

# VR-3046

## Home Gateway

### User Manual



**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](mailto: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.
- Never install telephone wiring during stormy weather conditions.

**CAUTION:**

- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.
- Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.
- Do not stack equipment or place equipment in tight spaces, in drawers, or on carpets. Be sure that your equipment is surrounded by at least 2 inches of air space.
- To prevent interference with cordless phones, ensure that the gateway is at least 5 feet ( 1.5m ) from the cordless phone base station.
- If you experience trouble with this equipment, disconnect it from the network until the problem has been corrected or until you are sure that equipment is not malfunctioning.

**WARNING**

- Disconnect the power line from the device before servicing
- For indoor use only
- Do NOT open the casing
- Do NOT use near water
- Do NOT insert sharp objects into the RJ-11 jack
- Keep away from the fire
- For use in ventilated environment / space
- Use 26 AWG or larger cable connect to RJ-11 port
  
- Débranchez l'alimentation électrique avant l'entretien
- Cet appareil est conçu pour l'usage intérieur seulement
- N'ouvrez pas le boîtier
- N'utilisez pas cet appareil près de l'eau
- N'insérez pas d'objets tranchants dans la prise RJ-11
- N'approchez pas du feu
- Veuillez utiliser dans un environnement aéré
- Veuillez utiliser fil électrique de 26AWG pour port RJ-11

Power Specifications ( Alimentation ) Input: 12Vdc, 1.0A 

**User Information**

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

**Note:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

This Class B digital apparatus complies with Canadian ICES-003.  
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.  
This device complies with Part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s).

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 Canada. Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s).

Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

## **ISED**

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

Le numéro REN (Ringer Equivalence Number) indique le nombre maximal de périphériques pouvant être connectés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque d'appareils, à la condition que la somme des REN de tous les appareils ne dépasse pas cinq.

## **Certification**

- FCC / IC standard
  - Part 15B / ICES-003
  - TIA-968 / IC-CS03
  - UL 62368-1 / CSA 62368-1

**Copyright**

Copyright©2022 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.

<b>NOTE:</b> This document is subject to change without notice.
---

**Open Source Software Notice**

Comtrend's products use open source software to fulfill their function.

Licenses for the open source software are granted under the GNU General Public License in various versions. For further information on the GNU General Public License see <http://www.gnu.org/licenses/>

You are allowed to modify all open source code (except for proprietary programs) and to conduct reverse engineering for the purpose of debugging such modifications; to the extent such programs are linked to libraries licensed under the GNU Lesser General Public License. You are not allowed to distribute information resulting from such reverse engineering or to distribute the modified proprietary programs.

The rights owners of the open source software require you to refer to the following disclaimer which shall apply with regard to those rights owners:

**Warranty Disclaimer**

THE OPEN SOURCE SOFTWARE IN THIS PRODUCT 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 APPLICABLE LICENSES FOR MORE DETAILS. Comtrend's products will strictly follow the market's standard requirements. It is not permitted to modify any Wi-Fi parameters, including the Wi-Fi power setting.

**Obtain Source Code**

If you wish to download the open source code please see:  
<https://www.comtrend.com/gplcddl.html>

If you do not see the required source code on our website link and wish to be provided with the entire source code for that product, we will provide it to you and any third party with the source code of the software licensed under an open source software license. Please send us a written request by email or mail to one of the following addresses:

**Email:** Comtrend support team - [opensource@comtrend.com](mailto:opensource@comtrend.com)

**Postal:** Comtrend Corporation  
3F-1, 10 Lane 609,  
Chongxin Rd., Section 5,  
Sancong Dist,  
New Taipei City 241405,  
Taiwan  
Tel: 886-2-2999-8261

In detail, name the product and firmware version for which you request the source code and indicate means to contact you and send you the source code.

PLEASE NOTE WE WILL CHARGE THE COSTS OF A DATA CARRIER AND THE POSTAL CHARGES TO SEND THE DATA CARRIER TO YOU. THE AMOUNT WILL VARY ACCORDING TO YOUR LOCATION AND THE COMTREND SUPPORT TEAM WILL NOTIFY THE EXACT COSTS WHEN REVIEWING THE REQUEST.

THIS OFFER IS VALID FOR THREE YEARS FROM THE MOMENT WE DISTRIBUTED THE PRODUCT. FOR MORE INFORMATION AND THE OPEN SOURCE LIST (& RESPECTIVE LICENCES) FOR INDIVIDUAL PRODUCTS PLEASE SEE:

<https://www.comtrend.com/gplcddl.html>

### **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

<b>CHAPTER 1 INTRODUCTION.....</b>	<b>8</b>
<b>CHAPTER 2 INSTALLATION.....</b>	<b>9</b>
2.1 HARDWARE SETUP.....	9
2.1.1 Back Panel.....	10
2.1.2 Front Panel.....	11
<b>CHAPTER 3 WEB USER INTERFACE.....</b>	<b>12</b>
3.1 DEFAULT SETTINGS .....	12
3.2 IP CONFIGURATION.....	13
3.3 LOGIN PROCEDURE.....	15
<b>CHAPTER 4 STATUS.....</b>	<b>17</b>
4.1 DEVICE.....	17
4.2 IPV6 .....	18
4.3 LAN PORT.....	19
<b>CHAPTER 5 LAN .....</b>	<b>20</b>
<b>CHAPTER 6 WAN.....</b>	<b>21</b>
6.1 WAN MODE .....	21
6.2 PTM WAN .....	22
6.3 ATM WAN .....	23
6.4 ATM SETTINGS.....	25
6.5 DSL SETTINGS.....	26
<b>CHAPTER 7 SERVICES.....</b>	<b>28</b>
7.1 DHCP.....	28
7.1.1 DHCP Server.....	28
7.1.2 DHCP Relay.....	31
7.2 VLAN ON LAN.....	32
7.3 DNS – DYNAMIC DNS .....	33
7.3.1 Dynamic DNS.....	33
7.4 FIREWALL .....	34
7.4.1 IP/Port Filtering .....	34
7.4.2 MAC Filtering .....	36
7.4.3 Port Forwarding.....	37
7.4.4 URL Blocking .....	39
7.4.5 Domain Blocking.....	40
7.4.6 Parental Control.....	41
7.4.7 DMZ.....	42
7.5 UPnP.....	43
7.6 RIP.....	44
<b>CHAPTER 8 ADVANCED.....</b>	<b>45</b>
8.1 ARP TABLE.....	45
8.2 BRIDGING .....	46
8.3 ROUTING .....	47
8.4 SNMP .....	48
8.5 IP QoS.....	50
8.5.1 QoS Policy.....	50
8.5.2 QoS Classification.....	52
8.6 OTHERS .....	55
8.7 IPV6 .....	56
8.7.1 IPv6 .....	56
8.7.2 RADVD.....	57
8.7.3 DHCPv6 .....	58
8.7.3.1 DHCPv6 – DHCP Server (Auto).....	59
8.7.3.2 DHCPv6 – NONE.....	59
8.7.3.3 DHCPv6 – DHCP Relay.....	60

8.7.3.4 DHCPv6 – DHCP Server (Manual) .....	61
8.7.4 MLD Proxy .....	63
8.7.5 MLD Snooping.....	64
8.7.6 IPv6 Routing.....	65
8.7.7 IP/Port Filtering .....	66
<b>CHAPTER 9 DIAGNOSTICS.....</b>	<b>68</b>
9.1 PING .....	68
9.2 ATM LOOPBACK.....	69
9.3 DSL TONE .....	70
9.4 ADSL CONNECTION .....	71
<b>CHAPTER 10 ADMIN.....</b>	<b>72</b>
10.1 COMMIT/REBOOT .....	72
10.2 BACKUP/RESTORE .....	73
10.3 SYSTEM LOG .....	74
10.4 PASSWORD.....	75
10.5 FIRMWARE UPGRADE.....	76
10.6 ACL .....	77
10.7 TIME ZONE .....	78
10.8 TR-069.....	80
<b>CHAPTER 11 STATISTICS .....</b>	<b>83</b>
11.1 INTERFACE.....	83
11.2 DSL.....	84
<b>APPENDIX A - PIN ASSIGNMENTS .....</b>	<b>87</b>
<b>APPENDIX B – SPECIFICATIONS .....</b>	<b>88</b>
<b>APPENDIX C - SSH CLIENT .....</b>	<b>89</b>
<b>APPENDIX D – WALL MOUNTING .....</b>	<b>90</b>



## Chapter 1 Introduction

VR-3046 is designed as multi-DSL Router provides wired access for high-bandwidth applications in the home or office. It includes one Giga Ethernet port and supports ADSL2/2+ and VDSL2 connections with automatic fallback to ADSL2+. The VR-3046 supports routed or bridged mode and up to profile 35b in VDSL2 mode for 100Mbps upstream and 300Mbps downstream high-speed bandwidth. On longer loops, VDSL2 35b falls back to VDSL2 17a vectoring performance. With the exclusion of wireless access, support and installation is simple and straightforward.

## Chapter 2 Installation

### 2.1 Hardware Setup



DO NOT STACK

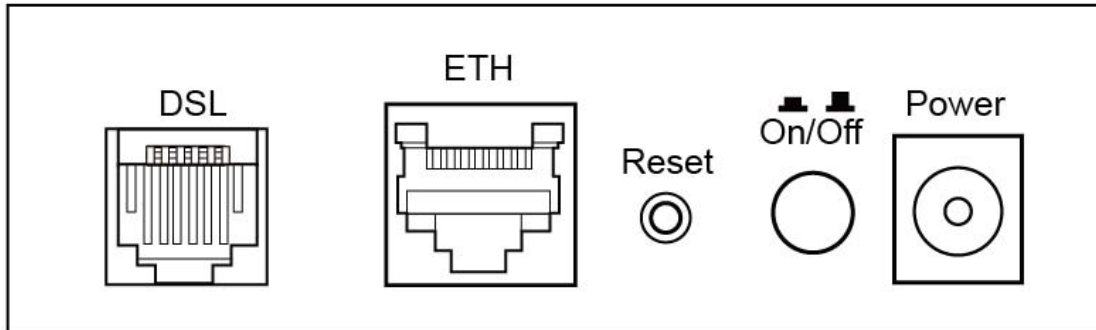
#### **Non-stackable**

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

Follow the instructions below to complete the hardware setup.

