

VR-3031u

Multi-DSL Router

User Manual

Version A2.1, June 04, 2013



Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at <http://www.comtrend.com>

Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.



WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in [Appendix C - Specifications](#).

Copyright

Copyright©2013 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>

| |
|---|
| NOTE: This document is subject to change without notice. |
|---|

Protect Our Environment



This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed



separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

Table of Contents

| | |
|--|-----------|
| CHAPTER 1 INTRODUCTION..... | 6 |
| CHAPTER 2 INSTALLATION..... | 7 |
| 2.1 HARDWARE SETUP..... | 7 |
| 2.2 LED INDICATORS..... | 9 |
| CHAPTER 3 WEB USER INTERFACE..... | 11 |
| 3.1 DEFAULT SETTINGS | 11 |
| 3.2 IP CONFIGURATION..... | 12 |
| 3.3 LOGIN PROCEDURE..... | 14 |
| CHAPTER 4 DEVICE INFORMATION..... | 16 |
| 4.1 WAN | 17 |
| 4.2 STATISTICS..... | 18 |
| 4.2.1 LAN Statistics..... | 18 |
| 4.2.2 WAN Service | 19 |
| 4.2.3 XTM Statistics..... | 20 |
| 4.2.4 xDSL Statistics | 21 |
| 4.3 ROUTE | 26 |
| 4.4 ARP..... | 27 |
| 4.5 DHCP..... | 27 |
| 4.6 NAT SESSION | 29 |
| 4.7 IGMP PROXY | 30 |
| 4.8 IPV6 | 31 |
| 4.8.1 IPv6 Info..... | 31 |
| 4.8.2 IPv6 Neighbor | 32 |
| 4.8.3 IPv6 Route | 33 |
| 4.8.4 Network Map | 34 |
| CHAPTER 5 BASIC SETUP..... | 35 |
| 5.1 LAYER 2 INTERFACE | 35 |
| 5.1.1 WAN Service Setup | 36 |
| 5.2 NAT | 37 |
| 5.2.1 Virtual Servers | 37 |
| 5.2.2 Port Triggering..... | 38 |
| 5.2.3 DMZ Host..... | 40 |
| 5.2.4 IP Address Map | 41 |
| 5.2.5 IPSEC ALG..... | 43 |
| 5.2.6 SIP ALG..... | 44 |
| 5.3 LAN..... | 45 |
| 5.3.1 LAN IPv6 Autoconfig..... | 48 |
| 5.3.2 Static IP Neighbor | 51 |
| 5.3.3 UPnP..... | 52 |
| 5.4 WIRELESS | 53 |
| 5.4.1 Basic | 53 |
| 5.4.2 Security..... | 55 |
| CHAPTER 6 ADVANCED SETUP..... | 58 |
| 6.1 AUTO-DETECTION SETUP | 58 |
| 6.2 SECURITY | 63 |
| 6.2.1 IP Filtering | 63 |
| 6.2.2 MAC Filtering..... | 67 |
| 6.3 PARENTAL CONTROL..... | 69 |
| 6.3.1 Time Restriction..... | 69 |
| 6.3.2 URL Filter..... | 71 |
| 6.4 QUALITY OF SERVICE (QoS)..... | 73 |
| 6.4.1 QoS Queue Setup..... | 74 |
| 6.4.2 QoS Policer | 76 |
| 6.4.3 QoS Classification..... | 78 |

| | |
|--|------------|
| 6.5 ROUTING | 80 |
| 6.5.1 <i>Default Gateway</i> | 80 |
| 6.5.2 <i>Static Route</i> | 81 |
| 6.5.3 <i>Policy Routing</i> | 82 |
| 6.5.4 <i>RIP</i> | 83 |
| 6.6 DNS..... | 84 |
| 6.6.1 <i>DNS Server</i> | 84 |
| 6.6.2 <i>Dynamic DNS</i> | 85 |
| 6.6.3 <i>DNS Entries</i> | 86 |
| 6.6.4 <i>DNS Proxy/Relay</i> | 87 |
| 6.7 DSL..... | 88 |
| 6.8 HOME NETWORKING | 90 |
| 6.8.1 <i>Print Server</i> | 90 |
| 6.8.2 <i>DLNA</i> | 91 |
| 6.8.3 <i>Storage Service</i> | 92 |
| 6.9 INTERFACE GROUPING..... | 93 |
| 6.10 IP TUNNEL..... | 96 |
| 6.10.1 <i>IPv6inIPv4</i> | 96 |
| 6.10.2 <i>IPv4inIPv6</i> | 98 |
| 6.11 CERTIFICATE..... | 99 |
| 6.11.1 <i>Local</i> | 99 |
| 6.11.2 <i>Trusted CA</i> | 101 |
| 6.12 POWER MANAGEMENT | 102 |
| 6.13 MULTICAST..... | 103 |
| 6.14 WIRELESS..... | 105 |
| 6.14.1 <i>Basic</i> | 105 |
| 6.14.2 <i>Security</i> | 107 |
| 6.14.3 <i>MAC Filter</i> | 110 |
| 6.14.4 <i>Wireless Bridge</i> | 111 |
| 6.14.5 <i>Advanced</i> | 113 |
| CHAPTER 7 DIAGNOSTICS..... | 116 |
| 7.1 DIAGNOSTICS – INDIVIDUAL TESTS | 116 |
| 7.2 FAULT MANAGEMENT..... | 117 |
| 7.3 UPTIME STATUS..... | 118 |
| 7.4 PING | 119 |
| 7.5 TRACE ROUTE | 120 |
| 7.6 SYSTEM UTILIZATION | 121 |
| CHAPTER 8 MANAGEMENT | 122 |
| 8.1 SETTINGS..... | 122 |
| 8.1.1 <i>Backup Settings</i> | 122 |
| 8.1.2 <i>Update Settings</i> | 123 |
| 8.1.3 <i>Restore Default</i> | 123 |
| 8.2 SYSTEM LOG | 124 |
| 8.3 SNMP AGENT | 126 |
| 8.4 TR-069 CLIENT | 127 |
| 8.5 INTERNET TIME | 129 |
| 8.6 ACCESS CONTROL | 130 |
| 8.6.1 <i>Passwords</i> | 130 |
| 8.6.2 <i>Service Access</i> | 132 |
| 8.6.3 <i>IP Address</i> | 133 |
| 8.7 UPDATE SOFTWARE | 134 |
| 8.8 REBOOT..... | 135 |
| CHAPTER 9 LOGOUT | 136 |
| APPENDIX A - FIREWALL | 137 |
| APPENDIX B - PIN ASSIGNMENTS..... | 140 |
| APPENDIX C - SPECIFICATIONS..... | 141 |
| APPENDIX D - SSH CLIENT | 143 |

| | |
|---|------------|
| APPENDIX E- CONNECTION SETUP | 144 |
| APPENDIX F - WPS EXTERNAL REGISTRAR..... | 173 |
| APPENDIX G - PRINTER SERVER | 176 |

Chapter 1 Introduction

The VR-3031u is an 802.11n compliant Multi-DSL router that supports both ADSL2+ and VDSL2. The latter is a brand new standard and technology perfect for triple play (Video, Voice and Data) applications. The VR-3031u comes with four 10/100 Base-T Ethernet ports, and one USB host, combining wired LAN connectivity and an integrated 802.11n WiFi WLAN Access Point (AP) for wireless connectivity.

The VR-3031u is a cost effective solution designed to meet the needs of ISPs and carriers planning on deploying a single DSL device for covering end users in different loop range areas. Deploying VR-3031u is cost effective for ISPs and carriers because deploying a single CPE DSL device with multiple profile support minimizes the number of required upgrades.

Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.



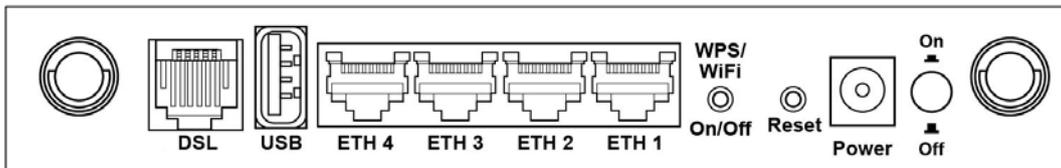
DO NOT STACK

Non-stackable

This device is not stackable – do not place units on top of each other, otherwise damage could occur.

BACK PANEL

The figure below shows the back panel of the device.



Power ON

Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section [2.2 LED Indicators](#)).

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

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

Reset Button

Restore the default parameters of the device by pressing the Reset button for 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section [2.2 LED Indicators](#) for details).

NOTE: If pressed down for more than 60 seconds, the VR-3031u will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

WPS/WiFi Button

Press and release WPS-WiFi button to activate WPS (make sure the WPS is enabled in Wireless->Security page).

Press and hold WPS-WIFI button more than 5 seconds to enable/disable WiFi.

Ethernet (LAN) Ports

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

USB Host Port (Type A)

This port can be used to connect the router to the print server.

DSL Port

Connect to an ADSL2/2+ or VDSL with this RJ11 Port. This device contains a micro filter which removes the analog phone signal. If you wish, you can connect a regular telephone to the same line by using a POTS splitter.

2.2 LED Indicators

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



| LED | Color | Mode | Function |
|------------|-------|-------|--|
| POWER | Green | On | The device is powered up. |
| | | Off | The device is powered down. |
| | Red | On | POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. |
| ETH 1 to 4 | Green | On | An Ethernet Link is established. |
| | | Off | An Ethernet Link is not established. |
| | | Blink | Data transmitting or receiving over LAN. |
| WLAN | Green | On | The wireless module is ready. (i.e. installed and enabled). |
| | | Off | The wireless module is not ready. (i.e. either not installed or disabled). |
| | | Blink | Data transmitting or receiving over WLAN. |
| WPS | Green | On | WPS enabled and PC connected to WLAN. |
| | | Off | WPS disabled when WPS configured. After clients are connected to router for about 5 minutes, LED is OFF. |
| | | Blink | The router is searching for WPS clients or WPS is un-configured. |
| USB | Green | On | USB mass storage, USB hub or USB printer is connected; or USB dongle connection is UP. |
| | | Off | No USB device connected. |
| | Red | On | USB dongle attached, connection is DOWN. |
| DSL | Green | On | xDSL Link is established. |
| | | Off | xDSL Link is not established. |
| | | Blink | fast: xDSL Link is training or data transmitting. slow: xDSL training failed. |
| INTERNET | Green | On | IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present. |

| | | | |
|--|-------|-------|---|
| | Green | Off | Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off. |
| | | Blink | IP connected and IP Traffic is passing thru the device (either direction) |
| | Red | On | Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.) |

Chapter 3 Web User Interface

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

3.1 Default Settings

The factory default settings of this device are summarized below.

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

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the VR-3031u powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

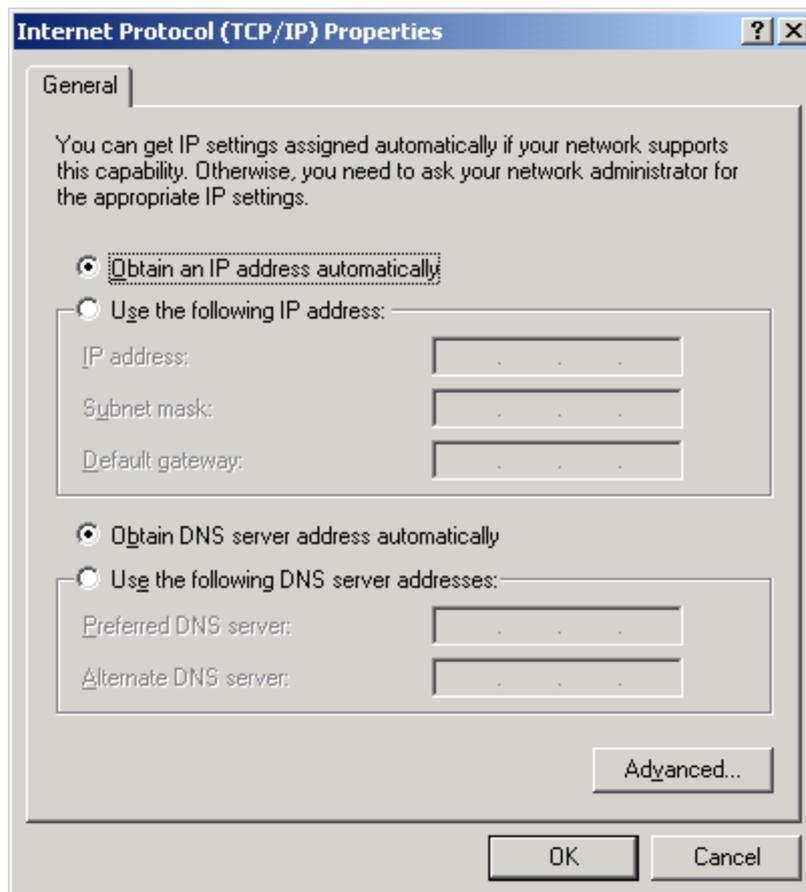
To obtain an IP address from the DHCP server, follow the steps provided below.

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

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

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

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



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

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

STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

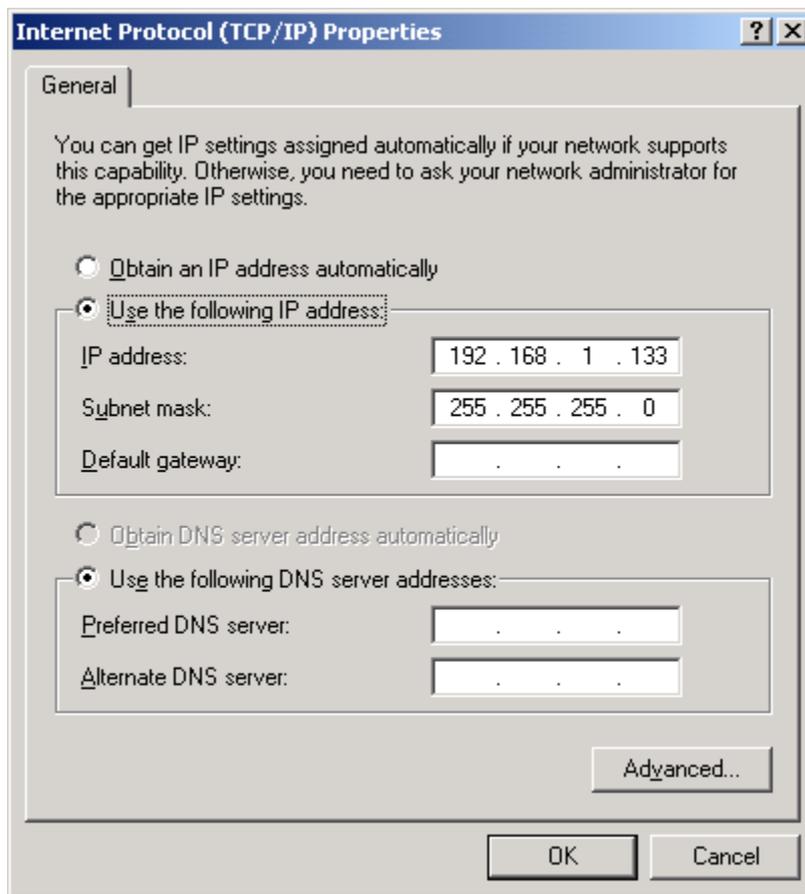
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

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



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

3.3 Login Procedure

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

NOTE: The default settings can be found in section [3.1 Default Settings](#).

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

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

STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section [3.1 Default Settings](#).



Click **OK** to continue.

NOTE: The login password can be changed later (see section [8.6.1 Passwords](#)).

