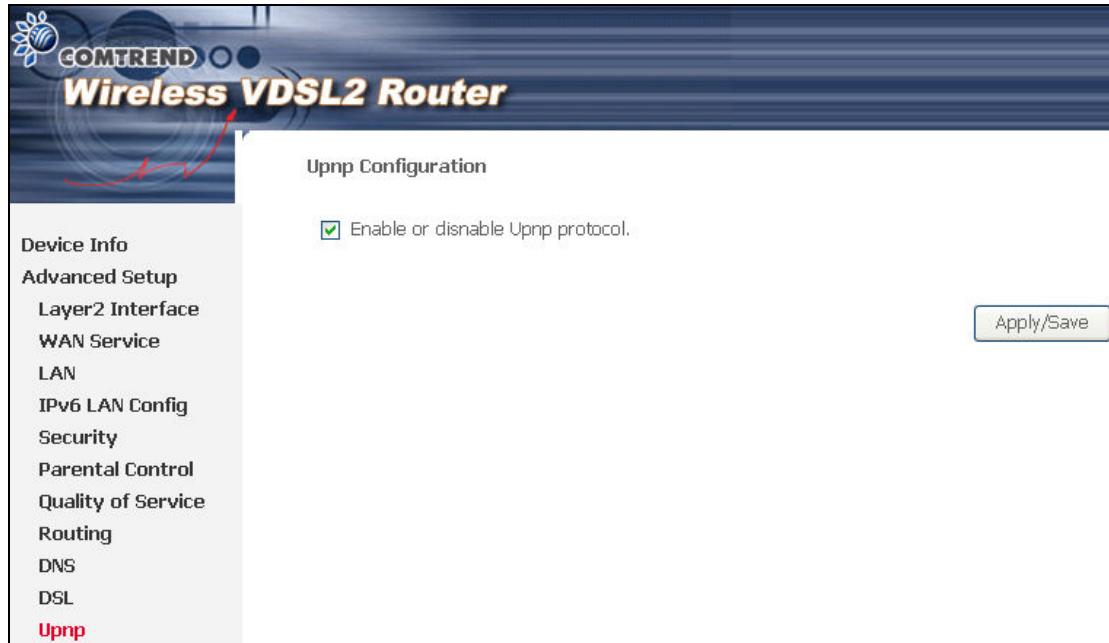
For WAN access, type: putty -ssh -l support WAN IP address

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

Appendix E - WSC External Registrar

Follow these steps to add an external registrar using the web user interface (WUI) on a personal computer running the Windows Vista operating system:

Step 1: Enable UPnP on the Advanced Setup.



Step 2: Open the Network folder and look for the BroadcomAP icon.