### 2.1.1 Back Panel

The figure below shows the back panel of the device.



#### DSL

Connect to the DSL port with the DSL RJ11 cable. The VR-3046 supports the following DSL profiles -

ADSL: ADSL, ADSL 2, ADSL 2+.

VDSL: 8a, 8b, 8c, 8d, 12a, 12b, 17a, 30a and 35b.

#### Ethernet (LAN) Port

You can connect the router to up to four LAN devices using RJ45 cables. The ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

#### 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 [2.1.2 Front Panel](#) for details).

**NOTE:** If pressed down for more than 60 seconds, the VR-3046 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.

#### Power ON

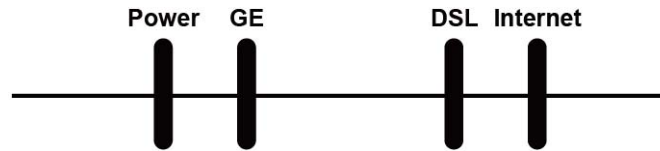
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section – LED Indicators).

**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.

## 2.1.2 Front Panel

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	Power On
		Off	Power Off
	RED	On	POST (Power On Self Test) failure (not bootable) or Device malfunction A malfunction is any error of internal sequence or state that will prevent the device from connecting to the OLT or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.
GE	GREEN	On	Giga Ethernet connected
		Off	Giga Ethernet not connected
		Blink	Giga Ethernet is transmitting/receiving
DSL	GREEN	On	xDSL Link is established.
		Off	xDSL Link is not established.
		Blink	xDSL Link is training
Internet	GREEN	On	IP connected and no traffic detected (the device has a WAN IP address from IPCP or DHCP is up or a static IP address is configured, PPP negotiation has successfully complete.
		Off	Modem power off, modem in bridged mode or WAN connection not present.
		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.)

### Note:

A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.

IP connected (the device has a WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured, PPP negotiation has successfully complete – if used – and DSL is up ) and no traffic detected. If the IP or PPPoE session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.

## 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**)
- 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-3046 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.

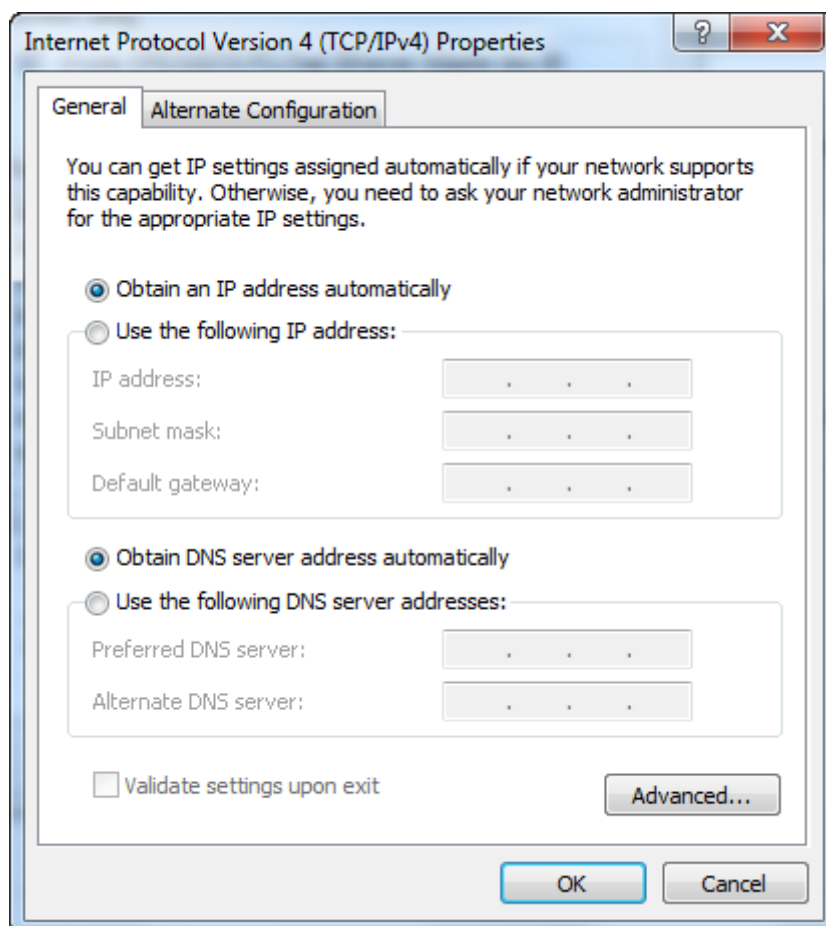
To obtain an IP address from the DHCP server, follow the steps provided below.

**NOTE:** The following procedure assumes you are running Windows. 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.

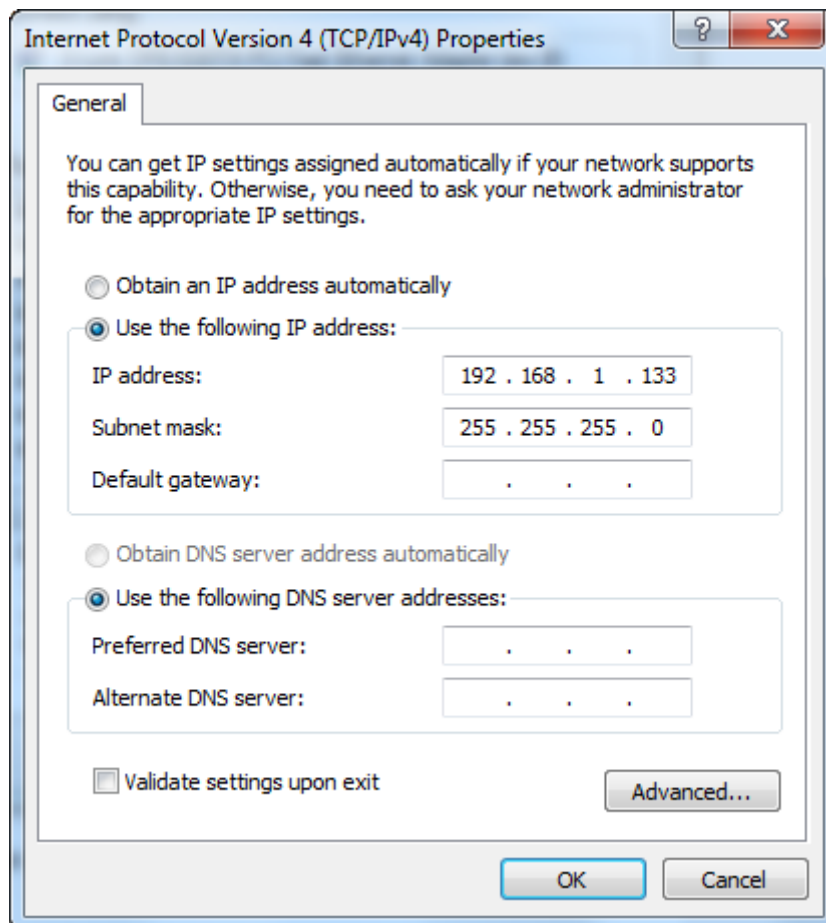
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

**NOTE:** The following procedure assumes you are running Windows. 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 Status](#) 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 [10.4 Password](#)).



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

**Device Status**

This page shows the current status and some basic settings of the device.

---

**System**

Model Name	VR-3046
Uptime	1:40
Firmware Version	CTU-1.0.2
DSP Version	v136h720
CPU Usage	0%
Memory Usage	21%
Name Servers	
IPv4 Default Gateway	
IPv6 Default Gateway	

**DSL**

Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps

**LANConfiguration**

IP Address	192.168.1.4
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	e8d12a304631

**WANConfiguration**

Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
Refresh						

## Chapter 4 Status

### 4.1 Device

This page shows the current status and some basic settings of the device. You can reach this page by clicking on the status icon located on the left side of the screen.

**Device Status**

This page shows the current status and some basic settings of the device.

System	
Model Name	VR-3046
Uptime	1:41
Firmware Version	CTU-1.0.2
DSP Version	v136h720
CPU Usage	0%
Memory Usage	21%
Name Servers	
IPv4 Default Gateway	
IPv6 Default Gateway	

DSL	
Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps

LAN Configuration	
IP Address	192.168.1.4
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	c8d12a304631

WAN Configuration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
Refresh						

## 4.2 IPv6

This page shows the current system status of IPv6 and the delegated prefix information.

**IPv6 Status**

This page shows the current system status of IPv6.

---

**LAN Configuration**

<b>IPv6 Address</b>	
IPv6 Link Local Address	fe80::cad1:2aff:fe30:4631/64

**Prefix Delegation**

<b>Prefix</b>	
---------------	--

**WAN Configuration**

Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Status
Refresh					

Click the **Refresh** button to refresh the page.

## 4.3 LAN Port

This page shows the current LAN port connection status and speed.

**COMTREND**

### LAN Port Status

This page shows the current LAN Port status.

LAN Port Status	
LAN	Up, 100Mb, Full

**Site contents:**

- Status
- Device
- IPv6
- LAN Port
- LAN
- WAN
- Services
- Advance
- Diagnostics
- Admin
- Statistics

Click the **Refresh** button to refresh the page.

## Chapter 5 LAN

This page is used to configure the LAN interface of your Device. Here you may change the setting for IP addresses, subnet mask, etc.

**COMTREND**

### LAN Interface Settings

This page is used to configure the LAN interface of your Device. Here you may change the setting for IP addresses, subnet mask, etc..

InterfaceName: **br0**

IP Address:

Subnet Mask:

Site contents:

- Status
- Device
- IPv6
- LAN Port
- LAN
- WAN
- Services
- Advance
- Diagnostics
- Admin
- Statistics

Click the **Apply Changes** button for your changes to take effect.

**Interface Name:** The name of the LAN interface.

**IP Address:** The IP address your LAN hosts use to identify the device's LAN port.

**Subnet Mask:** The subnet mask for the LAN port.

## Chapter 6 WAN

### 6.1 WAN Mode

This page is used to configure which WAN to use (ATM or PTM) of your Router.