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

The screenshot shows the Comtrend web management interface. At the top, there is a navigation bar with the Comtrend logo and several icons representing different management sections: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, the main content area is divided into several sections:

- Device:** A table listing hardware and software details.

| | |
|--------------------------|-------------------------------------|
| Model | VR-3031u |
| Board ID | 963168M-1341N1 |
| Serial Number | 1263031UXXF-AA000036 |
| Firmware Version | RA31-412CTU-C03_R01.A2pv6F038n.d24j |
| Bootloader (CFE) Version | 1.0.38-112.118-13 |
| Up Time | 2 mins:35 secs |
- Wireless:** A table listing wireless network settings.

| | |
|------------------------|---|
| Driver Version | 5.100.138.2008.cpe4.12L068.4 |
| Status | Enabled |
| Mode | Mixed 802.11b, 802.11g, 802.11n |
| Channel | 1 |
| Security | Secure |
| Primary SSID | Comtrend_FF38 |
| Primary Encryption | WPA2-PSK TKIP+AES |
| Primary Passphrase/Key | •••••••••• <input type="button" value="Show"/> |
- LAN:** A diagram showing four LAN ports (Port 1, Port 2, Port 3, Port 4) and a table of LAN settings.

| | |
|----------------------|-------------------|
| LAN IPv4 Address | 192.168.1.1 |
| LAN Subnet Mask | 255.255.255.0 |
| LAN MAC Address | 38:72:c0:52:ff:38 |
| DHCP Server | Enabled |
| LAN IPv6 ULA Address | |
- WAN:** A table listing WAN settings.

| | |
|----------------------|-----------------|
| Speed (down/up) | 0 kbps / 0 kbps |
| Default Gateway | |
| Primary DNS Server | 0.0.0.0 |
| Secondary DNS Server | 0.0.0.0 |
| Default IPv6 Gateway | |

You can also reach this page by clicking on the following icon located at the top of the screen.



Chapter 4 Device Information

You can reach this page by clicking on the following icon located at the top of the screen.



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

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

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

The Device Info Summary screen displays at startup.

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

| Device | |
|--------------------------|-------------------------------------|
| Model | VR-3031u |
| Board ID | 963168M-1341N1 |
| Serial Number | 1263031UXXF-AA000036 |
| Firmware Version | RA31-412CTU-C03_R01.A2pv6F038n.d24j |
| Bootloader (CFE) Version | 1.0.38-112.118-13 |
| Up Time | 2 mins:35 secs |

| Wireless | |
|------------------------|--|
| Driver Version | 5.100.138.2008.cpe4.12L068.4 |
| Status | Enabled |
| Mode | Mixed 802.11b, 802.11g, 802.11n |
| Channel | 1 |
| | Secure |
| Primary SSID | Comtrend_FF38 |
| Primary Encryption | WPA2-PSK TKIP+AES |
| Primary Passphrase/Key | <input type="button" value="Show"/> |

| LAN | |
|----------------------|-------------------|
| LAN IPv4 Address | 192.168.1.1 |
| LAN Subnet Mask | 255.255.255.0 |
| LAN MAC Address | 38:72:c0:52:ff:38 |
| DHCP Server | Enabled |
| LAN IPv6 ULA Address | |

| WAN | |
|----------------------|-----------------|
| Speed (down/up) | 0 kbps / 0 kbps |
| Default Gateway | |
| Primary DNS Server | 0.0.0.0 |
| Secondary DNS Server | 0.0.0.0 |
| Default IPv6 Gateway | |

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

4.1 WAN

Select WAN from the Device Info submenu to display the configured PVC(s).

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

4.2 Statistics

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

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

4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.

| Interface | Received | | | | Transmitted | | | |
|-----------|----------|------|------|-------|-------------|------|------|-------|
| | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Errs | Drops |
| ENET1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ENET2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ENET3 | 760254 | 7454 | 0 | 0 | 1751333 | 4053 | 0 | 0 |
| ENET4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| w10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Heading | Description |
|-----------------------|--|
| Interface | LAN interface(s) |
| Received/Transmitted: | <ul style="list-style-type: none"> - Bytes - Pkts - Errs - Drops |
| | <ul style="list-style-type: none"> Number of Bytes Number of Packets Number of packets with errors Number of dropped packets |

4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.

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

4.2.3 XTM Statistics

The following figure shows ATM (Asynchronous Transfer Mode)/PTM(Packet Transfer Mode) statistics.



ATM Interface Statistics

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

4.2.4 xDSL Statistics

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

VDSL

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6

Statistics -- xDSL

| | | | | |
|--|------------|----------|------------|----------|
| Mode: | ADSL2+ | | | |
| Traffic Type: | ATM | | | |
| Status: | Up | | | |
| Link Power State: | LO | | | |
| | Downstream | Upstream | | |
| PhyR Status: | Off | Off | | |
| Line Coding (Trellis): | On | On | | |
| SNR Margin (0.1 dB): | 71 | 64 | | |
| Attenuation (0.1 dB): | 20 | 116 | | |
| Output Power (0.1 dBm): | 111 | 123 | | |
| Attainable Rate (Kbps): | 27124 | 1009 | | |
| | Path 0 | Path 1 | | |
| | Downstream | Upstream | Downstream | Upstream |
| Rate (Kbps): | 25711 | 1001 | 3808 | 416 |
| MSGc (# of bytes in overhead channel message): | 56 | 13 | 0 | 0 |
| B (# of bytes in Mux Data Frame): | 119 | 13 | 0 | 0 |
| M (# of Mux Data Frames in FEC Data Frame): | 2 | 16 | 0 | 0 |
| T (Mux Data Frames over sync bytes): | 7 | 8 | 0 | 0 |
| R (# of check bytes in FEC Data Frame): | 14 | 10 | 0 | 0 |
| S (ratio of FEC over PMD Data Frame length): | 0.2983 | 7.0909 | 0.0000 | 0.0000 |
| L (# of bits in PMD Data Frame): | 6811 | 264 | 0 | 0 |
| D (interleaver depth): | 64 | 8 | 0 | 0 |
| Delay (msec): | 5 | 14 | 0 | 0 |
| INP (DMT symbol): | 0.50 | 1.00 | 0.00 | 0.00 |
| Super Frames: | 59569 | 11666 | 0 | 0 |
| Super Frame Errors: | 0 | 0 | 0 | 0 |
| RS Words: | 644983 | 26541 | 0 | 0 |
| RS Correctable Errors: | 0 | 0 | 0 | 0 |
| RS Uncorrectable Errors: | 0 | 0 | 0 | 0 |
| HEC Errors: | 0 | 0 | 0 | 0 |
| OCD Errors: | 0 | 0 | 0 | 0 |
| LCD Errors: | 0 | 0 | 0 | 0 |
| Total Cells: | 2919153 | 105731 | 0 | 0 |
| Data Cells: | 26 | 42 | 0 | 0 |
| Bit Errors: | 0 | 0 | 0 | 0 |
| Total ES: | 0 | 0 | | |
| Total SES: | 0 | 0 | | |
| Total UAS: | 619 | 619 | | |

xDSL BER Test Reset Statistics Draw Graph

ADSL

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6

Statistics -- xDSL

| | | | | |
|--|------------|----------|------------|----------|
| Mode: | VDSL2 | | | |
| Traffic Type: | PTM | | | |
| Status: | Up | | | |
| Link Power State: | LO | | | |
| | Downstream | | Upstream | |
| PhyR Status: | Off | Off | | |
| Line Coding (Trellis): | On | Off | | |
| SNR Margin (0.1 dB): | 189 | 0 | | |
| Attenuation (0.1 dB): | 65 | 0 | | |
| Output Power (0.1 dBm): | 145 | -225 | | |
| Attainable Rate (Kbps): | 136621 | 17326 | | |
| | Path 0 | | Path 1 | |
| | Downstream | Upstream | Downstream | Upstream |
| Rate (Kbps): | 79999 | 17326 | 0 | 0 |
| B (# of bytes in Mux Data Frame): | 63 | 223 | 0 | 0 |
| M (# of Mux Data Frames in an RS codeword): | 1 | 1 | 0 | 0 |
| T (# of Mux Data Frames in an OH sub-frame): | 59 | 1 | 0 | 0 |
| R (# of redundancy bytes in the RS codeword): | 16 | 16 | 0 | 0 |
| S (# of data symbols over which the RS code word spans): | 0.0255 | 0.4103 | 0.0000 | 0.0000 |
| L (# of bits transmitted in each data symbol): | 25144 | 4680 | 0 | 0 |
| D (interleaver depth): | 997 | 163 | 0 | 0 |
| I (interleaver block size in bytes): | 80 | 120 | 0 | 0 |
| N (RS codeword size): | 80 | 240 | 0 | 0 |
| Delay (msec): | 6 | 8 | 0 | 0 |
| INP (DMT symbol): | 2.50 | 1.00 | 0.00 | 0.00 |
| OH Frames: | 10606 | 1655 | 0 | 0 |
| OH Frame Errors: | 0 | 0 | 0 | 0 |
| RS Words: | 1721931 | 107484 | 0 | 0 |
| RS Correctable Errors: | 0 | 0 | 0 | 0 |
| RS Uncorrectable Errors: | 0 | 0 | 0 | 0 |
| HEC Errors: | 0 | 0 | 0 | 0 |
| OCD Errors: | 0 | 0 | 0 | 0 |
| LCD Errors: | 0 | 0 | 0 | 0 |
| Total Cells: | 1845038 | 0 | 0 | 0 |
| Data Cells: | 0 | 0 | 0 | 0 |
| Bit Errors: | 0 | 0 | 0 | 0 |
| Total ES: | 0 | 0 | | |
| Total SES: | 0 | 0 | | |
| Total UAS: | 583 | 583 | | |

xDSL BER Test Reset Statistics Draw Graph

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

| Field | Description |
|------------------------|--|
| Mode | G.Dmt, G.lite, T1.413, ADSL2, ADSL2+ |
| Traffic Type | Channel type Interleave or Fast |
| Status | Lists the status of the DSL link |
| Link Power State | Link output power state |
| Line Coding (Trellis) | Trellis On/Off |
| SNR Margin (0.1 dB) | Signal to Noise Ratio (SNR) margin |
| Attenuation (0.1 dB) | Estimate of average loop attenuation in the downstream direction |
| Output Power (0.1 dBm) | Total upstream output power |
| Attainable Rate (Kbps) | The sync rate you would obtain |

| Field | Description |
|-------------|--|
| Rate (Kbps) | Current sync rates downstream/upstream |

In VDSL mode, the following section is inserted.

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

In ADSL2+ mode, the following section is inserted.

| | |
|-------|---|
| MSGc | Number of bytes in overhead channel message |
| B | Number of bytes in Mux Data Frame |
| M | Number of Mux Data Frames in FEC Data Frame |
| T | Mux Data Frames over sync bytes |
| R | Number of check bytes in FEC Data Frame |
| S | Ratio of FEC over PMD Data Frame length |
| L | Number of bits in PMD Data Frame |
| D | The interleaver depth |
| Delay | The delay in milliseconds (msec) |
| INP | DMT symbol |

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

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

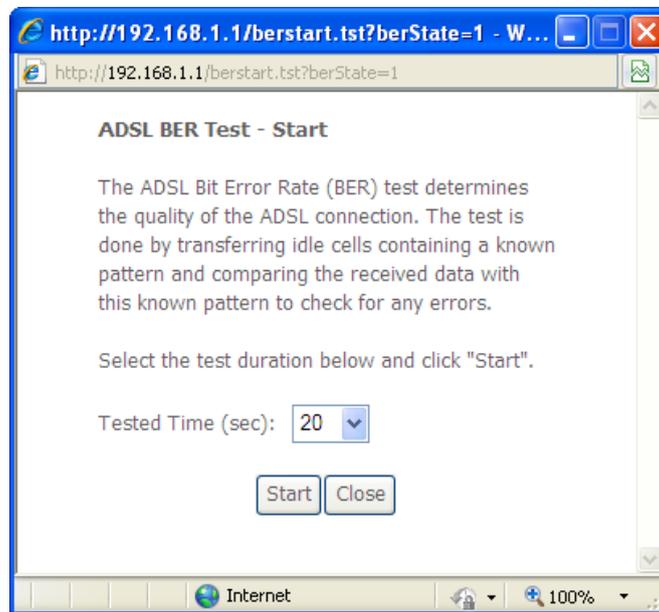
| | |
|-------------------------|--|
| Super Frames | Total number of super frames |
| Super Frame Errors | Number of super frames received with errors |
| RS Words | Total number of Reed-Solomon code errors |
| RS Correctable Errors | Total Number of RS with correctable errors |
| RS Uncorrectable Errors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

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

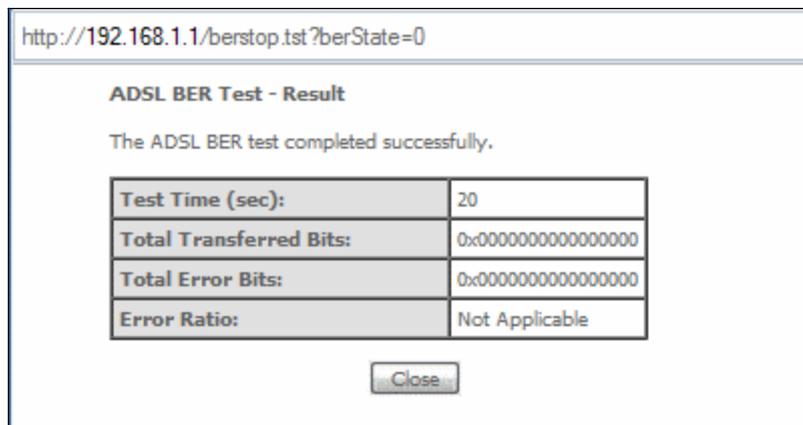
| | |
|-----------|--|
| Total ES | Total Number of Errored Seconds |
| Total SES | Total Number of Severely Errored Seconds |
| Total UAS | Total Number of Unavailable Seconds |

xDSL BER TEST

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

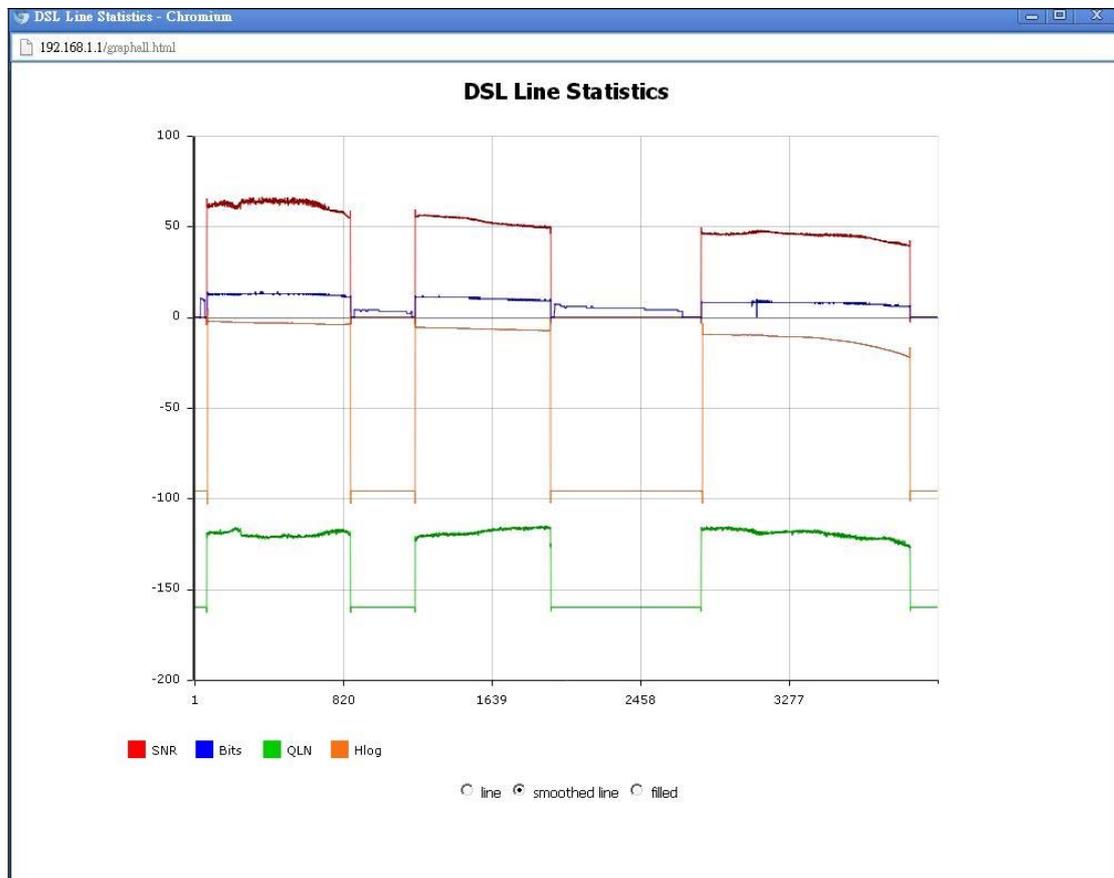


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



xDSL TONE GRAPH

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



4.3 Route

Choose **Route** to display the routes that the VR-3031u has found.