**WAN Mode**

This page is used to configure which WAN to use of your Router.

WAN Mode:  ATM  PTM

**Site contents:**

- Status
- LAN
- WAN
  - WAN Mode
  - PTM WAN
  - ATM WAN
  - ATM Settings
  - DSL Settings
- Services
- Advance
- Diagnostics
- Admin
- Statistics

Check the checkbox  to select the WAN mode. Make your choices and click the **Submit** button.

## 6.2 PTM WAN

This page is used to configure the parameters for PTM WAN. Your ISP determines the Internet access type that you should use.

The screenshot shows the PTM WAN configuration page. On the left is a sidebar with 'Site contents' including Status, LAN, WAN, WAN Mode, PTM WAN, ATM WAN, ATM Settings, DSL Settings, Services, Advance, Diagnostics, Admin, and Statistics. The main content area is titled 'PTM WAN' and contains the following configuration options:

- ptm0\_0 (dropdown)
- Enable VLAN:
- VLAN ID:  802.1p\_Mark:
- Channel Mode:
- Bridge Mode:
- Enable NAPT:
- Admin Status:  Enable  Disable
- Connection Type:
- Enable IGMP-Proxy:
- Enable QoS:

Buttons for 'Apply Changes' and 'Delete' are at the bottom.

Item	Description
Enable VLAN	Check the checkbox to enable a virtual LAN
VLAN ID	Input the VLAN ID number
Channel Mode	Select the channel mode from the drop-down menu. <b>Bridged</b> – Select this option to use the device as an AP <b>IPoE</b> – Select this option if you are connected to the Internet through a cable modem line <b>PPPoE</b> – Select this option if you are connected to the Internet through a DSL line
Bridge Mode	Select the bridge mode from the drop-down menu
Enable NAPT	Check the checkbox to enable network address port translation
Admin Status	Enable/disable admin status
Connection Type	Select the connection type from the drop-down menu
Enable IGMP Proxy	Check the checkbox to enable
802.1p_Mark	Select the 802.1P_mark (0-7) from the drop-down menu
Enable QoS	Check the checkbox to enable quality of service

## 6.3 ATM WAN

This page is used to configure the parameters for WAN mode.

Once you have made your settings, click the **Add** button.

Item	Description
VPI	ATM VPI (0-255) Input the value provided by the ISP
VCI	ATM VCI (32-65535) Input the value provided by the ISP
Enable NAPT	Check the checkbox to enable network address port translation
Admin Status	Check the checkbox to enable or disable this channel
Connection Type	Select the connection type based on the service required from the drop-down menu
Enable VLAN	Check the checkbox to enable a virtual LAN and input the number for the VLAN ID (0-4095)
802.1p_Mark	Select the 802.1P_mark (0-7) from the drop-down menu
Enable IGMP Proxy	Check the checkbox to enable
Encapsulation	Select the AAL5 encapsulation method
Enable QoS	Check the checkbox to enable quality of service



Channel Mode	Select from the operation channel mode from the drop-down menu
*Enable Auto-PVC Search	<p>Check the checkbox to enable auto-pvc search. Then input the VPI (virtual path index) and VCI (virtual channel identifier) and click the <b>Apply</b> button.</p> <p>To add an entry, input the VPI/VCI and click the <b>Apply</b> button.</p> <p>To remove an entry, select it, and then click the <b>Delete</b> button.</p>

**\* Auto PVC Search**

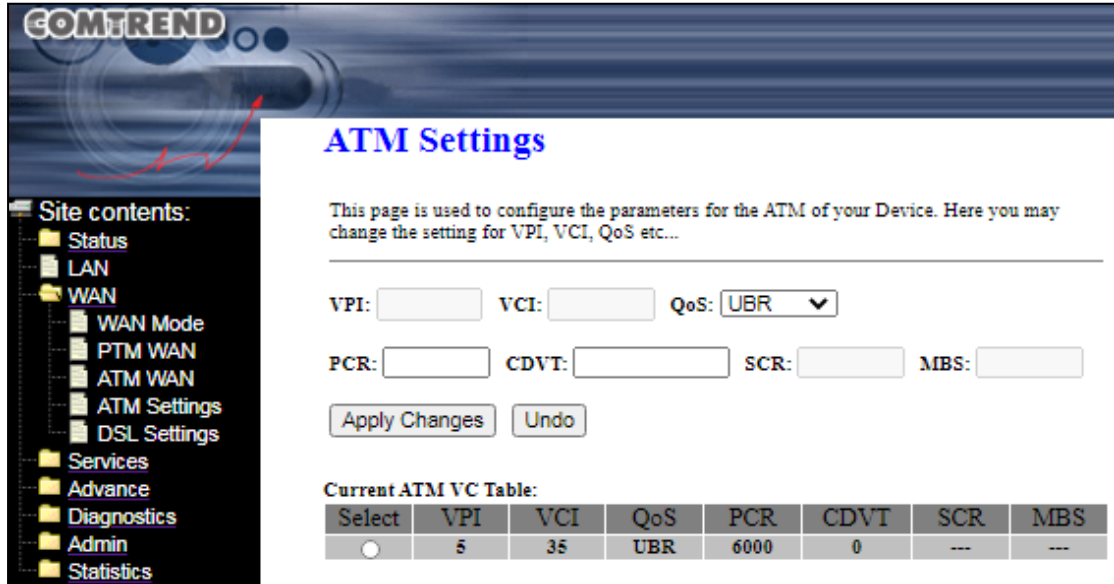
The overall operation of the auto-sensing PVC feature relies on end-to-end OAM pings or packet discovery to defined PVCs. There are two kinds of PVCs: customer default PVCs which are defined by the OEM/ISP and the backup PVCs. The backup list of PVCs are some pre defined VPI/VCI. We can add/delete VPI/VCI into the backup list. By clicking the **Apply** button, the auto-search mechanism can be enabled.

During connection establishment, the PVC module will first search the first customer default PVC. If the first default PVC is found, the module will stop this search. If not found, the backup PVC list is used. If a PVC is found, the PVC module will update the particular PVC as the default PVC, If no PVC is found again, the module will let the end user know that no available VCC was found.

With the connection established, the PVC is stored in flash as the default PVC. Therefore upon reboot, this PVC is automatically chosen as the PVC for that connection.

## 6.4 ATM Settings

This page is used to configure the parameters for the ATM of your Device. Here you may change the setting for VPI, VCI, QoS etc.



**ATM Settings**

This page is used to configure the parameters for the ATM of your Device. Here you may change the setting for VPI, VCI, QoS etc...

VPI:  VCI:  QoS:

PCR:  CDVT:  SCR:  MBS:

**Current ATM VC Table:**

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	5	35	UBR	6000	0	---	---

Once you have made your changes, click the **Apply Changes** button.

Item	Description
VPI	Virtual Path Identifier (0-255)
VCI	Virtual Channel Identifier (32-65535) The VCI together with the VPI, are used to identify the next destination of a cell as it passes through the ATM switch.
Enable QoS	Quality of Service (QoS) is a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. Select the QoS mode from the drop-down menu.
PCR	Peak Cell Rate, the maximum allowable rate at which cells can be transported along a connection in the ATM network
CDVT	Cell Delay Variation Tolerance, which indicates how much jitter is allowable
SCR	Sustainable Cell Rate. A calculation of the average allowable, long-term cell transfer rate on a specific connection
MBS	Maximum Burst Size, The maximum allowable burst size of cells that can be transmitted continuously on a particular connection

## 6.5 DSL Settings

This page is used to configure the parameters for the bands of your Device.

**DSL Settings**

This page is used to configure the parameters for the bands of your Device.

**DSL Modulation:**

- G.Lite
- G.Dmt
- T1.413
- ADSL2
- ADSL2+
- VDSL2

**AnnexL Option:** (Note: Only ADSL 2 supports AnnexL)

Enabled

**AnnexM Option:** (Note: Only ADSL 2/2+ support AnnexM)

Enabled

**G.Vector Option:**

Enabled

**VDSL2 Profile:**

- 8a
- 8b
- 8c
- 8d
- 12a
- 12b
- 17a
- 30a
- 35b

**DSL Capability:**

- Enabled Bitswap
- Enabled SRA

Click the **Apply Changes** button for your changes to take effect.

Item	Description
DSL Modulation	Check the checkbox to select your preferred DSL standard protocols

AnnexJ Option	Check the checkbox to enable Annex J
G.Vector Option	Check the checkbox to enable the G.Vector option
VDSL2 Profile	Check the checkbox to select VDSL profiles
DSL Capability	Enables Bitswap and Seamless Rate Adaptation capability

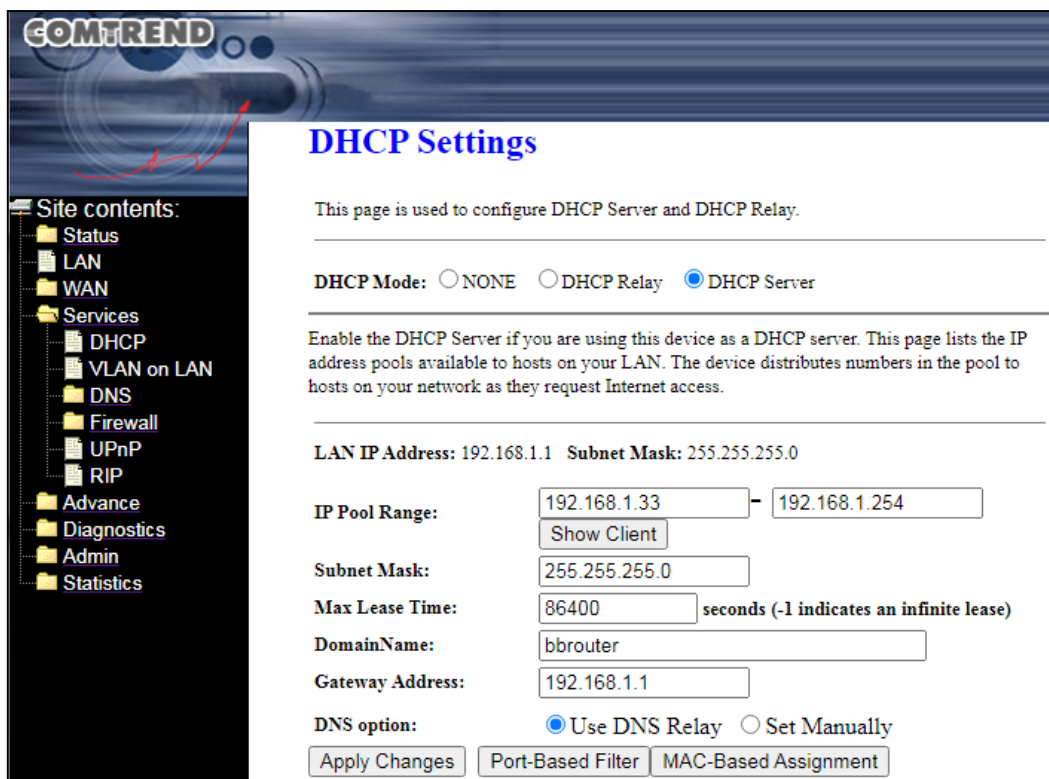
## Chapter 7 Services

### 7.1 DHCP

This page is used to configure DHCP Server and DHCP Relay.

#### 7.1.1 DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

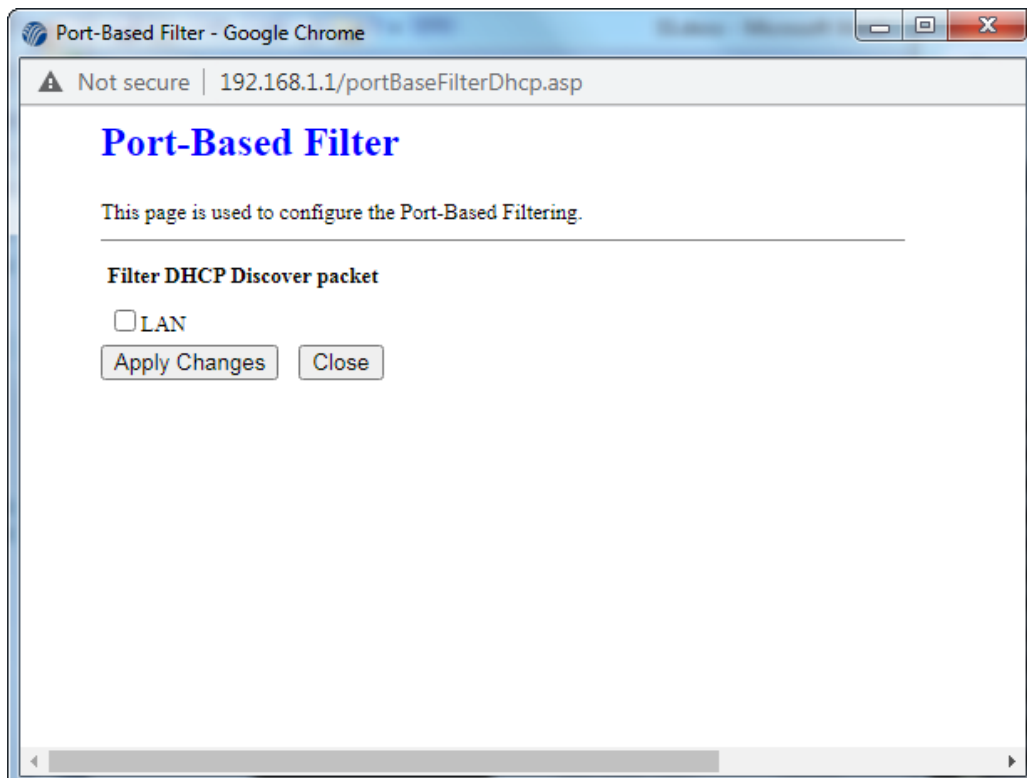


Click the **Apply Changes** button for your changes to take effect.

Item	Description
LAN IP Address/Subnet Mask	Displays the IP address and Subnet Mask for the LAN port
IP Pool Range	The range of IP addresses that is used for the DHCP server
Subnet Mask	The subnet mask used for the DHCP server

<p>Max Lease Time</p>	<p>The lease time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the lease time, the lease is either renewed or a new IP address is issued by the DHCP server. The default value is 86400 seconds (1 day).</p>
<p>Domain Name</p>	<p>Input the Domain name</p>
<p>Gateway Address</p>	<p>Input the Default Gateway IP address of the DHCP network</p>
<p>DNS option</p>	<p>If Use DNS Relay radio button is selected, the DHCP server will use the device IP (i.e. 192.168.1.1) as DNS address; if Set Manually is selected, the DHCP server will use manually assigned DNS addresses in the leased IP configuration.</p>

Click the **Port-Based Filter** button to configure the Port-Based Filtering. In this page you can drop DHCP packets coming from some LAN ports.



Click the **MAC-Based Assignment** to configure the static IP base on MAC Address. You can assign/delete the static IP. For the Host MAC Address, please input a string with hex numbers. Such as 00-d0-59-c6-12-43. For the Assigned IP Address, please input a string with digits. Such as 192.168.1.100

MAC-Based Assignment - Google Chrome

Not secure | 192.168.1.1/macptbl.asp

## MAC-Based Assignment

This page is used to configure the static IP base on MAC Address. You can assign/delete the static IP. The Host MAC Address, please input a string with hex number. Such as 00-d0-59-c6-12-43. The Assigned IP Address, please input a string with digit. Such as 192.168.1.100 .

MAC Address (xx-xx-xx-xx-xx-xx):

Assigned IP Address (xxx.xxx.xxx.xxx):

MAC-Based Assignment Table:

Select	MAC Address	Assigned IP Address
--------	-------------	---------------------

### 7.1.2 DHCP Relay

Some Internet Service Providers perform the DHCP server function for their customers' home/small office network. In this case, you can configure this device to act as a DHCP relay agent. When a host on your network requests internet access, the device contacts your ISP to obtain the IP configuration, and then forwards that information to the host.



Click the **Apply Changes** button for your changes to take effect.

Item	Description
DHCP Server IP Address	Specify the IP address of your ISP's DHCP server. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.



## 7.2 VLAN on LAN

If the LAN interface needs to support VLAN tagging, the CPE can tag VLAN on the LAN.



Click the **Apply Changes** button for your changes to take effect.

## 7.3 DNS – Dynamic DNS

### 7.3.1 Dynamic DNS

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO or No-IP. Here you can Add/Remove to configure Dynamic DNS.

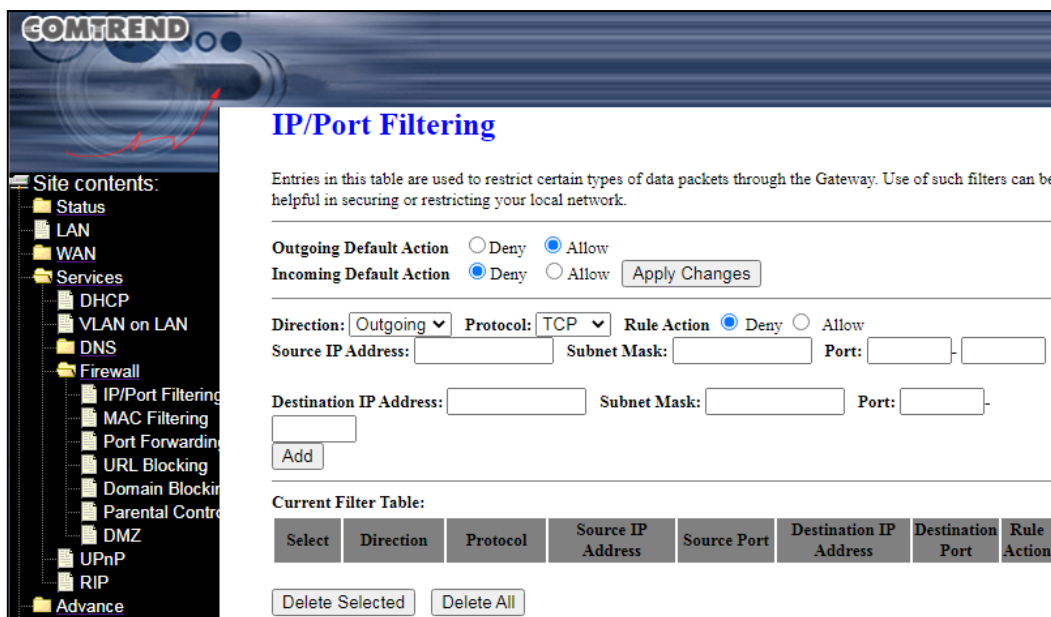
Item	Description
Enable	Check the checkbox to enable Dynamic DNS
DDNS Provider	Select the DDNS provider from the drop-down menu
Hostname	Input the DDNS HostName
Interface	Select the interface from the drop-down menu
<b>DynDns/No-IP Settings</b>	
UserName	Input the username
Password	Input the password
<b>TZO Settings</b>	
Email	Input the Email address of TZO account
Key	Input the password of TZO account

## 7.4 Firewall

Firewall contains several features that are used to deny or allow traffic from passing through the device.

### 7.4.1 IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



Click the **Apply Changes** button for your changes to take effect.