The screenshot shows the Comtrend VR-3031u web interface. The navigation menu includes: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area is titled 'Device Info -- Route'. It includes a legend for flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). Below the legend is a table with the following data:

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

On the left side of the interface, there is a sidebar menu with the following options: Summary, WAN, Statistics, Route (highlighted), ARP, DHCP, NAT Session, IGMP Proxy, and IPv6.

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

4.4 ARP

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

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area displays the ARP table under the heading "Device Info -- ARP". On the left side, there is a sidebar menu with options: Summary, WAN, Statistics, Route, ARP (highlighted), and DHCP.

| IP address | Flags | HW Address | Device |
|-------------|----------|-------------------|--------|
| 192.168.1.2 | Complete | 00:25:11:af:fd:f8 | br0 |

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

4.5 DHCP

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

The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area displays the DHCP Leases table under the heading "Device Info -- DHCP Leases". On the left side, there is a sidebar menu with options: Summary, WAN, Statistics, Route, ARP, DHCP (highlighted), DHCPv4, and DHCPv6.

| Hostname | MAC Address | IP Address | Expires In |
|---------------|-------------------|-------------|------------|
| trevorowens01 | 00:25:11:af:fd:f8 | 192.168.1.2 | 46 seconds |

| Field | Description |
|--------------|--|
| IPv6 Address | Shows IP address of device/host/PC |
| MAC Address | Shows the Ethernet MAC address of the device/host/PC |
| IP Address | Shows IP address of device/host/PC |
| Expires In | Shows how much time is left for each DHCP Lease |

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP
DHCPv4
DHCPv6

Device Info -- DHCPv6 Leases

| IPv6 Address | MAC Address | Duration | Expires In |
|--------------|-------------|----------|------------|
|--------------|-------------|----------|------------|

| Field | Description |
|--------------|--|
| IPv6 Address | Shows IP address of device/host/PC |
| MAC Address | Shows the Ethernet MAC address of the device/host/PC |
| Duration | Shows leased time in hours |
| Expires In | Shows how much time is left for each DHCP Lease |

4.6 NAT Session

Click the "Show All" button to display the following.

| Source IP | Source Port | Destination IP | Destination Port | Protocol | Timeout |
|-------------|-------------|----------------|------------------|----------|---------|
| 192.168.1.2 | 54927 | 192.168.1.1 | 53 | udp | 8 |
| 192.168.1.2 | 61978 | 192.168.1.1 | 53 | udp | 29 |
| 192.168.1.2 | 137 | 192.168.1.255 | 137 | udp | 16 |
| 192.168.1.2 | 58233 | 192.168.1.1 | 53 | udp | 23 |
| 192.168.1.2 | 68 | 192.168.1.1 | 67 | udp | 15 |
| 192.168.1.2 | 3700 | 192.168.1.1 | 80 | tcp | 4 |
| 192.168.1.2 | 3567 | 192.168.1.1 | 80 | tcp | 19 |
| 192.168.1.2 | 61516 | 192.168.1.1 | 53 | udp | 26 |
| 192.168.1.2 | 3699 | 192.168.1.1 | 80 | tcp | 4 |
| 192.168.1.2 | 55639 | 192.168.1.1 | 53 | udp | 8 |
| 192.168.1.2 | 3557 | 192.168.1.1 | 80 | tcp | 13 |

| Field | Description |
|------------------|--|
| Source IP | The source IP from which the NAT session is established |
| Source Port | The source port from which the NAT session is established |
| Destination IP | The IP which the NAT session was connected to |
| Destination Port | The port which the NAT session was connected to |
| Protocol | The Protocol used in establishing the particular NAT session |
| Timeout | The time remaining for the TCP/UDP connection to be active |

4.7 IGMP Proxy

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP
NAT Session
IGMP Proxy

List of IGMP Proxy Entries

| Interface | WAN | Groups | Member | Timeout |
|-----------|-----|--------|--------|---------|
|-----------|-----|--------|--------|---------|

| Field | Description |
|-----------|--|
| Interface | The Source interface from which the IGMP report was received |
| WAN | The WAN interface from which the multicast traffic is received |
| Groups | The destination IGMP group address |
| Member | The Source IP from which the IGMP report was received |
| Timeout | The time remaining before the IGMP report expires |

4.8 IPv6

4.8.1 IPv6 Info

The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left, a sidebar menu lists various system functions, with 'IPv6 Info' highlighted. The main content area is titled 'IPv6 WAN Connection Info' and contains a table with columns for Interface, Status, Address, and Prefix. Below this is a 'General Info' section with a table listing configuration details:

| IPv6 WAN Connection Info | | | |
|---------------------------|---------------------------|---------|--------|
| Interface | Status | Address | Prefix |
| General Info | | | |
| Device Link-local Address | fe80::200:ff:fe55:5555/64 | | |
| Default IPv6 Gateway | | | |
| IPv6 DNS Server | | | |

| Field | Description |
|---------------------------|--|
| Interface | WAN interface with IPv6 enabled |
| Status | Connection status of the WAN interface |
| Address | IPv6 Address of the WAN interface |
| Prefix | Prefix received/configured on the WAN interface |
| Device Link-local Address | The CPE's LAN Address |
| Default IPv6 Gateway | The default WAN IPv6 gateway |
| IPv6 DNS Server | The IPv6 DNS servers received from the WAN interface / configured manually |

4.8.2 IPv6 Neighbor

The screenshot shows the Comtrend web interface. At the top left is the Comtrend logo. To its right is a navigation bar with icons and labels: Device Info (line graph), Basic Setup (floppy disk), Advanced Setup (gears), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). Below the navigation bar is a sidebar menu with the following items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, IPv6 Info, **IPv6 Neighbor** (highlighted), and IPv6 Route. The main content area is titled "Device Info -- IPv6 Neighbor Discovery table" and contains a table with the following columns: IPv6 address, Flags, HW Address, and Device.

| Field | Description |
|--------------|--|
| IPv6 Address | Ipv6 address of the device(s) found |
| Flags | Status of the neighbor device |
| HW Address | MAC address of the neighbor device |
| Device | Interface from which the device is located |

4.8.3 IPv6 Route

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Summary
WAN
Statistics
Route
ARP
DHCP
NAT Session
IGMP Proxy
IPv6
IPv6 Info
IPv6 Neighbor
IPv6 Route

Device Info -- IPv6 Route

| Destination | Gateway | Metric | Interface |
|-------------|---------|--------|-----------|
|-------------|---------|--------|-----------|

| Field | Description |
|-------------|---|
| Destination | Destination IP Address |
| Gateway | Gateway address used for destination IP |
| Metric | Metric specified for gateway |
| Interface | Interface used for destination IP |

4.8.4 Network Map

The network map is a graphical representation of router's wan status and LAN devices. The feature is only available using a non-IE browser.



The screenshot displays the Comtrend network management interface. At the top left is the Comtrend logo. To its right is a navigation menu with icons and labels: Device Info (line graph), Basic Setup (floppy disk), Advanced Setup (gears), Diagnostics (stethoscope), Management (person), and Logout (door with person). Below the navigation menu is a sidebar with a list of menu items: Summary, WAN, Statistics, Route, ARP, DHCP, NAT Session, IGMP Proxy, IPv6, and Network Map (highlighted in blue). The main content area shows a network diagram. On the left, a globe icon is connected to a vertical line labeled 'WAN Cable', which is connected to a router icon. A horizontal line connects the router to a computer icon. To the right of the computer icon is a text box containing the IP address '192.168.1.33 (you)'.

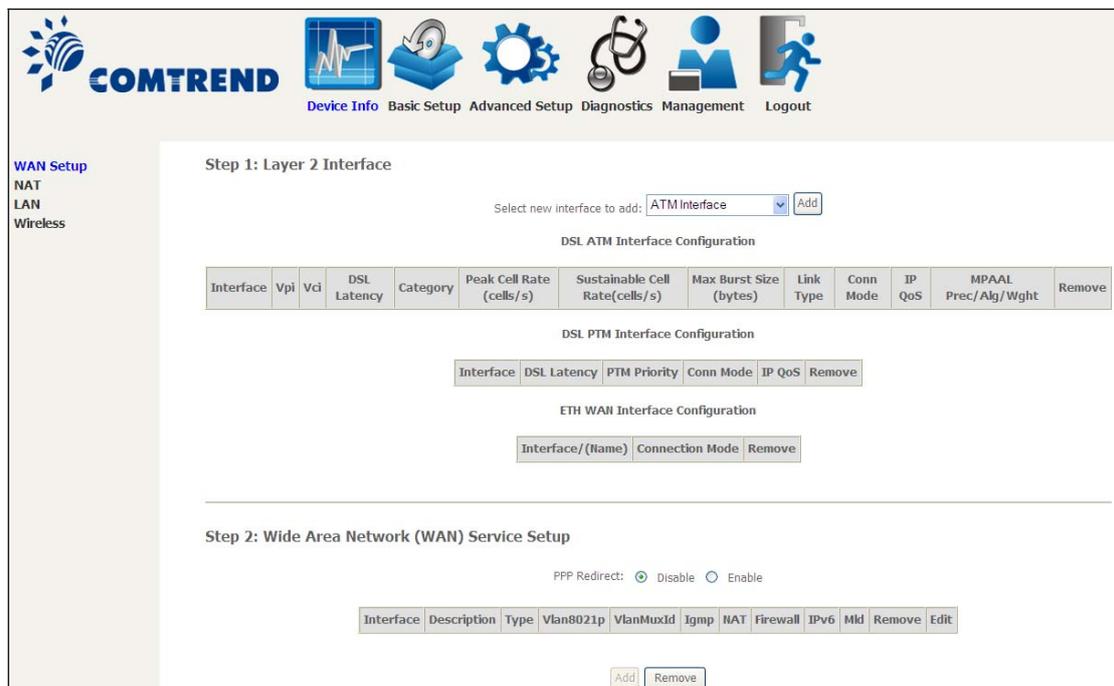
Chapter 5 Basic Setup

You can reach this page by clicking on the following icon located at the top of the screen.



5.1 Layer 2 Interface

Add or remove ATM, PTM and ETH WAN interface connections here.



The screenshot shows the COMTREND Basic Setup interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area is titled "Step 1: Layer 2 Interface". It features a dropdown menu to "Select new interface to add:" with "ATM Interface" selected and an "Add" button. Below this are three configuration sections: "DSL ATM Interface Configuration" with a table of columns (Interface, Vpl, Vci, DSL Latency, Category, Peak Cell Rate, Sustainable Cell Rate, Max Burst Size, Link Type, Conn Mode, IP QoS, MPAAL Prec/Alg/Wght, Remove), "DSL PTM Interface Configuration" with a table of columns (Interface, DSL Latency, PTM Priority, Conn Mode, IP QoS, Remove), and "ETH WAN Interface Configuration" with a table of columns (Interface/(Name), Connection Mode, Remove). Below these is "Step 2: Wide Area Network (WAN) Service Setup" with a "PPP Redirect:" option (Disable selected, Enable unselected) and a table of columns (Interface, Description, Type, Vlan8021p, VlanMuxId, Igmp, NAT, Firewall, IPv6, Mld, Remove, Edit). At the bottom of Step 2, there are "Add" and "Remove" buttons.

Click **Add** to create a new ATM interface (see [Appendix E - Connection Setup](#)).

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

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

5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.

Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect: Disable Enable

| Interface | Description | Type | Vlan8021p | VlanMuxId | Igmp | NAT | Firewall | IPv6 | Mld | Remove | Edit |
|--|-------------|------|-----------|-----------|------|-----|----------|------|-----|--------|------|
| <div style="display: flex; justify-content: center; gap: 20px;"> Add Remove </div> | | | | | | | | | | | |

Click the **Add** button to create a new connection. For connections on ATM or ETH WAN interfaces see [Appendix E - Connection Setup](#).

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

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

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

NOTE: ETH and ATM service connections cannot coexist. In Default Mode, up to 8 WAN connections can be configured; while VLAN Mux Connection Mode supports up to 16 WAN connections.

NOTE: Up to 16 PVC profiles can be configured and saved in flash memory. Also, ETH and PTM/ATM service connections cannot coexist.

5.2 NAT

To display this option, NAT must be enabled in at least one PVC. *NAT is not an available option in Bridge mode.*

5.2.1 Virtual Servers

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



COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

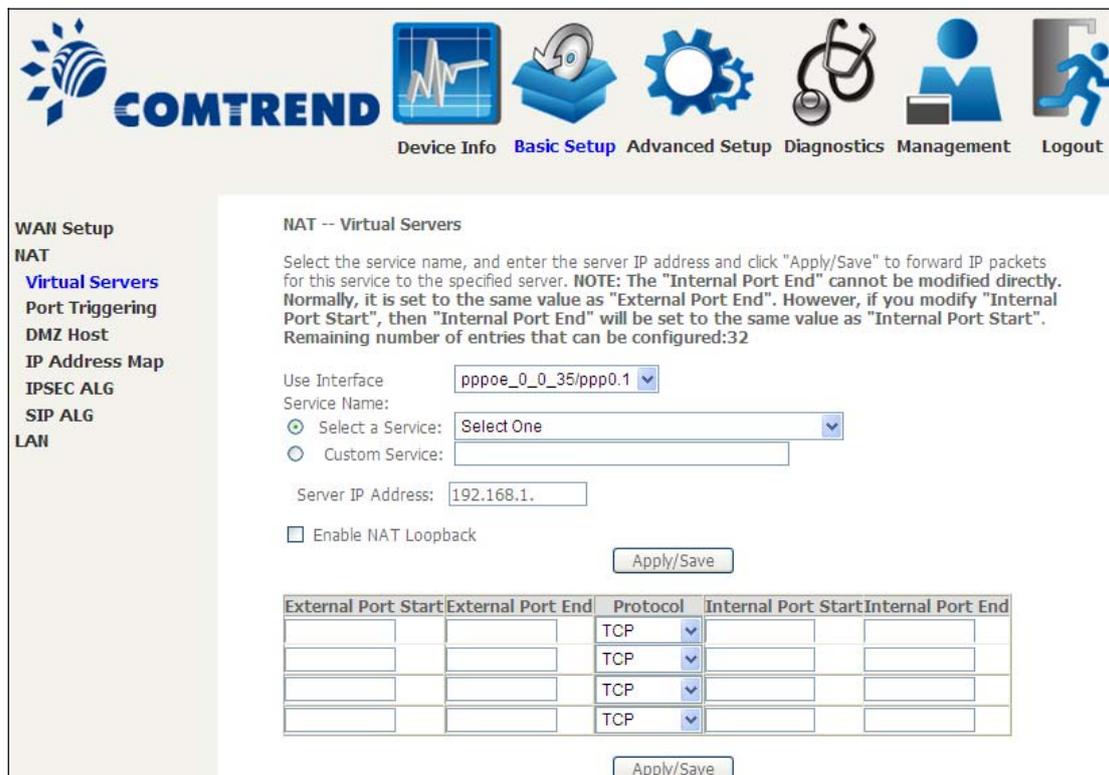
WAN Setup
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG
LAN

NAT -- Virtual Servers Setup

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

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

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



COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG
LAN

NAT -- Virtual Servers

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

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

Enable NAT Loopback

| External Port Start | External Port End | Protocol | Internal Port Start | Internal Port End |
|---------------------|-------------------|----------|---------------------|-------------------|
| | | TCP | | |

Consult the table below for field and header descriptions.

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

5.2.2 Port Triggering

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

The screenshot shows the Comtrend router's web interface. The navigation menu includes: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The main content area is titled "NAT -- Port Triggering Setup". It contains a description: "Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured." Below the description are "Add" and "Remove" buttons. A table is shown with the following structure:

| Application Name | Trigger | | Open | | | WAN Interface | Remove |
|------------------|----------|------------|----------|------------|-------|---------------|--------|
| | Protocol | Port Range | Protocol | Port Range | | | |
| | | Start | | End | Start | | |
| | | | | | | | |

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

Click Save/Apply to save and apply the settings.

Consult the table below for field and header descriptions.

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

5.2.3 DMZ Host

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



The screenshot shows the COMTREND router web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different functions: Device Info, Basic Setup (highlighted), Advanced Setup, Diagnostics, Management, and Logout. On the left side, there is a sidebar menu with the following items: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host (highlighted), IP Address Map, IPSEC ALG, SIP ALG, and LAN. The main content area is titled "NAT -- DMZ Host" and contains the following text: "The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer." Below this, there are two instructions: "Enter the computer's IP address and click 'Apply' to activate the DMZ host." and "Clear the IP address field and click 'Apply' to deactivate the DMZ host." There is a text input field labeled "DMZ Host IP Address:" and a checkbox labeled "Enable NAT Loopback". At the bottom right of the form, there is a "Save/Apply" button.

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

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

Enable NAT Loopback allows PC on the LAN side to access servers in the LAN network via the router's WAN IP.

5.2.4 IP Address Map

Mapping Local IP (LAN IP) to some specified Public IP (WAN IP).

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG
LAN

NAT -- IP Address Mapping Setup

| Rule | Type | Local Start IP | Local End IP | Public Start IP | Public End IP | Remove |
|--|------|----------------|--------------|-----------------|---------------|--------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> | | | | | | |

| Field/Header | Description |
|-----------------|------------------------------------|
| Rule | The number of the rule |
| Type | Mapping type from local to public. |
| Local Start IP | The beginning of the local IP |
| Local End IP | The ending of the local IP |
| Public Start IP | The beginning of the public IP |
| Public End IP | The ending of the public IP |
| Remove | Remove this rule |

Click the Add button to display the following.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

WAN Setup
NAT
Virtual Servers
Port Triggering
DMZ Host
IP Address Map
IPSEC ALG
SIP ALG
LAN

NAT -- IP Address Mapping Setup
Remaining number of entries that can be configured:32

Server Name:
 Select a Service: One to One

| Local Start IP | Local End IP | Public Start IP | Public End IP |
|----------------|--------------|-----------------|---------------|
| | 0.0.0.0 | | 0.0.0.0 |

Select a Service, then click the **Save/Apply** button.

One to One: mapping one local IP to a specific public IP

Many to one: mapping a range of local IP to a specific public IP

Many to many(Overload): mapping a range of local IP to a different range of public IP

Many to many(No Overload): mapping a range of local IP to a same range of public IP

5.2.5 IPSEC ALG

IPSEC ALG provides multiple VPN passthrough connection support, allowing different clients on LAN side to establish a secured IP Connection to the WAN server.



The screenshot displays the Comtrend web interface. At the top left is the Comtrend logo. To its right is a navigation bar with icons and labels: Device Info, Basic Setup (highlighted in blue), Advanced Setup, Diagnostics, Management, and Logout. On the left side of the main content area is a vertical menu with the following items: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG (highlighted in blue), and SIP ALG. The main content area is titled 'IPSEC ALG settings' and contains the following text: 'This page allows you to enable / disable IPSEC ALG.' followed by a note: 'NOTE: This configuration doesn't take effect until router is rebooted.' Below this is a checkbox labeled 'Enable IPSEC ALG.' which is checked. At the bottom right of the settings area is a 'Save' button.

To enable IPSEC ALG, tick the checkbox and click the **Save** button.

5.2.6 SIP ALG

This page allows you to enable / disable SIP ALG.



The screenshot displays the Comtrend web management interface. At the top left is the Comtrend logo. A navigation bar contains icons and labels for: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. On the left side, a vertical menu lists: WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, IPSEC ALG, SIP ALG (highlighted in blue), and LAN. The main content area is titled "SIP ALG settings" and contains the text: "This page allows you to enable / disable SIP ALG." followed by a bolded note: "NOTE: This configuration doesn't take effect until router is rebooted." Below this is a checked checkbox labeled "Enable SIP ALG." and a "Save" button.

5.3 LAN

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

The screenshot shows the Comtrend web interface for LAN configuration. The top navigation bar includes: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The sidebar menu on the left lists: WAN Setup, NAT, LAN (selected), IPv6 Autoconfig, Static IP Neighbor, and UPnP. The main content area is titled "Local Area Network (LAN) Setup" and contains the following configuration options:

- Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName:
- IP Address:
- Subnet Mask:
- IGMP Snooping mode:
 - Standard Mode
 - Blocking Mode
- Enable LAN side firewall
- Disable DHCP Server
- Enable DHCP Server
 - Start IP Address:
 - End IP Address:
 - Leased Time (hour):
- Setting TFTP Server
- Static IP Lease List: (A maximum 32 entries can be configured)

| MAC Address | IP Address | Remove | WOL |
|-------------|------------|--------|-----|
|-------------|------------|--------|-----|
- Configure the second IP Address and Subnet Mask for LAN interface
- Ethernet Media Type
 - Port 1:
 - Port 2:
 - Port 3:
 - Port 4:

Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

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

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

IGMP Snooping:

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

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

Enable LAN side firewall: Enable by ticking the checkbox .

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

Setting TFTP Server: Enable by ticking the checkbox . Then, input the TFTP server address or an IP address.

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

| MAC Address | IP Address | Remove | WOL |
|--|------------|---|-----|
| <input type="button" value="Add Entries"/> | | <input type="button" value="Remove Entries"/> | |

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

DHCP Static IP Lease

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

MAC Address:

IP Address:

Enable Wake On Lan.

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

| MAC Address | IP Address | Remove | WOL |
|--|--------------|---|---------|
| 12:34:56:78:90:12 | 192.168.1.33 | <input checked="" type="checkbox"/> | Disable |
| <input type="button" value="Add Entries"/> | | <input type="button" value="Remove Entries"/> | |

2ND LAN INTERFACE

To configure a secondary IP address, tick the checkbox outlined (in RED) below.

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | Configure the second IP Address and Subnet Mask for LAN interface |
| IP Address: | <input type="text"/> |
| Subnet Mask: | <input type="text"/> |

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

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

Ethernet Media Type:

Configure auto negotiation, or enforce selected speed and duplex mode for the Ethernet ports.

| | |
|--------------|---|
| Auto | ▼ |
| Auto | |
| 10Mbps-Half | |
| 10Mbps-Full | |
| 100Mbps-Half | |
| 100Mbps-Full | |

5.3.1 LAN IPv6 Autoconfig

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

The screenshot shows the COMTREND web interface for IPv6 LAN Auto Configuration. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists configuration options: WAN Setup, NAT, LAN, IPv6 Autoconfig (selected), Static IP Neighbor, and UPnP.

IPv6 LAN Auto Configuration
Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

LAN IPv6 Link-Local Address Configuration
 EUI-64
 User Setting
Interface Identifier:

Static LAN IPv6 Address Configuration
Interface Address (prefix length is required):

IPv6 LAN Applications
 Enable DHCPv6 Server
 Stateless
Refresh Time (sec):
 Stateful
Start interface ID:
End interface ID:
Leased Time (hour):
Static IP Lease List: (A maximum 32 entries can be configured)

| MAC Address | Interface ID | Remove |
|--|--------------|--------|
| <input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/> | | |

Enable SLAAC (RADVD)
RA interval Min(sec):
RA interval Max(sec):
Reachable Time(ms):
Default Preference:
 MTU (bytes):
 Enable Prefix Length Relay

Enable Configuration Mode

Enable ULA Prefix Advertisement
 Randomly Generate
 Statically Configure
Prefix:
Preferred Life Time (hour):
Valid Life Time (hour):

Enable MLD Snooping
 Standard Mode
 Blocking Mode

Consult the field descriptions below for more details.

LAN IPv6 Link-Local Address Configuration

| Heading | Description |
|--------------|---|
| EUI-64 | Use EUI-64 algorithm to calculate link-local address from MAC address |
| User Setting | Use the Interface Identifier field to define a link-local address |

Static LAN IPv6 Address Configuration

| Heading | Description |
|--|--|
| Interface Address (prefix length is required): | Configure static LAN IPv6 address and subnet prefix length |

IPv6 LAN Applications

| Heading | Description |
|---------------------|---|
| Stateless | Use stateless configuration |
| Refresh Time (sec): | The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6 |
| Stateful | Use stateful configuration |
| Start interface ID: | Start of interface ID to be assigned to dhcpv6 client |
| End interface ID: | End of interface ID to be assigned to dhcpv6 client |
| Leased Time (hour): | Lease time for dhcpv6 client to use the assigned IP address |

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

| MAC Address | IP Address | Remove |
|--|------------|---|
| <input type="button" value="Add Entries"/> | | <input type="button" value="Remove Entries"/> |

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

DHCP Static IP Lease

Enter the Mac address and Static Interface ID then click "Apply/Save" .

MAC Address:

Interface ID:

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

| MAC Address | Interface ID | Remove |
|-------------------|--------------|-------------------------------------|
| 00:11:22:33:44:55 | 0:0:0:2 | <input checked="" type="checkbox"/> |

| Heading | Description |
|---------------------------------|--|
| Enable RADVD | Enable use of router advertisement daemon |
| RA interval Min(sec): | Minimum time to send router advertisement |
| RA interval Max(sec): | Maximum time to send router advertisement |
| Reachable Time(ms): | The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation |
| Default Preference: | Preference level associated with the default router |
| MTU (bytes): | MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value |
| Enable Prefix Length Relay | Use prefix length receive from WAN interface |
| Enable Configuration Mode | Manually configure prefix, prefix length, preferred lifetime and valid lifetime used in router advertisement |
| Enable ULA Prefix Advertisement | Allow RADVD to advertise Unique Local Address Prefix |
| Randomly Generate | Use a Randomly Generated Prefix |
| Statically Configure Prefix | Specify the prefix to be used |
| Statically Configure | The prefix to be used |
| Preferred Life Time (hour) | The preferred life time for this prefix |
| Valid Life Time (hour) | The valid life time for this prefix |
| Enable MLD Snooping | Enable/disable IPv6 multicast forward to LAN ports |

5.3.2 Static IP Neighbor



Click the Add button to display the following.



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

| Heading | Description |
|----------------------|--|
| IP Version | The IP version used for the neighbor device |
| IP Address | Define the IP Address for the neighbor device |
| MAC Address | The MAC Address of the neighbor device |
| Associated Interface | The interface where the neighbor device is located |

5.3.3 UPnP

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



The screenshot displays the Comtrend web interface. At the top left is the Comtrend logo. To its right is a navigation bar with icons and labels: Device Info (line graph), Basic Setup (floppy disk), Advanced Setup (gears), Diagnostics (stethoscope), Management (person with laptop), and Logout (person running). Below the navigation bar is a sidebar menu with the following items: WAN Setup, NAT, LAN, IPv6 Autoconfig, Static IP Neighbor, and UPnP (highlighted in blue). The main content area is titled 'UPnP Configuration' and contains a note: 'NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.' Below the note is a checkbox labeled 'Enable UPnP' which is checked. At the bottom right of the main content area is an 'Apply/Save' button.

5.4 Wireless

5.4.1 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 **Apply/Save** 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. |

| Option | Description |
|--|--|
| 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 <input checked="" type="checkbox"/> to enable this function. |
| Enable WiFi Button | Select the checkbox <input checked="" type="checkbox"/> to enable the WiFi button. |
| 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> |

5.4.2 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 Comtrend web interface for configuring wireless security. At the top, there is a navigation bar with icons and labels for 'Device Info', 'Basic Setup', 'Advanced Setup', 'Diagnostics', 'Management', and 'Logout'. The 'Management' icon is highlighted. On the left side, there is a sidebar menu with options: 'WAN Setup', 'NAT', 'LAN', 'Wireless', 'Basic', and 'Security'. The 'Security' option is selected and highlighted in blue. The main content area is titled 'Wireless -- Security' and contains the following text: 'This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protected Setup(WPS) Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled'. Below this, there is a 'WPS Setup' section with a label 'Enable WPS' and a dropdown menu set to 'Disabled'. The 'Manual Setup AP' section follows, with instructions: '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.' The configuration fields are: 'Select SSID:' with a dropdown menu set to 'Comtrend_FF38'; 'Network Authentication:' with a dropdown menu set to 'WPA2-PSK'; 'WPA/WAPI passphrase:' with a text input field containing dots and a link 'Click here to display'; 'WPA Group Rekey Interval:' with a text input field containing '3600'; 'WPA/WAPI Encryption:' with a dropdown menu set to 'TKIP+AES'; and 'WEP Encryption:' with a dropdown menu set to 'Disabled'. At the bottom of the form is an 'Apply/Save' button.

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

WIRELESS SECURITY

Setup 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: | 3600 |
| RADIUS Server IP Address: | 0.0.0.0 |
| RADIUS Port: | 1812 |
| RADIUS Key: | |
| WPA/WAPI Encryption: | TKIP+AES |
| WEP Encryption: | Disabled |

Apply/Save

The settings for WPA-PSK authentication are shown next.

| | | |
|---|----------------|---------------------------------------|
| Network Authentication: | WPA-PSK | <input type="button" value="v"/> |
| WPA/WAPI passphrase: | ●●●●●●●●●●●●●● | Click here to display |
| WPA Group Rekey Interval: | 3600 | |
| WPA/WAPI Encryption: | TKIP+AES | <input type="button" value="v"/> |
| WEP Encryption: | Disabled | <input type="button" value="v"/> |
| <input type="button" value="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.

Please see [Section 6.14](#) for MAC Filter, Wireless Bridge and Advanced Wireless features.

Chapter 6 Advanced Setup

You can reach this page by clicking on the following icon located at the top of the screen.



6.1 Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications.

The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several menu items: Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout. Below the navigation bar, on the left, is a sidebar menu with various configuration options: Auto-Detection (highlighted), Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. The main content area is titled "Auto-detection setup" and contains the following text: "The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function." Below this text is a checkbox labeled "Enable auto-detect" which is currently unchecked. At the bottom of the main content area, there are two buttons: "Apply/Save" and "Restart".

The Auto Detection page simply provides a checkbox allowing users to enable or disable the feature. Check the checkbox to display the following configuration options.

Auto-Detection
 Security
 Parental Control
 Quality of Service
 Routing
 DNS
 DSL
 Home Networking
 Interface Grouping
 IP Tunnel
 Certificate
 Power Management
 Multicast
 Wireless

Auto-detection setup

The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interface. The feature is designed for the scenario that requires only **one WAN service** in different applications. Users shall enter given PPP username/password and pre-configure service list for auto-detection. After that, clicking "Apply/Save" will activate the auto-detect function.

Enable auto-detect

Auto-detection status: Waiting for DSL or Ethernet line connect

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Select a LAN-as-WAN Ethernet port for auto-detect:

Auto-detect service list: Auto-detect will detect the pre-configured services in the list in order. A maximum 7 entries can be configured.

Select Service:

| VPI[0-255] | VCI[32-65535] | Service | Option |
|--------------------------------|---------------------------------|---|--|
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Disable"/> | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Disable"/> | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Disable"/> | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Disable"/> | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Disable"/> | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Disable"/> | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Disable"/> | <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |
| <input type="text" value="0"/> | <input type="text" value="32"/> | <input type="text" value="Default Bridge"/> | |

In the boxes below, enter the PPP user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Enter the PPP username/password given by your service provider for PPP service detection.