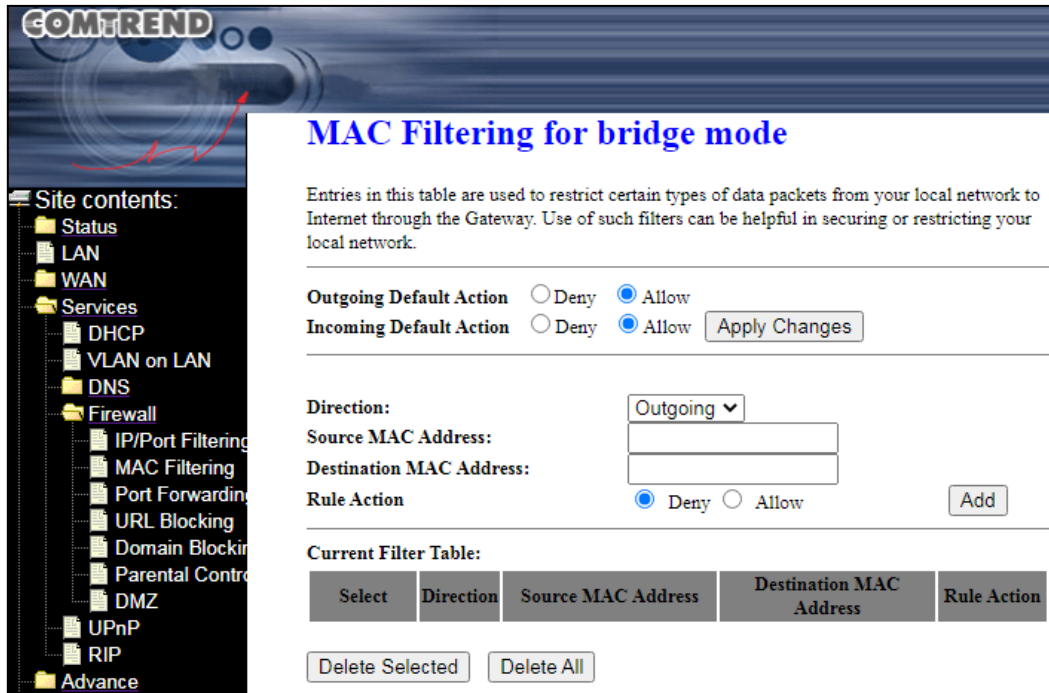
Click the **Add** button to add a filter.

Item	Description
Outgoing Default Action	Deny/Allow outgoing default action feature
Incoming Default Action	Deny/Allow incoming default action feature
Direction	Select the direction from the drop-down menu
Protocol	Select the protocol from the drop-down menu
Rule Action	Deny/Allow the rule action feature
Source IP Address	Input the source IP address
Subnet Mask	Input the Subnet Mask

Port	Input the source port number or range
Destination IP Address	Input the destination IP address
Subnet Mask	Input the Subnet Mask
Port	Input the destination port number or range

### 7.4.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



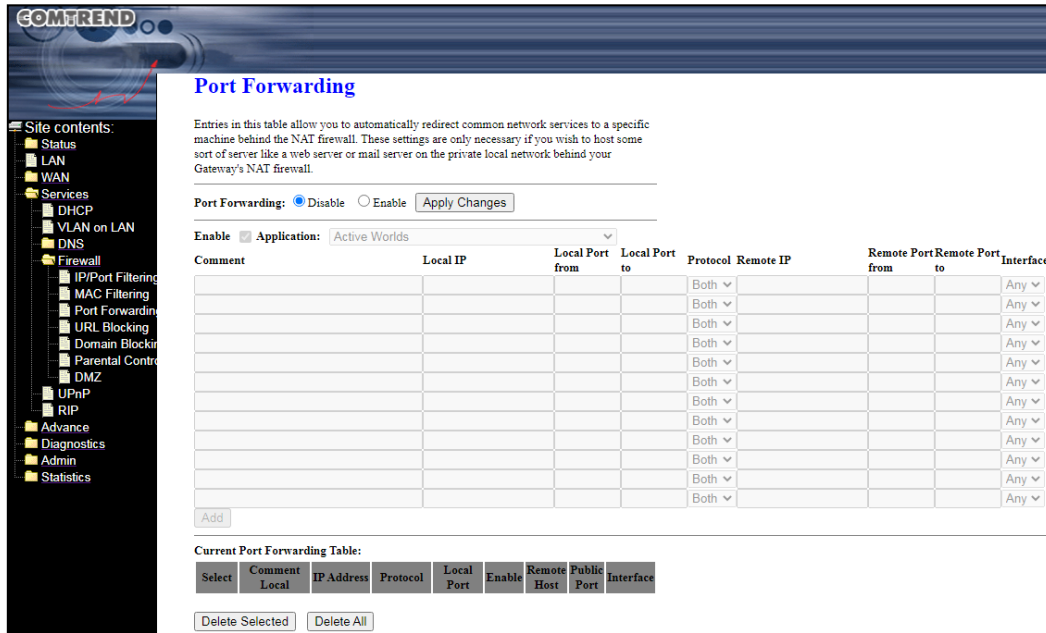
Click the **Apply Changes** button for your changes to take effect.

Click the **Add** button to add a filter.

Item	Description
Outgoing Default Action	Deny/Allow outgoing default action feature
Incoming Default Action	Deny/Allow incoming default action feature
Direction	Select the direction from the drop-down menu
Source MAC Address	Input the Source MAC Address
Destination MAC Address	Input the Destination MAC Address
Rule Action	Deny/Allow the rule action feature

### 7.4.3 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.



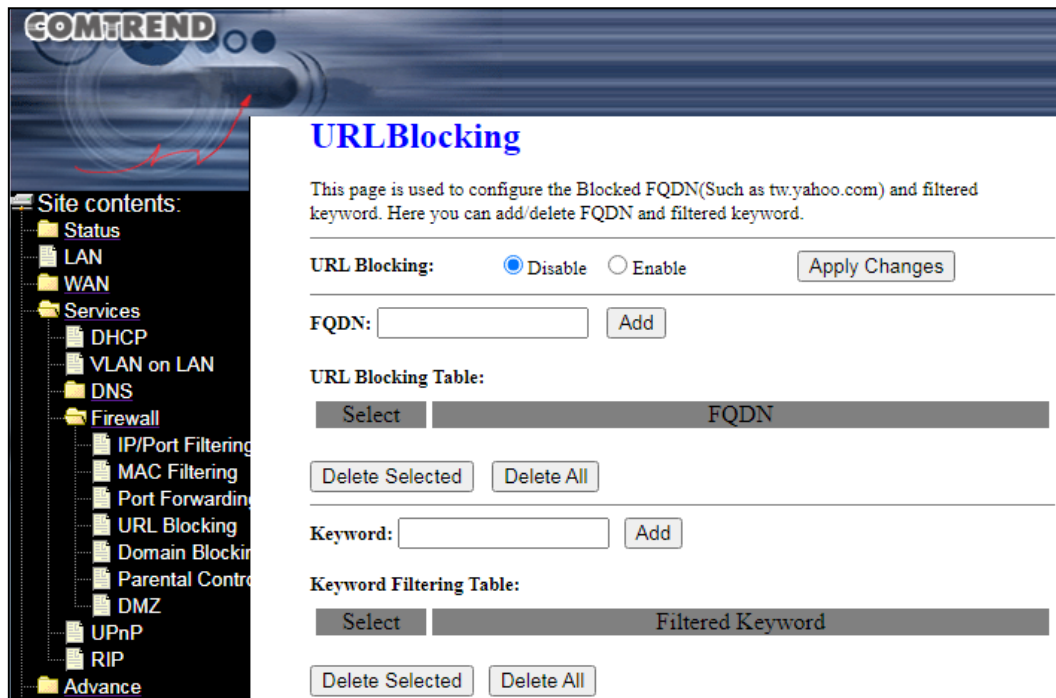
Click the **Apply Changes** button for your changes to take effect.

Item	Description
Port Forwarding	Enable or disable Port Forwarding by selecting the appropriate radio button
Enable	Check the checkbox to enable Port Forwarding entries
Application	Select from the drop-down menu or User-defined service name
Comment	User-defined service name
Local IP	Input the IP address for Local Server
Local Port from	Input the starting port number
Local Port to	Input the ending port number
Protocol	Select the protocol from the drop-down menu
Remote IP	Input the Remote IP address

Remote Port from	Input the remote(external) starting port number
Remote Port to	Input the remote(external) ending port number
Interface	Select from the drop-down menu

### 7.4.4 URL Blocking

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.



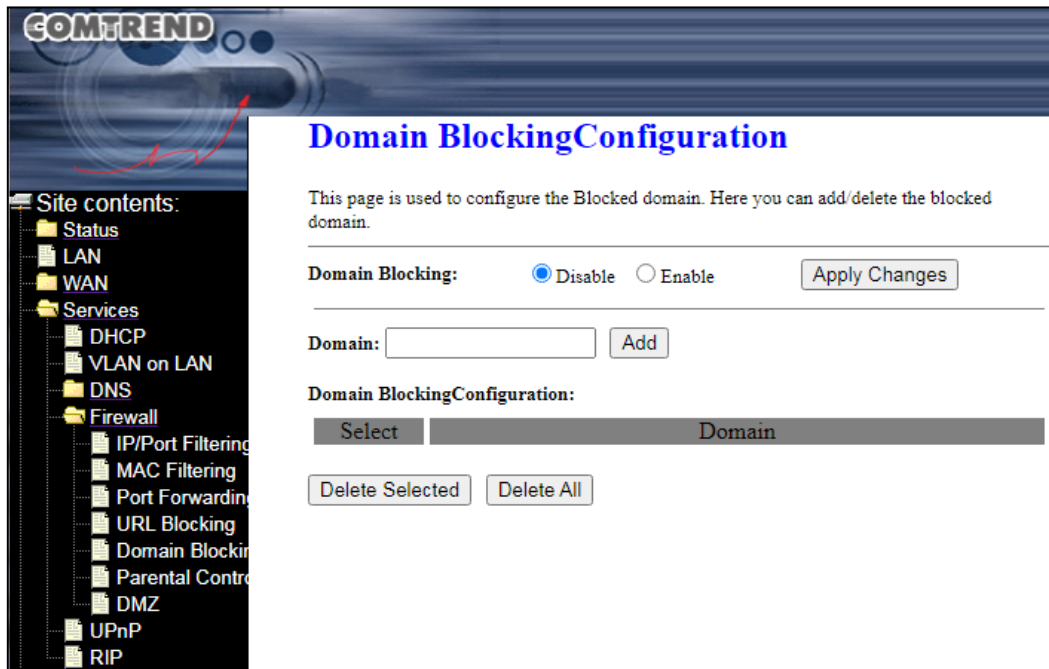
Click the **Apply Changes** button for your changes to take effect.