Select a LAN-as-WAN Ethernet port for auto-detect:

Select the Ethernet Port that will be used as ETHWAN during auto-detection.

Select Service

ATM

| VPI[0-255] | VCI[32-65535] | Service |
|------------|---------------|----------------|
| 0 | 32 | Disable |
| 0 | 32 | PPPoE |
| 0 | 32 | PPPoA |
| 0 | 32 | IPoE |
| 0 | 32 | Disable |
| 0 | 32 | Default Bridge |

WAN services list for ATM mode: A maximum of 7 WAN services with corresponding PVC are required to be configured for ADSL ATM mode. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of those services to meet their own requirement and also reduce the detection cycle.

Select Service

PTM/ETHWAN

| VLAN ID[0-4094] | Service |
|-----------------|----------------|
| -1 | Disable |
| -1 | Default Bridge |

WAN services list for PTM mode: A maximum of 7 WAN services with corresponding VLAN ID (-1 indicates no VLAN ID is required for the service) are required to be configured for ADSL/VDSL PTM mode and ETHWAN. The services will be detected in order. Users can modify the 7 pre-configured services and select **disable** to ignore any of the services to meet their own requirement and also reduce the detection cycle.



Click "Apply/Save" to activate the auto-detect function.

Options for each WAN service: These options are selectable for each WAN service. Users can pre-configure both WAN services and other provided settings to meet their deployed requirements.

| VPI[0-255] | VCI[32-65535] | Service | Option |
|------------|---------------|---------|--|
| 0 | 33 | PPPoE | <input checked="" type="checkbox"/> NAT <input checked="" type="checkbox"/> Firewall <input type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |

| VLAN ID[0-4094] | Service | Option |
|-----------------|---------|--|
| 8 | PPPoE | <input checked="" type="checkbox"/> NAT <input type="checkbox"/> Firewall <input checked="" type="checkbox"/> IGMP Proxy <input type="checkbox"/> IP extension |

Auto Detection status and Restart

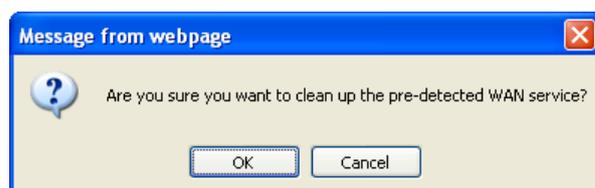
The Auto-detection status is used to display the real time status of the Auto-detection feature.



The **Restart** button is used to detect all the WAN services that are either detected by the auto-detection feature or configured manually by users.



The following window will pop up upon clicking the **Restart** button. Click the **OK** button to proceed.



Auto Detection notice

Note: The following description concerning ETHWAN is for multiple LAN port devices only.

- 1) This feature will automatically detect one WAN service only. If customers require multiple WAN services, manual configuration is required.
- 2) If a physical ETHWAN port is detected, the Auto Detection for ETHWAN will be fixed on the physical ETHWAN port and cannot be configured for any LAN port; if the physical ETHWAN port is not detected, the Auto Detection for ETHWAN will be configured to the 4th LAN port by default and allows it to be configured for any LAN port as well.
- 3) For cases in which both the DSL port and ETHWAN port are plugged in at the same time, the DSL WAN will have priority over ETHWAN. For example, the ETHWAN port is plugged in with a WAN service detected automatically and then the DSL port is plugged in and linked up. The Auto Detection feature will clear the WAN service for ETHWAN and re-detect the WAN service for DSL port.
- 4) If none of the pre-configured services are detected, a Bridge service will be created.

6.2 Security

To display this function, you must enable the firewall feature in WAN Setup. For detailed descriptions, with examples, please consult [Appendix A - Firewall](#).

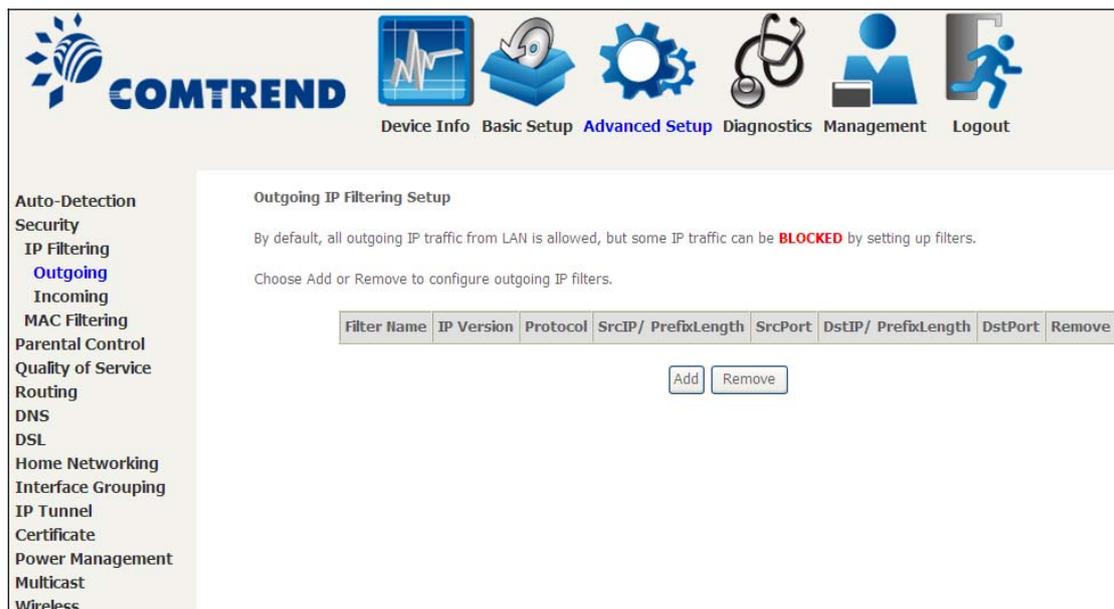
6.2.1 IP Filtering

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

NOTE: This function is not available when in bridge mode. Instead, [MAC Filtering](#) performs a similar function.

OUTGOING IP FILTER

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



The screenshot shows the Comtrend web interface for 'Outgoing IP Filtering Setup'. The top navigation bar includes icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar lists various settings categories, with 'IP Filtering' and 'Outgoing' selected. The main content area contains the following text:

Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

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

Below the table are 'Add' and 'Remove' buttons.

To add a filter (to block some outgoing IP traffic), click the **Add** button.

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

COMTREND Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
IP Filtering
Outgoing
 Incoming
 MAC Filtering
 Parental Control
 Quality of Service
 Routing
 DNS
 DSL
 Home Networking
 Interface Grouping
 IP Tunnel
 Certificate
 Power Management
 Multicast
 Wireless

Add IP Filter -- Outgoing

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

Filter Name:

IP Version: IPv4

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

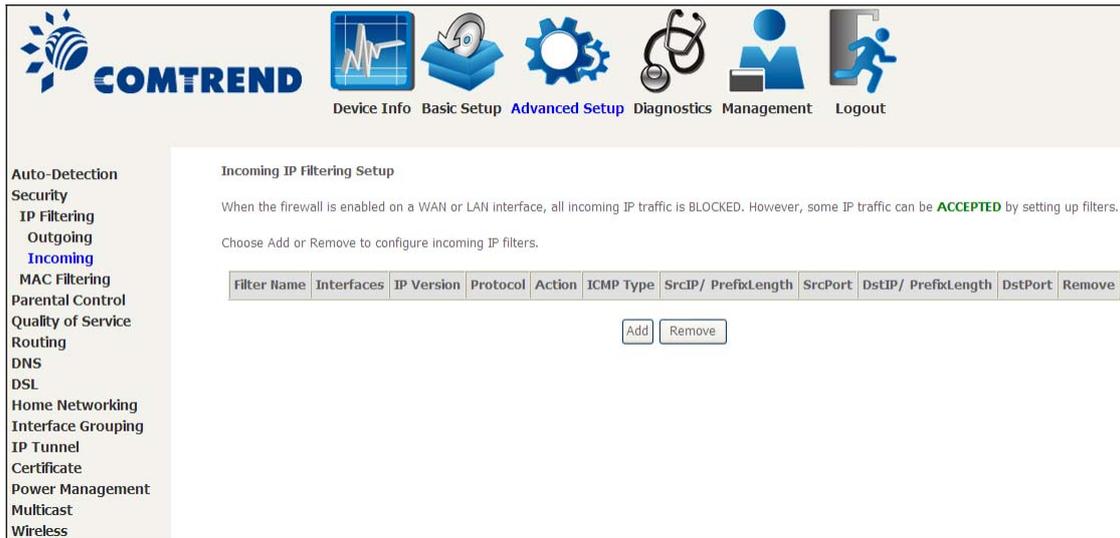
Destination Port (port or port:port):

Consult the table below for field descriptions.

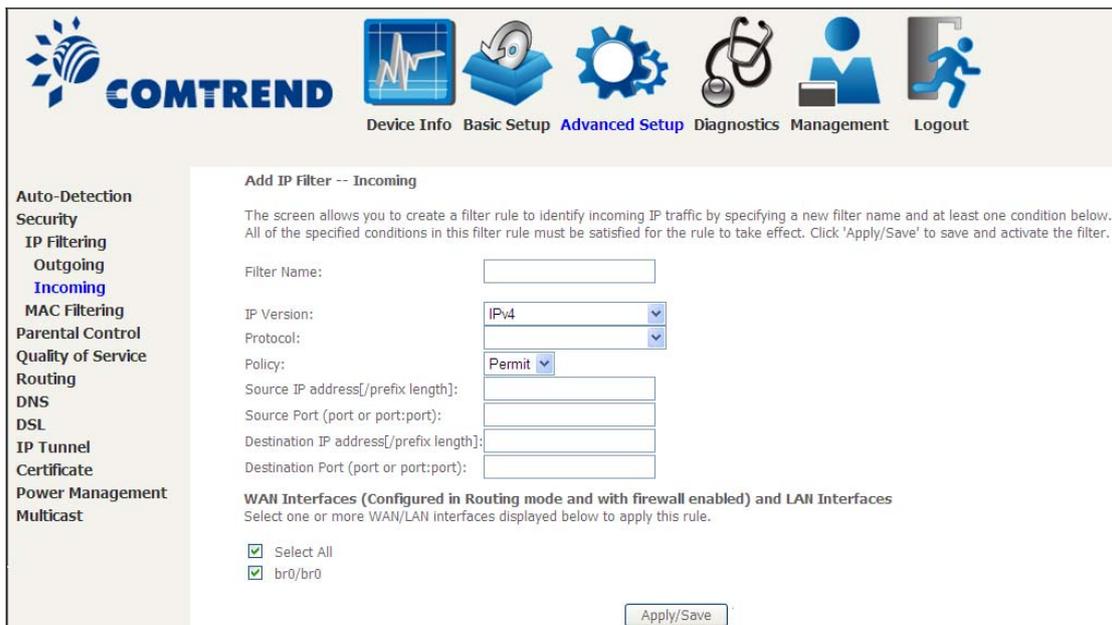
| Field | Description |
|--------------------------------------|---|
| Filter Name | The filter rule label |
| IP Version | Select from the drop down menu. |
| Protocol | TCP, TCP/UDP, UDP, or ICMP. |
| Source IP address | Enter source IP address. |
| Source Port (port or port:port) | Enter source port number or range. |
| Destination IP address | Enter destination IP address. |
| Destination Port (port or port:port) | Enter destination port number or range. |

INCOMING IP FILTER

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



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



Consult the table below for field descriptions.

| Field | Description |
|---------------------------------|---|
| Filter Name | The filter rule label. |
| IP Version | Select from the drop down menu. |
| Protocol | TCP, TCP/UDP, UDP, or ICMP. |
| Policy | Permit/Drop packets specified by the firewall rule. |
| Source IP address | Enter source IP address. |
| Source Port (port or port:port) | Enter source port number or range. |

| Field | Description |
|--------------------------------------|---|
| Destination IP address | Enter destination IP address. |
| Destination Port (port or port:port) | Enter destination port number or range. |

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

6.2.2 MAC Filtering

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

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the VR-3031u can be set according to the following procedure.

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

COMTREND Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
IP Filtering
MAC Filtering
Parental Control
Quality of Service
Routing
DSL
Home Networking
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

MAC Filtering Setup

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

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

| Interface | Policy | Change |
|-----------|----------------|--------------------------|
| atm0.1 | FORWARD | <input type="checkbox"/> |

Choose Add or Remove to configure MAC filtering rules.

| Interface | Protocol | Destination MAC | Source MAC | Frame Direction | Remove |
|-----------|----------|-----------------|------------|-----------------|--------|
|-----------|----------|-----------------|------------|-----------------|--------|

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

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

Consult the table below for detailed field descriptions.

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

6.3 Parental Control

This selection provides WAN access control functionality.

6.3.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.5 Internet Time, so that the scheduled times match your local time.

COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Time Restriction
Url Filter
Quality of Service
Routing
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

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

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

Add Remove

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

COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Time Restriction
Url Filter
Quality of Service
Routing
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

Access Time Restriction

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

User Name

Browser's MAC Address

Other MAC Address

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

Days of the week Mon Tue Wed Thu Fri Sat Sun

Click to select

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Apply/Save

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

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

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

Other MAC Address: MAC address of another LAN device.

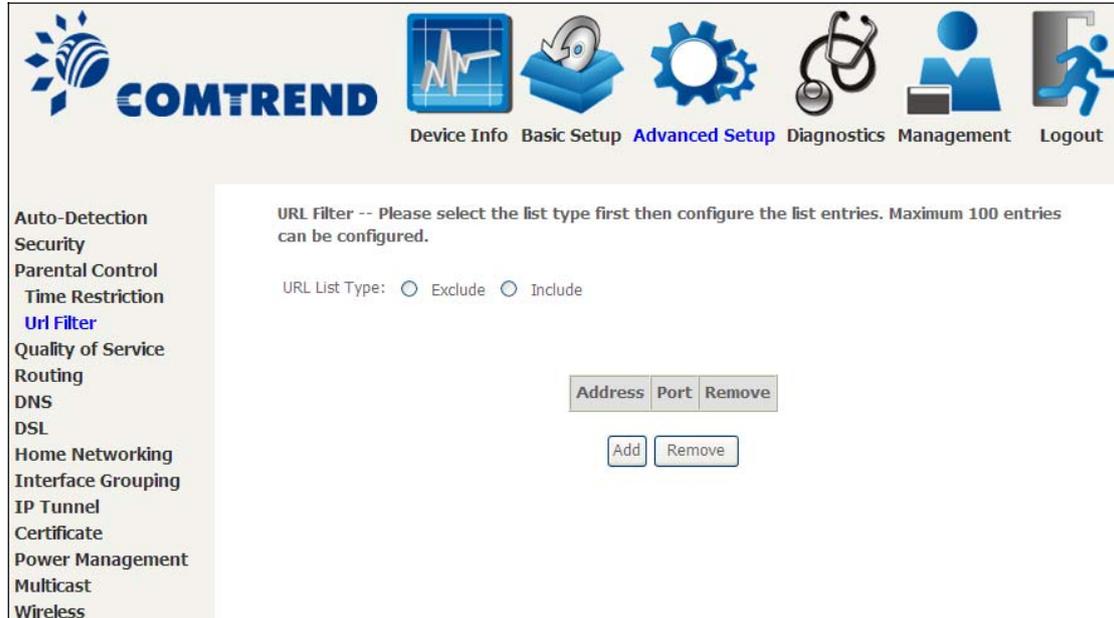
Days of the Week: The days the restrictions apply.

Start Blocking Time: The time the restrictions start.

End Blocking Time: The time the restrictions end.

6.3.2 URL Filter

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

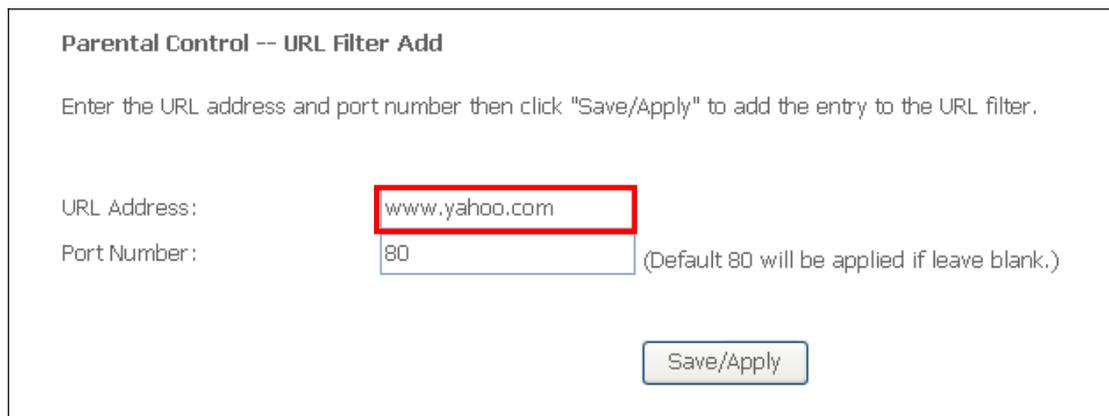


Select URL List Type: Exclude or Include.

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

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

Then click **Add** to display the following screen.



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

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

URL List Type: Exclude Include

| Address | Port | Remove |
|---------------|------|--------------------------|
| www.yahoo.com | 80 | <input type="checkbox"/> |

Add

Remove

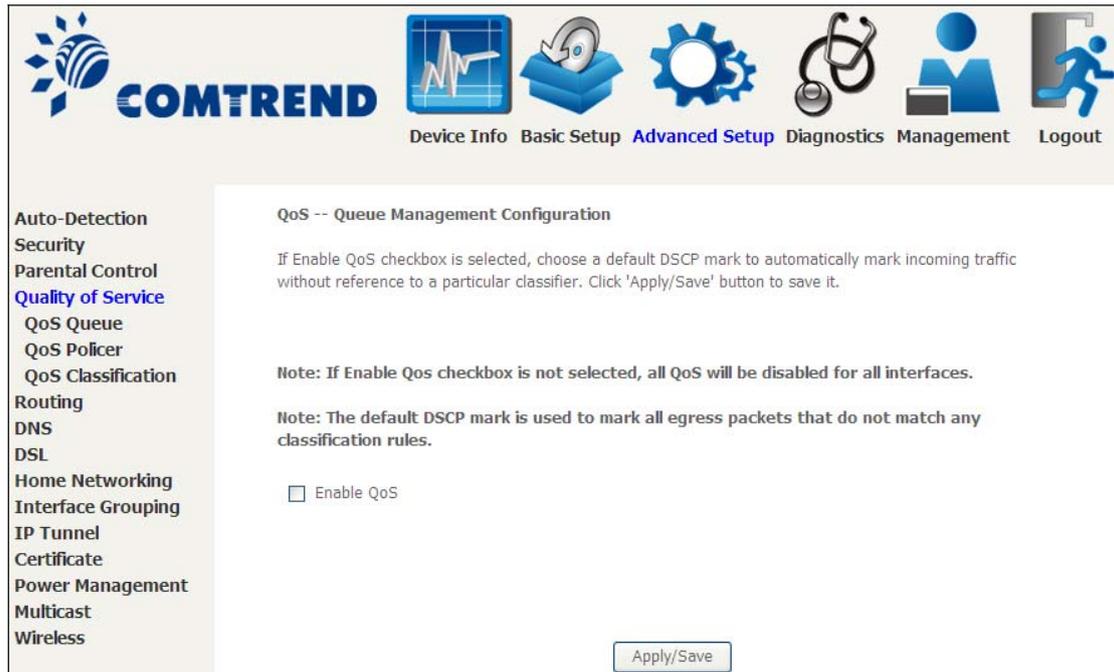
A maximum of 100 entries can be added to the URL Filter list.

6.4 Quality of Service (QoS)

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

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

Click Apply/Save to activate QoS.



The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with icons for Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. On the left, there is a sidebar menu with options like Auto-Detection, Security, Parental Control, **Quality of Service**, QoS Queue, QoS Policer, QoS Classification, Routing, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. The main content area is titled 'QoS -- Queue Management Configuration'. It contains the following text: 'If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.' Below this, there are two notes: 'Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.' and 'Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.' There is an unchecked checkbox labeled 'Enable QoS' and an 'Apply/Save' button at the bottom right.

QoS and DSCP Mark are defined as follows:

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

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

6.4.1 QoS Queue Setup

Configure queues with different priorities to be used for QoS setup.

In ATM mode, maximum 16 queues can be configured.

In PTM mode, maximum 8 queues can be configured.

For each Ethernet interface, maximum 3 queues can be configured.

QoS Queue Setup

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

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

| Name | Key | Interface | Qid | Prec/Alg/Wght | DSL Latency | PTM Priority | Shaping Rate (bits/s) | Burst Size (bytes) | Enable | Remove |
|--------------------|-----|-----------|-----|---------------|-------------|--------------|-----------------------|--------------------|---------|--------|
| WMM Voice Priority | 1 | w/0 | 1 | 1/SP | | | | | Enabled | |
| WMM Voice Priority | 2 | w/0 | 2 | 2/SP | | | | | Enabled | |
| WMM Video Priority | 3 | w/0 | 3 | 3/SP | | | | | Enabled | |
| WMM Video Priority | 4 | w/0 | 4 | 4/SP | | | | | Enabled | |
| WMM Best Effort | 5 | w/0 | 5 | 5/SP | | | | | Enabled | |
| WMM Background | 6 | w/0 | 6 | 6/SP | | | | | Enabled | |
| WMM Background | 7 | w/0 | 7 | 7/SP | | | | | Enabled | |
| WMM Best Effort | 8 | w/0 | 8 | 8/SP | | | | | Enabled | |

To add a queue, click the **Add** button.

To remove queues, check their remove-checkboxes (for user created queues), then click the **Remove** button.

The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effect. This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button. Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.

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

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
Home Networking
Interface Grouping

QoS Queue Configuration

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

Name:

Enable:

Interface:

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

Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

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

6.4.2 QoS Policer

To remove policers, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the policer after page reload.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel
Certificate

QoS Policer Setup -- maximum 32 policers can be configured.

To add a policer, click the **Add** button.
To remove policers, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every policers in the table. Policers with enable-checkbox checked will be enabled. Policers with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the policer after page reload.

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

| Name | Key | MeteringType | Committed Rate (kbps) | Committed BurstSize (bytes) | Excess BurstSize (bytes) | Peak Rate (kbps) | Peak BurstSize (bytes) | Conform Action | PartialConform Action | NonConform Action | Enable | Remove |
|--|-----|--------------|-----------------------|-----------------------------|--------------------------|------------------|------------------------|----------------|-----------------------|-------------------|--------|--------|
| <input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/> | | | | | | | | | | | | |

To add a policer, click the **Add** button.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
QoS Queue
QoS Policer
QoS Classification
Routing
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

QoS Policer Configuration

This screen allows you to configure a QoS policer.
Click 'Apply/Save' to save the policer.

Notes:
--For TwoRateThreeColor policer, Peak Rate shall be higher than Committed Rate.
--CBS and EBS shall be minimally larger than the size of the largest possible IP packet in the stream.
--PBS shall be minimally larger than CBS by the size of the largest possible IP packet in the stream.

Name:

Enable:

Meter Type:

Committed Rate (kbps):

Committed Burst Size (bytes):

Conforming Action:

Nonconforming Action:

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

| Field | Description |
|------------------------------|--|
| Name | Name of this policer rule |
| Enable | Enable/Disable this policer rule |
| Meter Type | Meter type used for this policer rule |
| Committed Rate (kbps) | Defines the rate allowed for committed packets |
| Committed Burst Size (bytes) | Maximum amount of packets that can be processed by this policer |
| Conforming Action | Defines action to be taken if packets match this policer |
| Nonconforming Action | Defines actions to be taken if packets do not match this policer |

6.4.3 QoS Classification

The network traffic classes are listed in the following table.

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.
 To remove rules, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

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

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

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

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

Add Network Traffic Class Rule

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

Traffic Class Name:

Rule Order: ▼

Rule Status: ▼

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

Class Interface: ▼

Ether Type: ▼

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

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

Specify Class Queue (Required): ▼
 - Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Specify Class Policer: ▼

Mark Differentiated Service Code Point (DSCP): ▼

Mark 802.1p priority: ▼
 - Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Click **Apply/Save** to save and activate the rule.

| Field | Description |
|--|--|
| Traffic Class Name | Enter a name for the traffic class. |
| Rule Order | Last is the only option. |
| Rule Status | Disable or enable the rule. |
| Classification Criteria | |
| Class Interface | Select an interface (i.e. Local, eth0-4, wl0) |
| Ether Type | Set the Ethernet type (e.g. IP, ARP, IPv6). |
| Source MAC Address | A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field. |
| Source MAC Mask | This is the mask used to decide how many bits are checked in Source MAC Address. |
| Destination MAC Address | A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask. |
| Destination MAC Mask | This is the mask used to decide how many bits are checked in Destination MAC Address. |
| Classification Results | |
| Specify Class Queue | Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface. |
| Specify Class Policer | Packets classified into a policer will be marked based on the conforming action of the policer |
| Mark Differentiated Service Code Point | The selected Code Point gives the corresponding priority to packets that satisfy the rule. |
| Mark 802.1p Priority | Select between 0-7. Lower values have higher priority. |
| Set Rate Limit | The data transmission rate limit in kbps. |

6.5 Routing

The following routing functions are accessed from this menu:

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

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

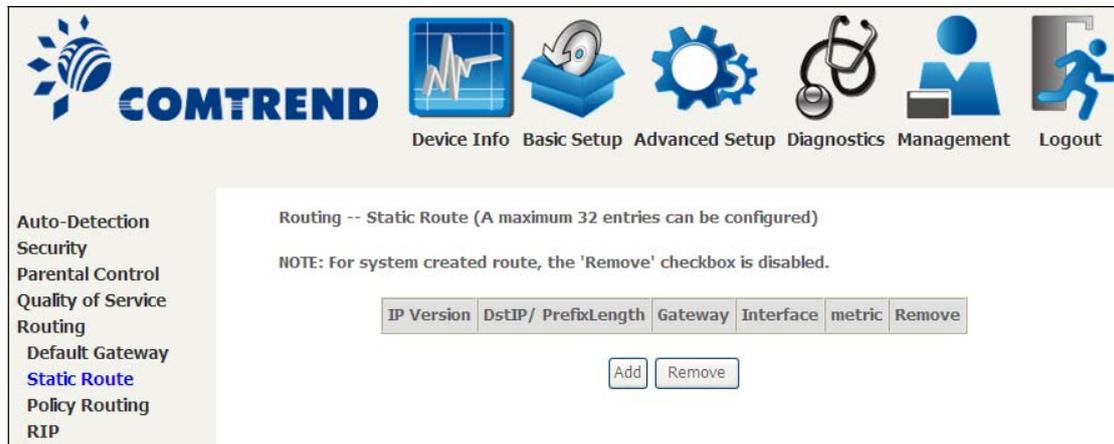
6.5.1 Default Gateway

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

The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with various options: Auto-Detection, Security, Parental Control, Quality of Service, Routing (highlighted), Default Gateway (highlighted), Static Route, Policy Routing, RIP, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. The main content area is titled "Routing -- Default Gateway" and contains the following text: "Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again." Below this text, there are two columns: "Selected Default Gateway Interfaces" and "Available Routed WAN Interfaces". Both columns are currently empty. Between the columns are two buttons: ">" and "<". Below the columns, there is a note: "TODO: IPV6 ***** Select a preferred wan interface as the system default IPv6 gateway." At the bottom, there is a dropdown menu labeled "Selected WAN Interface" with the value "NO CONFIGURED INTERFACE" and an "Apply/Save" button.

6.5.2 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.



COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP

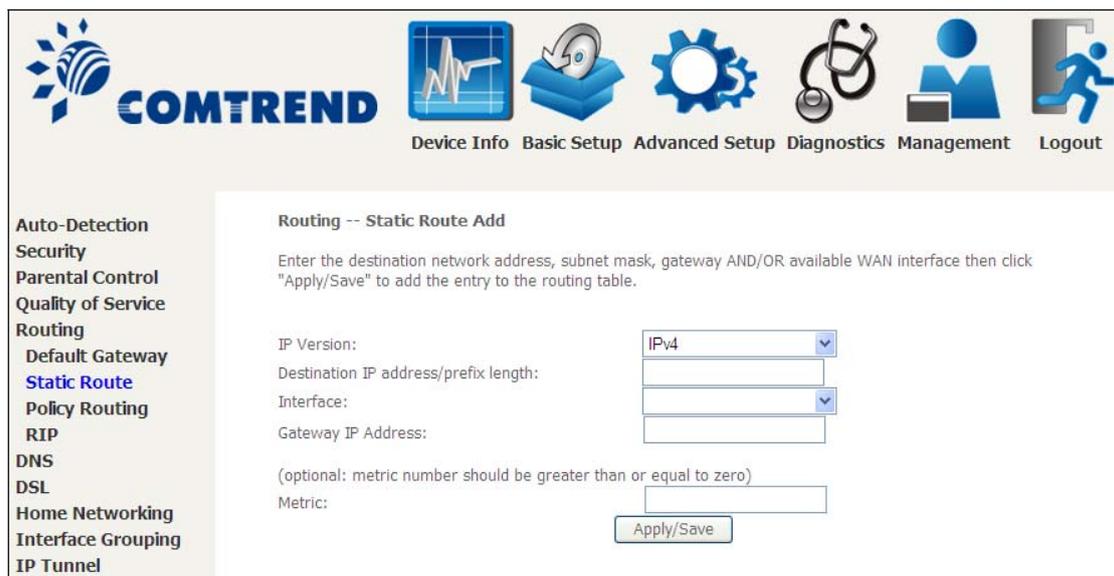
Routing -- Static Route (A maximum 32 entries can be configured)

NOTE: For system created route, the 'Remove' checkbox is disabled.

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

Add Remove

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



COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
Default Gateway
Static Route
Policy Routing
RIP
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel

Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

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

Metric:

Apply/Save

- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

After completing the settings, click **Apply/Save** to add the entry to the routing table.

6.5.3 Policy Routing

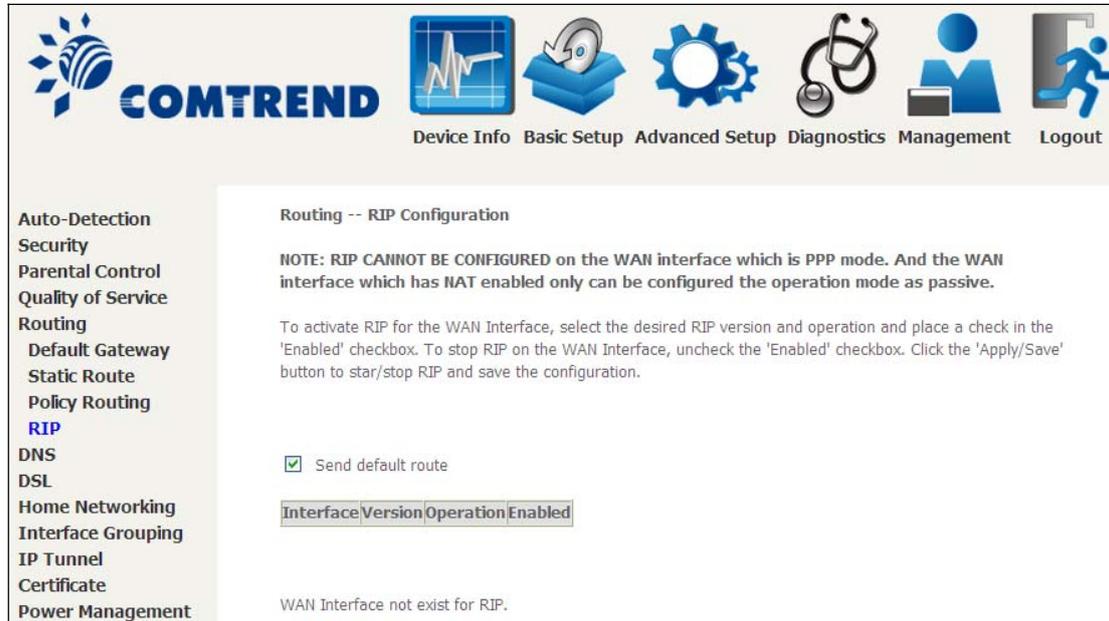
This option allows for the configuration of static routes by policy. Click **Add** to create a routing policy or **Remove** to delete one.