Item	Description
URL Blocking	Disable/Enable the URL blocking feature
FQDN	Input the Fully Qualified Domain Name
Keyword	This filtered keyword such as yahoo, if the URL includes this keyword, the yahoo URL's will be blocked access
Keyword Filtering Table	Displays the Keyword filtering entries



### 7.4.5 Domain Blocking

This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.

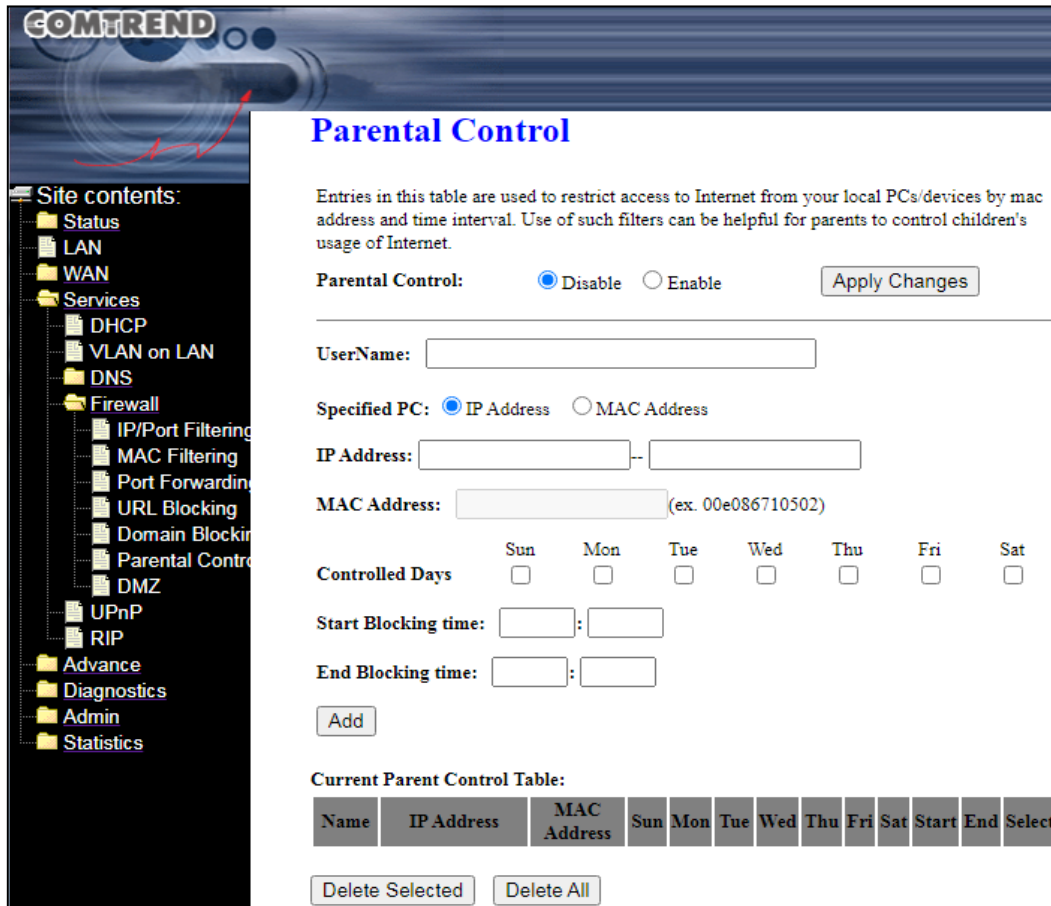


Click the **Apply Changes** button for your changes to take effect.

Item	Description
Domain Blocking	Disable/Enable the domain blocking feature
Domain	Input the domain name

### 7.4.6 Parental Control

Entries in this table are used to restrict access to Internet from your local PCs/devices by MAC address and time interval. Use of such filters can be helpful for parents to control children's usage of Internet.

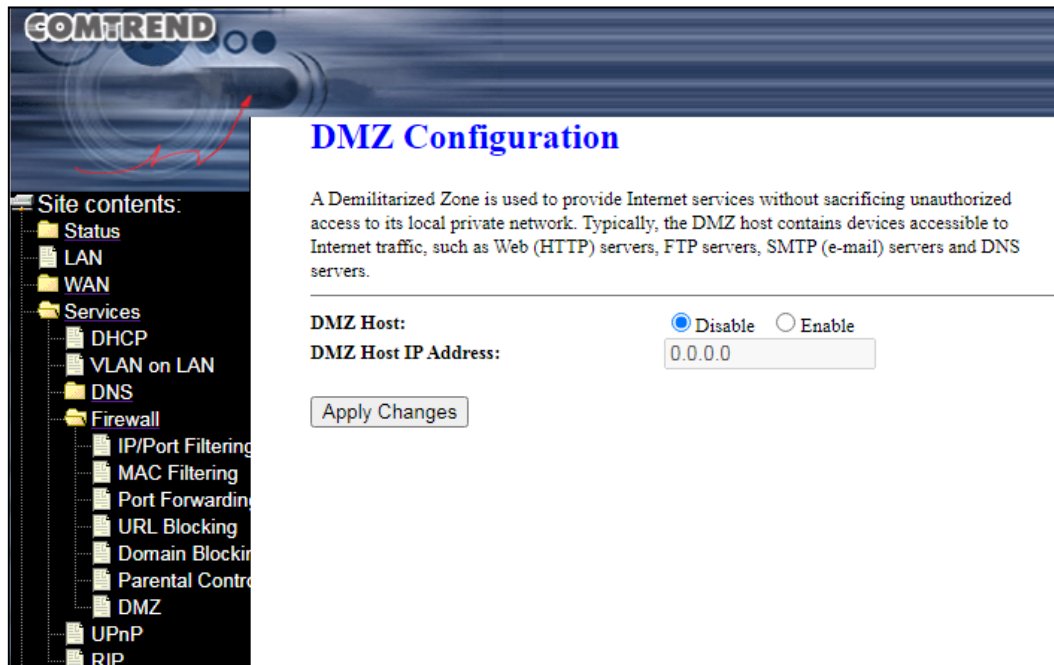


Click the **Add** button to add a time restriction.

Item	Description
Parental Control	Disable/Enable the parental control feature
User Name	Input your user name
Specified PC	Select the IP Address/MAC Address radio button
IP Address	Input the IP address range
MAC Address	Input the MAC address
Controlled Days	Select the days for the restrictions to apply
Start Blocking time	The time the restrictions start
End Blocking time	The time the restrictions end

## 7.4.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

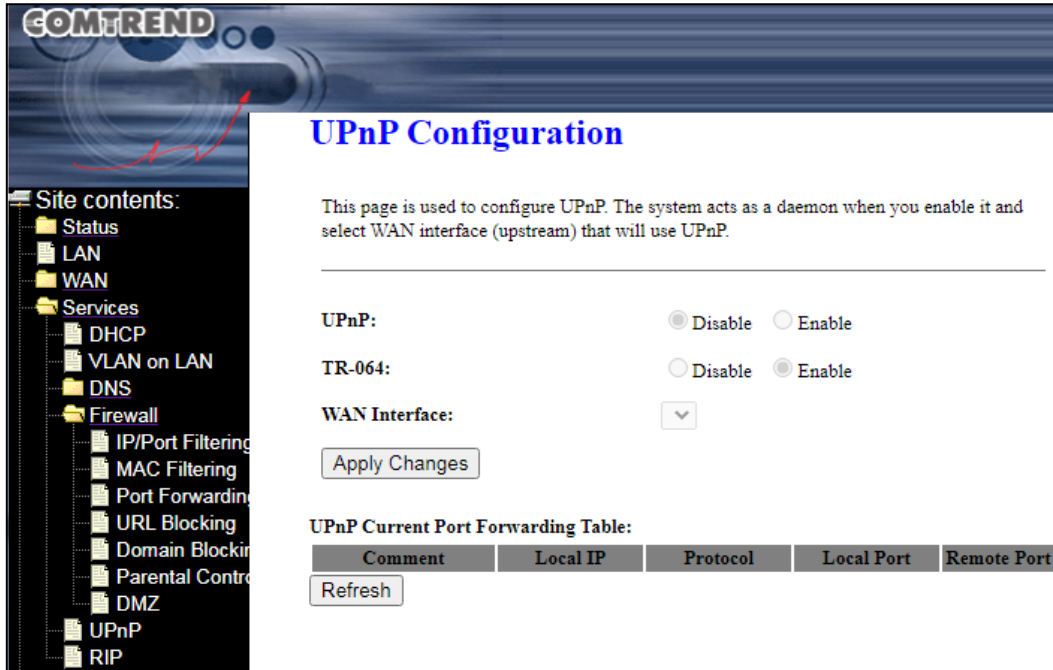


If you want to use DMZ select the Enable radio button and input the internal DMZ host IP address.

Click the **Apply Changes** button for your changes to take effect.

## 7.5 UPnP

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.



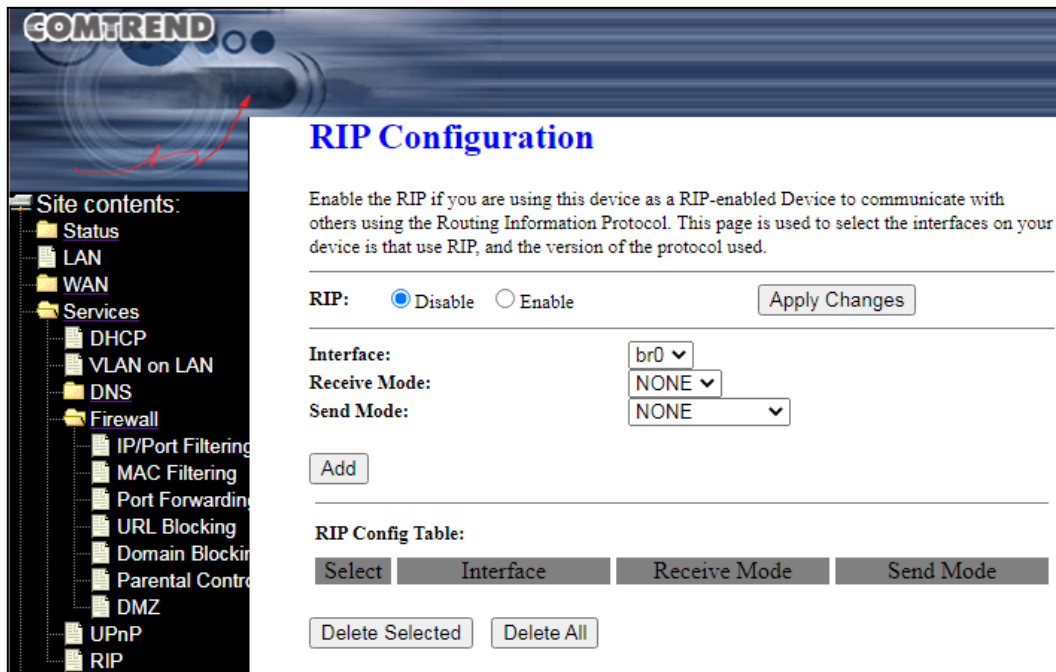
Click the **Apply Changes** button for your changes to take effect.