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

| Field | Description |
|--------------------|--|
| Policy Name | Name of the route policy |
| Physical LAN Port | Specify the port to use this route policy |
| Source IP | IP Address to be routed |
| Use Interface | Interface that traffic will be directed to |
| Default Gateway IP | IP Address of the default gateway |

6.5.4 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**.



The screenshot shows the Comtrend web interface for RIP configuration. At the top, there is a navigation bar with the Comtrend logo and several icons representing different sections: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a left sidebar with a list of menu items: Auto-Detection, Security, Parental Control, Quality of Service, Routing, Default Gateway, Static Route, Policy Routing, RIP (highlighted in blue), DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, and Power Management. The main content area is titled "Routing -- RIP Configuration" and contains a note: "NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive." Below the note, there is a paragraph explaining how to activate RIP for the WAN interface. A checkbox labeled "Send default route" is checked. Below this, there is a table with the following header: "Interface|Version|Operation|Enabled". The table is currently empty. At the bottom of the main content area, there is a message: "WAN Interface not exist for RIP."

6.6 DNS

6.6.1 DNS Server

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

The screenshot shows the Comtrend web interface for DNS Server Configuration. At the top, there is a navigation bar with icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. The left sidebar contains a menu with categories like Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. The main content area is titled "DNS Server Configuration" and contains the following text: "Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. **DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again." Below this text, there are two radio buttons: "Select DNS Server Interface from available WAN interfaces:" (which is currently unselected) and "Use the following Static DNS IP address:" (which is selected). The "Select DNS Server Interface" option includes two empty boxes labeled "Selected DNS Server Interfaces" and "Available WAN Interfaces" with arrows between them. The "Use the following Static DNS IP address" option includes two input fields for "Primary DNS server:" and "Secondary DNS server:". An "Apply/Save" button is located at the bottom right of the configuration area.

Click **Apply/Save** to save the new configuration.

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

6.6.2 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 VR-3031u to be more easily accessed from various locations on the Internet.

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DNS Entries
DNS Proxy/Relay
DSL

Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

| Hostname | Username | Service | Interface | DDNS Server | URL | Remove |
|----------|----------|---------|-----------|-------------|-----|--------|
| | | | | | | |

Add Remove

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

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DNS Entries
DNS Proxy/Relay
DSL
Home Networking
Interface Grouping
IP Tunnel
Certificate

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO. Additionally, it is possible to configure a Custom Dynamic DNS service.

D-DNS provider: DynDNS.org

Hostname:

Interface:

DynDNS Settings

Username:

Password:

Apply/Save

Click Apply/Save to save your settings.

Consult the table below for field descriptions.

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

6.6.3 DNS Entries

The DNS Entry page allows you to add domain names and IP address desired to be resolved by the DSL router.

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DNS Entries
DNS Proxy/Relay

DNS Entries

The DNS Entry page allows you to add domain names and IP address desired to be resolved by the DSL router. Choose Add or Remove to configure DNS Entry. The entries will become active after save/reboot.

A maximum 16 entries can be configured.

| Domain Name | IP Address | Remove |
|-------------|------------|--------|
|-------------|------------|--------|

Add Remove

Choose Add or Remove to configure DNS Entry. The entries will become active after save/reboot.

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DNS Entries
DNS Proxy/Relay

DNS Entry

Enter the domain name and IP address that needs to be resolved locally, and click 'Add Entry.'

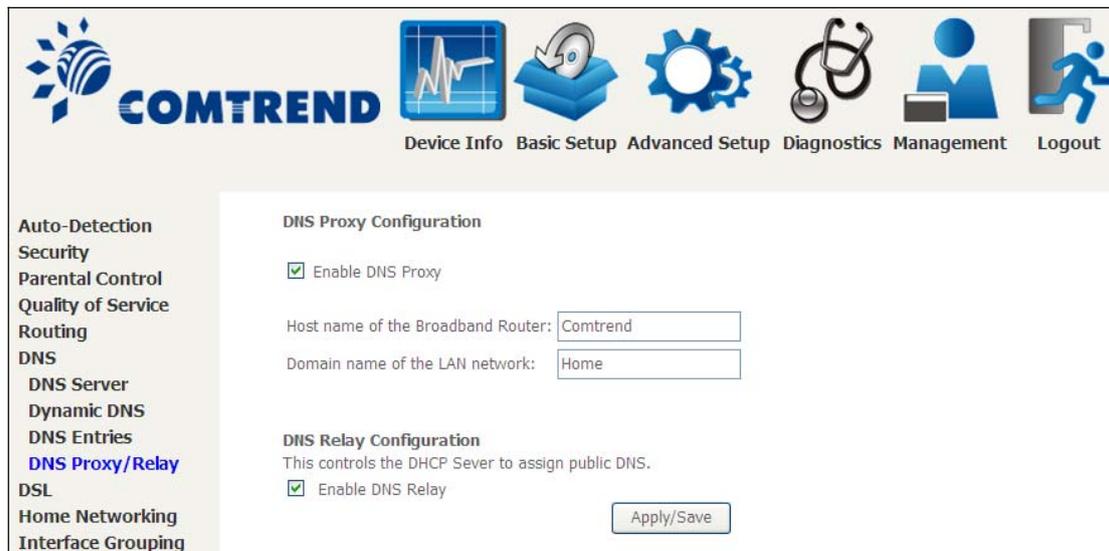
| Domain Name | IP Address |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |

Add Entry

Enter the domain name and IP address that needs to be resolved locally, and click the **Add Entry** button.

6.6.4 DNS Proxy/Relay

DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and the PC can access route with "Comtrend.Home".



The screenshot displays the Comtrend web management interface. At the top, the Comtrend logo is on the left, and navigation icons for Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout are on the right. A left sidebar lists various settings, with "DNS Proxy/Relay" highlighted in blue. The main content area is titled "DNS Proxy Configuration" and includes a checked checkbox for "Enable DNS Proxy". Below this are two text input fields: "Host name of the Broadband Router:" with the value "Comtrend" and "Domain name of the LAN network:" with the value "Home". A second section, "DNS Relay Configuration", includes a checked checkbox for "Enable DNS Relay" and a sub-note: "This controls the DHCP Sever to assign public DNS." An "Apply/Save" button is located at the bottom right of the configuration area.

6.7 DSL

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

| DSL 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 |

| DSL Mode | Data Transmission Rate - Mbps (Megabits per second) |
|--------------------------------|---|
| 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) |
| Select DSL LED behavior | Normal (TR-68 compliant): Select this option for DSL LED to operate normally (See menu 2.2 LED Indicator) Off:DSL LED will always be OFF |
| G997.1 EOC xTU-R Serial Number | Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages |

Advanced DSL Settings

Click **Advanced Settings** to reveal additional options.

The screenshot shows the Comtrend DSL Advanced Settings page. The navigation menu on the left includes: Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, **DSL**, Home Networking, Interface Grouping, IP Tunnel, Certificate, Power Management, Multicast, and Wireless. 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. An 'Apply' button is located at the bottom right of the settings area.

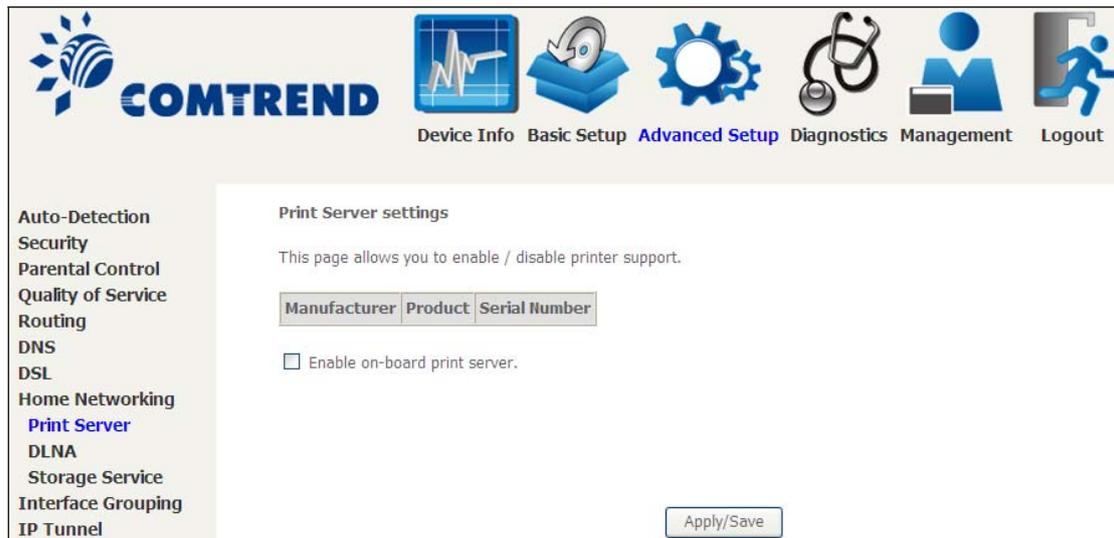
On this screen you select the required test mode, then click the **Apply** button.

| Field | Description |
|------------|---|
| Normal | DSL line signal is detected and sent normally |
| Reverb | DSL line signal is sent continuously in reverb mode |
| Medley | DSL line signal is sent continuously in medley mode |
| No Retrain | DSL line signal will always be on even when DSL line is unplugged |
| L3 | DSL line is set in L3 power mode |

6.8 Home Networking

6.8.1 Print Server

This page allows you to enable or disable printer support.



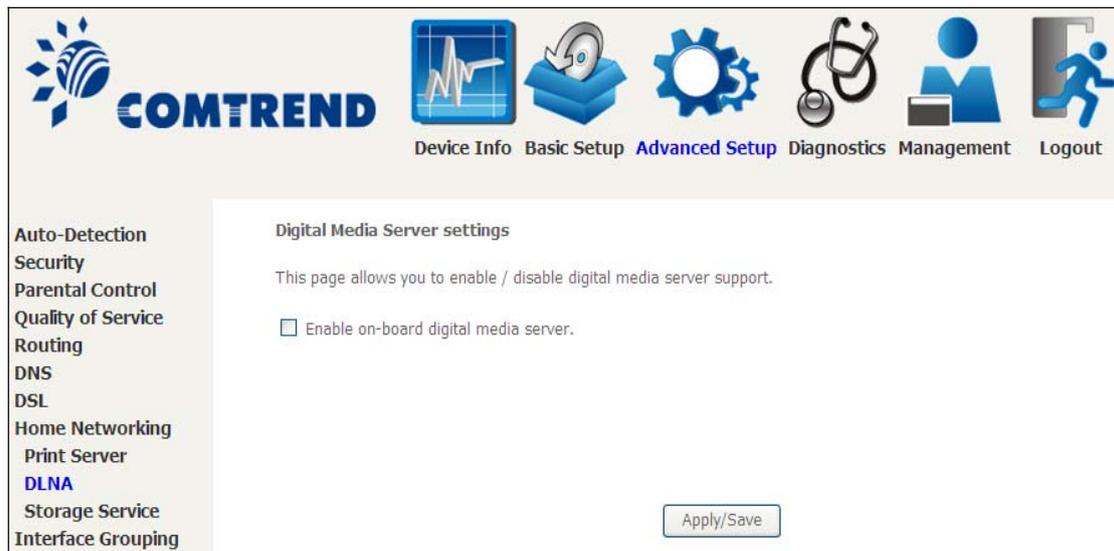
The screenshot displays the Comtrend web interface. At the top left is the Comtrend logo. To its right is a navigation bar with icons and labels: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, **Print Server** (highlighted), DLNA, Storage Service, Interface Grouping, and IP Tunnel. The main content area is titled "Print Server settings" and contains the text: "This page allows you to enable / disable printer support." Below this text are three input fields labeled "Manufacturer", "Product", and "Serial Number". A checkbox labeled "Enable on-board print server." is present and is currently unchecked. At the bottom right of the main content area is an "Apply/Save" button.

Please reference [Appendix G](#) to see the procedure for enabling the Printer Server.

6.8.2 DLNA

Enabling DLNA allows users to share digital media, like pictures, music and video, to other LAN devices from the digital media server.

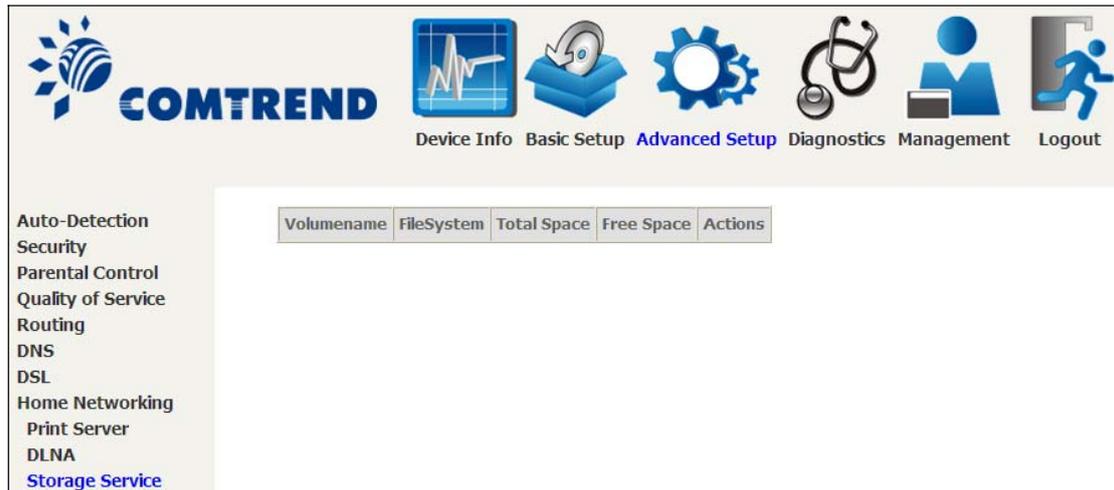
Insert USB drive to the USB host port on the back of router. Modify media library path to the corresponding path of the USB drive and click Apply/Save to enable the DLNA media server.



The screenshot displays the Comtrend router's web management interface. At the top, the Comtrend logo is on the left, and a navigation menu with icons is on the right, including Device Info, Basic Setup, **Advanced Setup**, Diagnostics, Management, and Logout. A left sidebar lists various settings categories, with **DLNA** highlighted in blue. The main content area is titled "Digital Media Server settings" and contains the text: "This page allows you to enable / disable digital media server support." Below this text is a single checkbox labeled "Enable on-board digital media server." which is currently unchecked. An "Apply/Save" button is located at the bottom right of the settings area.

6.8.3 Storage Service

This page displays storage devices attached to USB host.



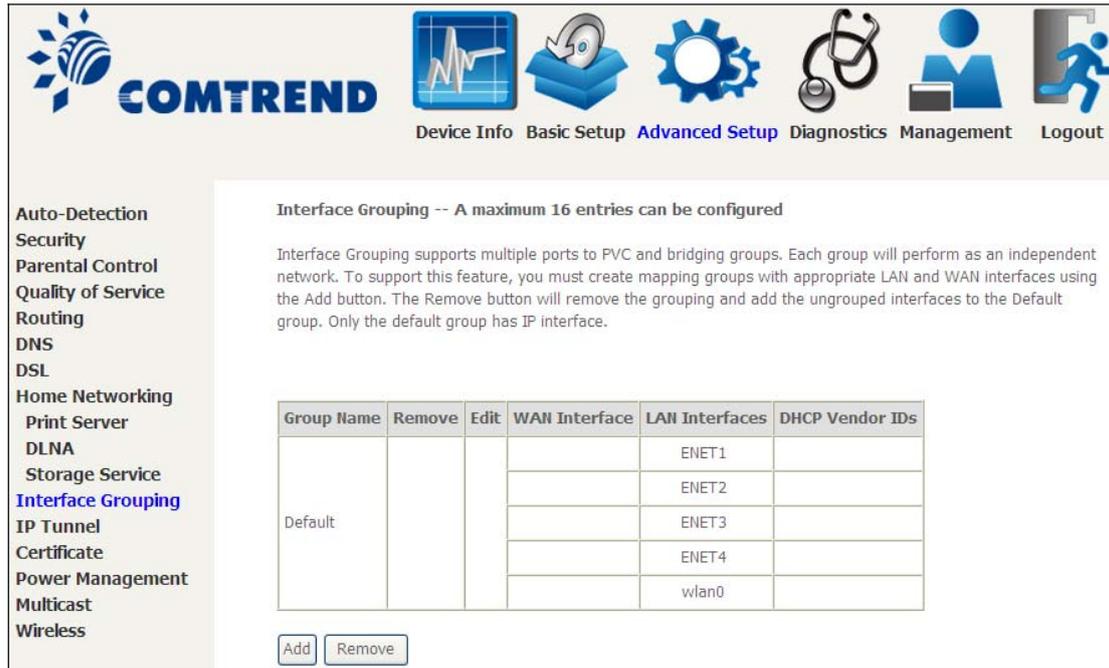
The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several menu items: Device Info, Basic Setup, **Advanced Setup** (highlighted in blue), Diagnostics, Management, and Logout. On the left side, there is a vertical menu with the following items: Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, Print Server, DLNA, and **Storage Service** (highlighted in blue). The main content area displays a table with the following columns: Volumename, FileSystem, Total Space, Free Space, and Actions.

Display after storage device attached (for your reference).

| Volumename | FileSystem | Total Space | Free Space | Actions |
|------------|------------|-------------|------------|--|
| usb1_1 | fat | 30517 MB | 19419 MB | <input type="button" value="Safely remove"/> |

6.9 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

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DSL
Home Networking
Print Server
DLNA
Storage Service
Interface Grouping
IP Tunnel
Certificate
Power Management
Multicast
Wireless

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 | Edit | WAN Interface | LAN Interfaces | DHCP Vendor IDs |
|------------|--------|------|---------------|----------------|-----------------|
| Default | | | | ENET1 | |
| | | | | ENET2 | |
| | | | | ENET3 | |
| | | | | ENET4 | |
| | | | | wlan0 | |

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

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Interface grouping Configuration

To create a new interface group:

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

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

Group Name:

Grouped WAN Interfaces Available WAN Interfaces

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.

6.10 IP Tunnel

6.10.1 IPv6inIPv4

Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.

COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel
IPv6inIPv4
IPv4inIPv6

IP Tunneling -- 6in4 Tunnel Configuration

| Name | WAN | LAN | Dynamic | IPv4 Mask Length | 6rd Prefix | Border Relay Address | Remove |
|--|-----|-----|---------|------------------|------------|----------------------|--------|
| <input type="button" value="Add"/> <input type="button" value="Remove"/> | | | | | | | |

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

COMTREND

Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel
IPv6inIPv4
IPv4inIPv6
Certificate
Power Management
Multicast

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism: 6RD

Associated WAN Interface:

Associated LAN Interface: LAN/br0

Manual Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

| Options | Description |
|--------------------------|---|
| Tunnel Name | Input a name for the tunnel |
| Mechanism | Mechanism used by the tunnel deployment |
| Associated WAN Interface | Select the WAN interface to be used by the tunnel |

| Options | Description |
|-------------------------------|--|
| Associated LAN Interface | Select the LAN interface to be included in the tunnel |
| Manual/Automatic | Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling |
| IPv4 Mask Length | The subnet mask length used for the IPv4 interface |
| 6rd Prefix with Prefix Length | Prefix and prefix length used for the IPv6 interface |
| Border Relay IPv4 Address | Input the IPv4 address of the other device |

6.10.2 IPv4inIPv6

Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.

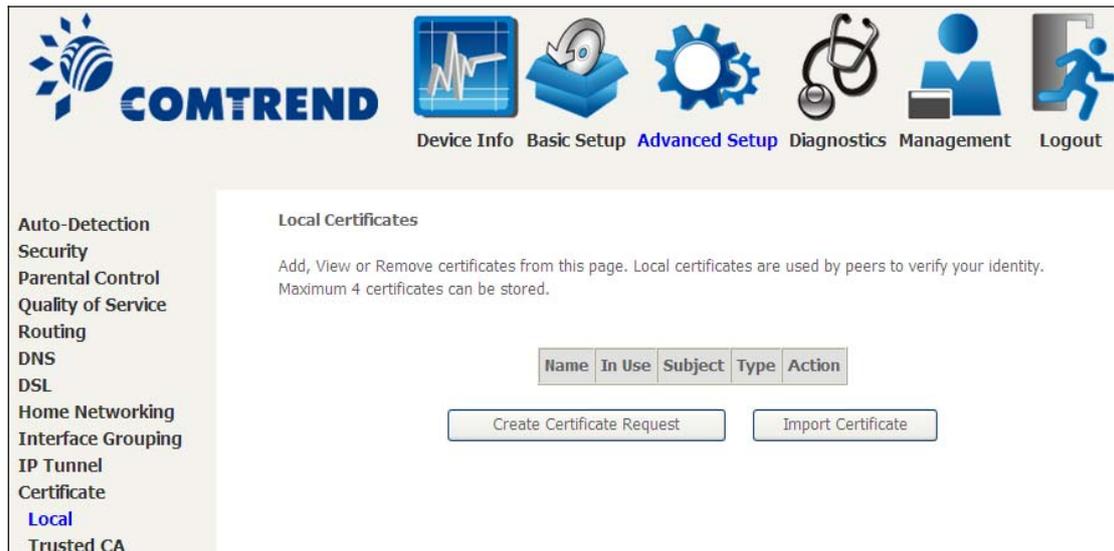
Click the **Add** button to display the following.

| Options | Description |
|--------------------------|--|
| Tunnel Name | Input a name for the tunnel |
| Mechanism | Mechanism used by the tunnel deployment |
| Associated WAN Interface | Select the WAN interface to be used by the tunnel |
| Associated LAN Interface | Select the LAN interface to be included in the tunnel |
| Manual/Automatic | Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling |
| AFTR | Address of Address Family Translation Router |

6.11 Certificate

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

6.11.1 Local

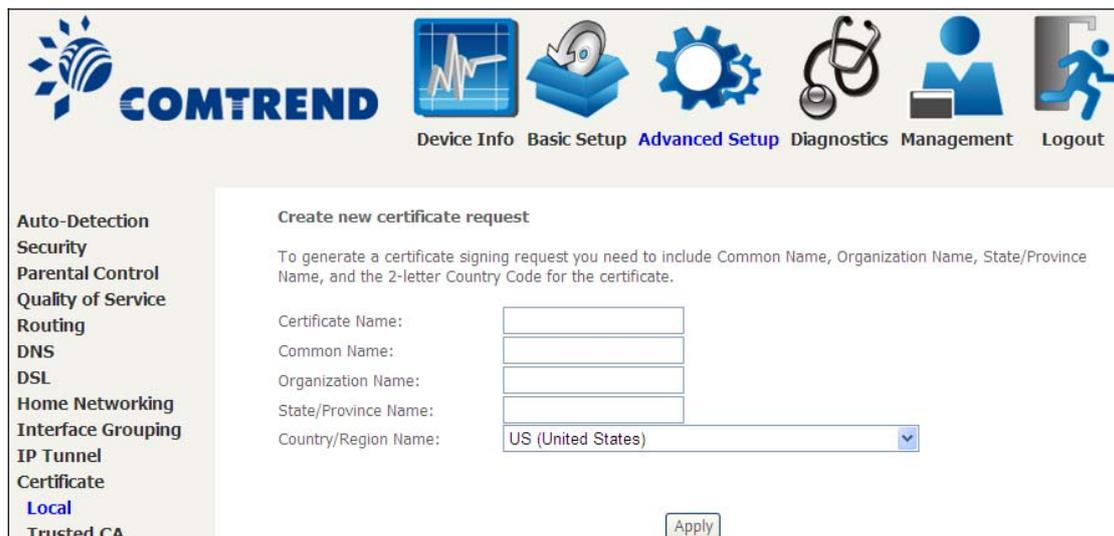


The screenshot shows the Comtrend web interface. At the top, there is a navigation bar with the Comtrend logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout. On the left side, there is a vertical menu with various settings categories: Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, Local (highlighted), and Trusted CA. The main content area is titled "Local Certificates" and contains the following text: "Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored." Below this text is a table with the following headers: Name, In Use, Subject, Type, and Action. Underneath the table are two buttons: "Create Certificate Request" and "Import Certificate".

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 screenshot shows the Comtrend web interface for creating a new certificate request. The navigation bar and left menu are the same as in the previous screenshot. The main content area is titled "Create new certificate request" and contains the following text: "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." Below this text are five input fields: Certificate Name, Common Name, Organization Name, State/Province Name, and Country/Region Name. The Country/Region Name field is a dropdown menu with "US (United States)" selected. At the bottom right of the form is an "Apply" button.

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.

COMTREND Device Info Basic Setup **Advanced Setup** Diagnostics Management Logout

Auto-Detection
Security
Parental Control
Quality of Service
Routing
DNS
DSL
Home Networking
Interface Grouping
IP Tunnel
Certificate
Local
Trusted CA
Power Management
Multicast
Wireless

Import certificate
Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

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

Private Key:

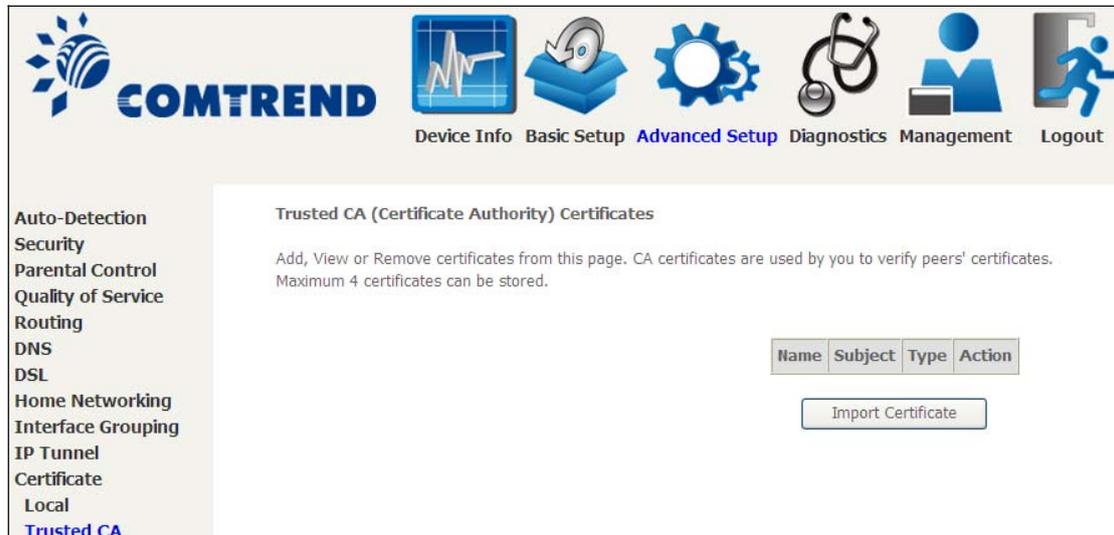
```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

Apply

Enter a certificate name and click the **Apply** button to import the certificate and its private key.

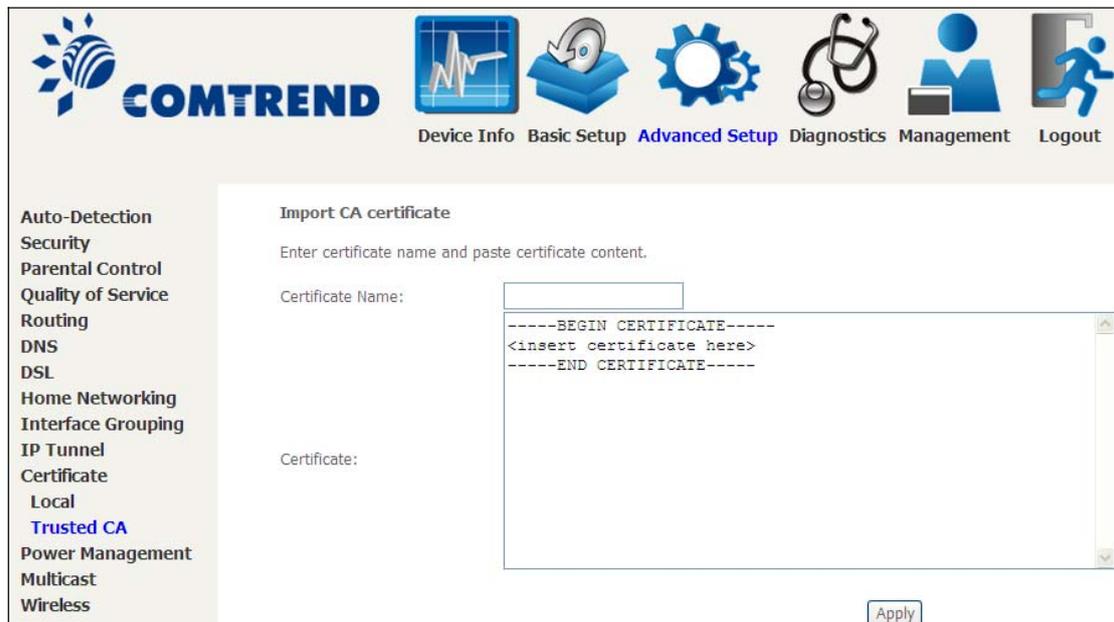
6.11.2 Trusted CA

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.



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout. On the left side, there is a vertical menu with various categories: Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, Local, and Trusted CA (highlighted). The main content area is titled "Trusted CA (Certificate Authority) Certificates". Below the title, there is a brief description: "Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored." Below this text, there is a table with columns for Name, Subject, Type, and Action. Below the table, there is a button labeled "Import Certificate".

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.



The screenshot shows the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup (highlighted), Diagnostics, Management, and Logout. On the left side, there is a vertical menu with various categories: Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, Local, Trusted CA (highlighted), Power Management, Multicast, and Wireless. The main content area is titled "Import CA certificate". Below the title, there is a brief description: "Enter certificate name and paste certificate content." Below this text, there is a form with two fields: "Certificate Name:" and "Certificate:". The "Certificate Name:" field is a text input box. The "Certificate:" field is a large text area with a placeholder text: "-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----". Below the form, there is a button labeled "Apply".

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

6.12 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 COMTREND web interface. At the top, there is a navigation bar with icons and labels for: Device Info, Basic Setup, **Advanced Setup** (highlighted), Diagnostics, Management, and Logout. The left sidebar contains a list of menu items: Auto-Detection, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Home Networking, Interface Grouping, IP Tunnel, Certificate, **Power Management** (highlighted), Multicast, and Wireless. The main content area is titled "Power Management" and contains the following text: "This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response." Below this text are three configuration sections: 1. "Wait instruction when Idle" with a checked checkbox for "Enable" and a status box showing "Enabled". 2. "Energy Efficient Ethernet" with an unchecked checkbox for "Enable" and a status box showing "Disabled". 3. "Ethernet Auto Power Down and Sleep" with a checked checkbox for "Enable" and a status box showing "Enabled". To the right of the third section, it displays "Number of ethernet interfaces: Powered up: 1" and "Powered down: 3". At the bottom right of the configuration area are "Apply" and "refresh" buttons.