Item	Description
UPnP	Disable/Enable the UPnP feature
TR-064	Disable/Enable the TR-064 feature
WAN Interface	Select the WAN interface that will use UPnP from the drop-down menu

Click the **Refresh** button to reload the page.

## 7.6 RIP

Enable the RIP if you are using this device as a RIP-enabled Device to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device that use RIP, and the version of the protocol used.



Click the **Add** button to configure an entry.

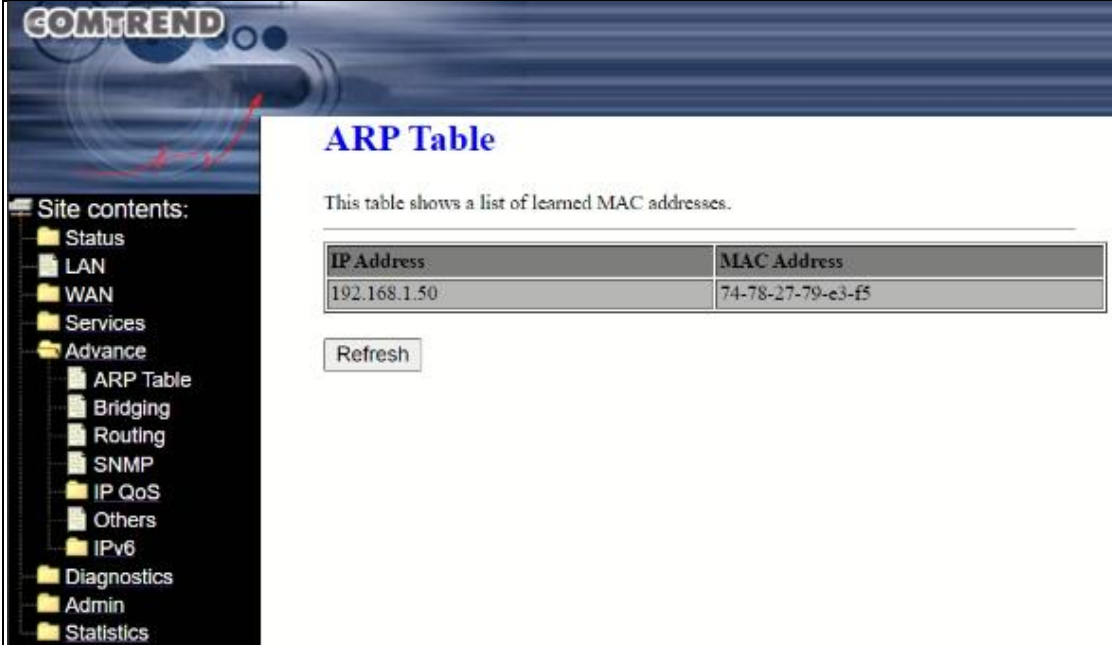
Click the **Apply Changes** button for your changes to take effect.

Item	Description
RIP	Enable/Disable the RIP feature
Interface	Select from the drop-down menu
Receive Mode	Select from the drop-down menu
Send Mode	Select from the drop-down menu

## Chapter 8 Advanced

### 8.1 ARP Table

ARP is used to map a MAC address to an IP address. ARP dynamically binds the IP address to the correct MAC address. This table shows a list of learned MAC addresses.



**ARP Table**

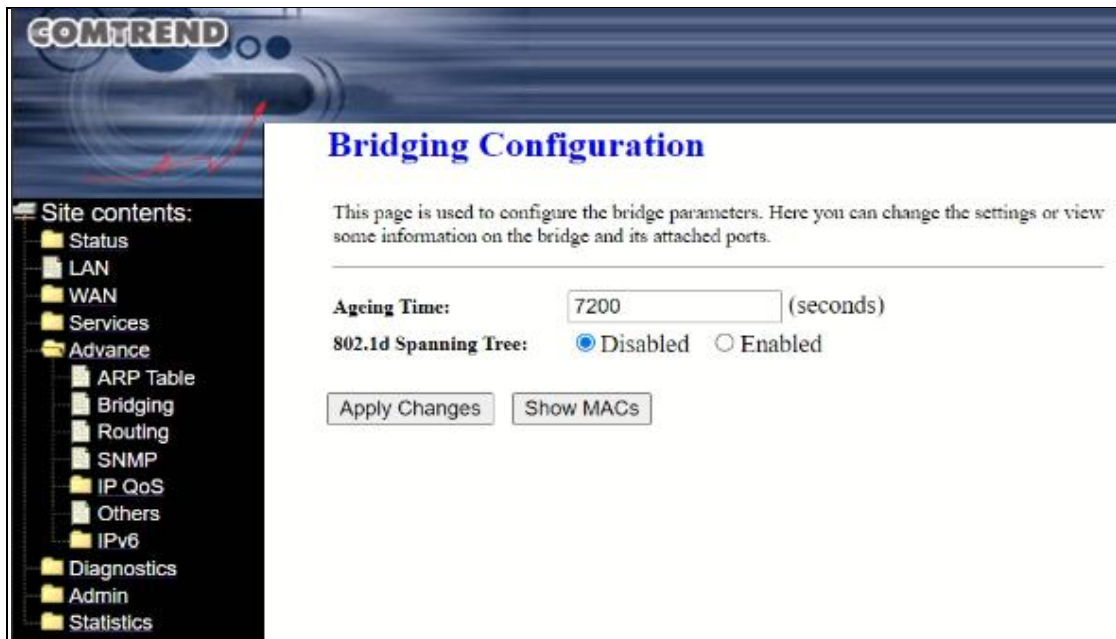
This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.1.50	74-78-27-79-e3-f5

Click the **Refresh** button to reload the page.

## 8.2 Bridging

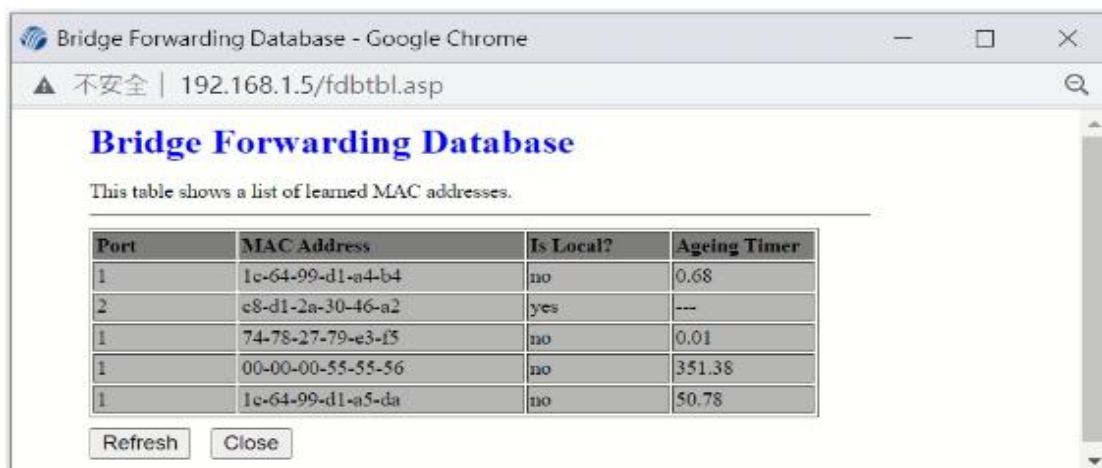
This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.



Click the **Apply Changes** button for your changes to take effect.

Item	Description
Ageing Time	Configure the ageing time, after (ageing time in seconds) of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from the Forwarding DataBase (fdb).
802.1d Spanning Tree	Disable/Enable the spanning tree protocol feature

Click the **Show MACs** button to display the following.



## 8.3 Routing

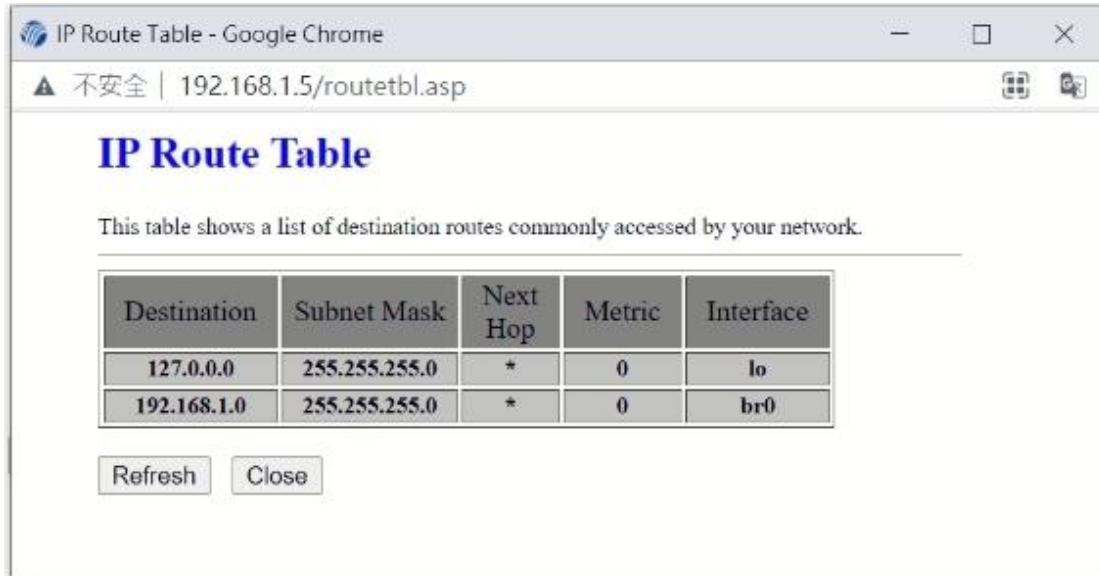
This page is used to configure the routing information. Here you can add/delete IP routes.



Item	Description
Enable	Check the checkbox to enable this route entry
Destination	The network IP address of the subnet. The destination can be specified as the IP address of the subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet
Next Hop	The next hop of this destination route
Metric	The metric value of routing defines the number of hops between network nodes that data packets travel
Interface	Select the WAN interface from the drop-down menu to which a static routing subnet is applied

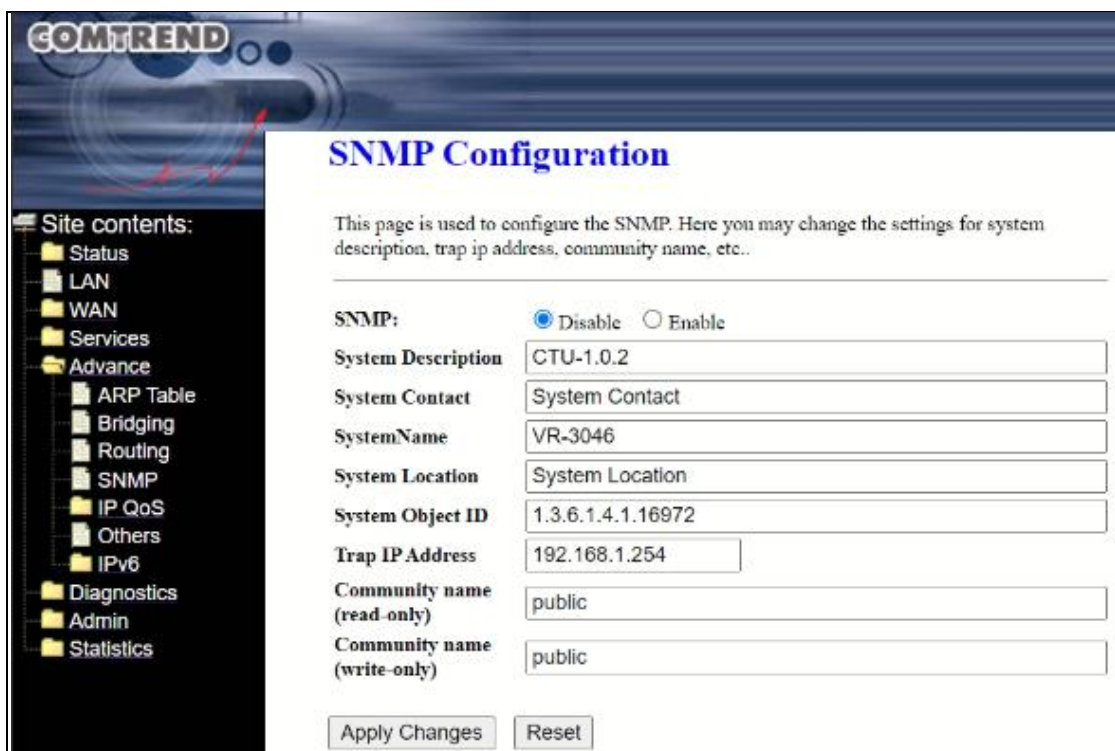
Click the Show Routes button to display the following.





## 8.4 SNMP

Simple Network Management Protocol (SNMP) is a troubleshooting management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The device can be managed locally or remotely by SNMP protocol. On this page you may change the settings for system description, trap IP address, community name, etc.



Click the **Apply Changes** button for your changes to take effect.

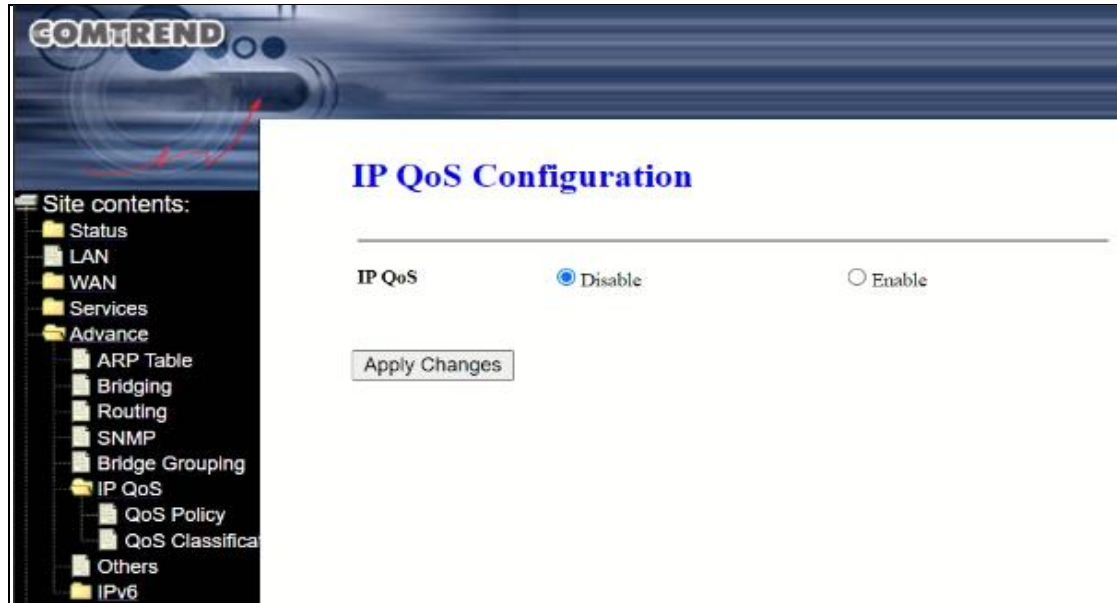
Click the **Reset** button to reset all page entries to their initial values.

Item	Description
SNMP	Select the Disable/Enable radio button
System Description	Input the system description of the device
System Contact	Input the contact person or information for the device
System Name	Input the system name for the device
System Location	Input the physical location of the device
System Object ID	Input the vendor object ID
Trap IP Address	Input the destination IP Address of the SNMP trap
Community name (read-only)	Name of the read-only Community. The read-only Community allows read operation to all objects in the MIB (Management Information Base).
Community name (write-only)	Name of the write-only Community. The write-only Community allows write operation to the objects defined as read-writable the MIB.

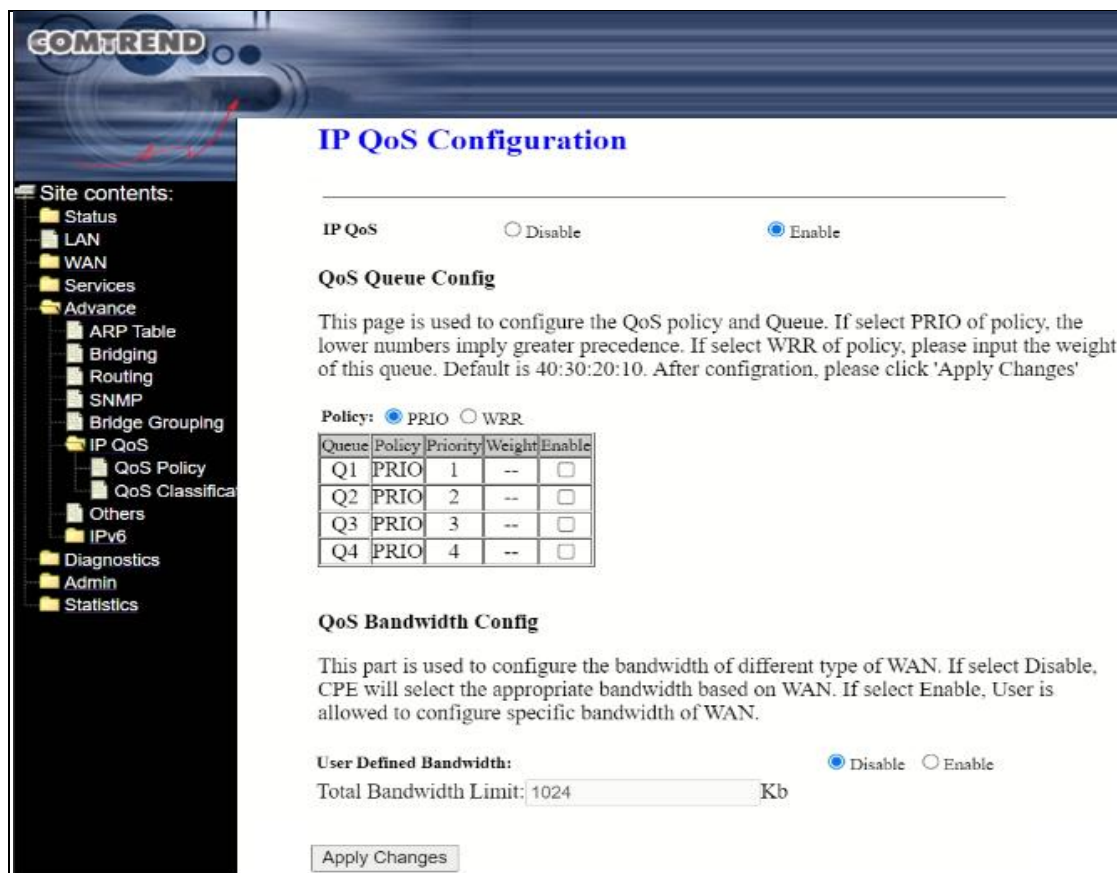
## 8.5 IP QoS

### 8.5.1 QoS Policy

The device provides a control mechanism which serves traffic with different priority



To enable IP QoS, select the Enable radio button to display the following.



Configure your settings and click the **Apply Changes** button.

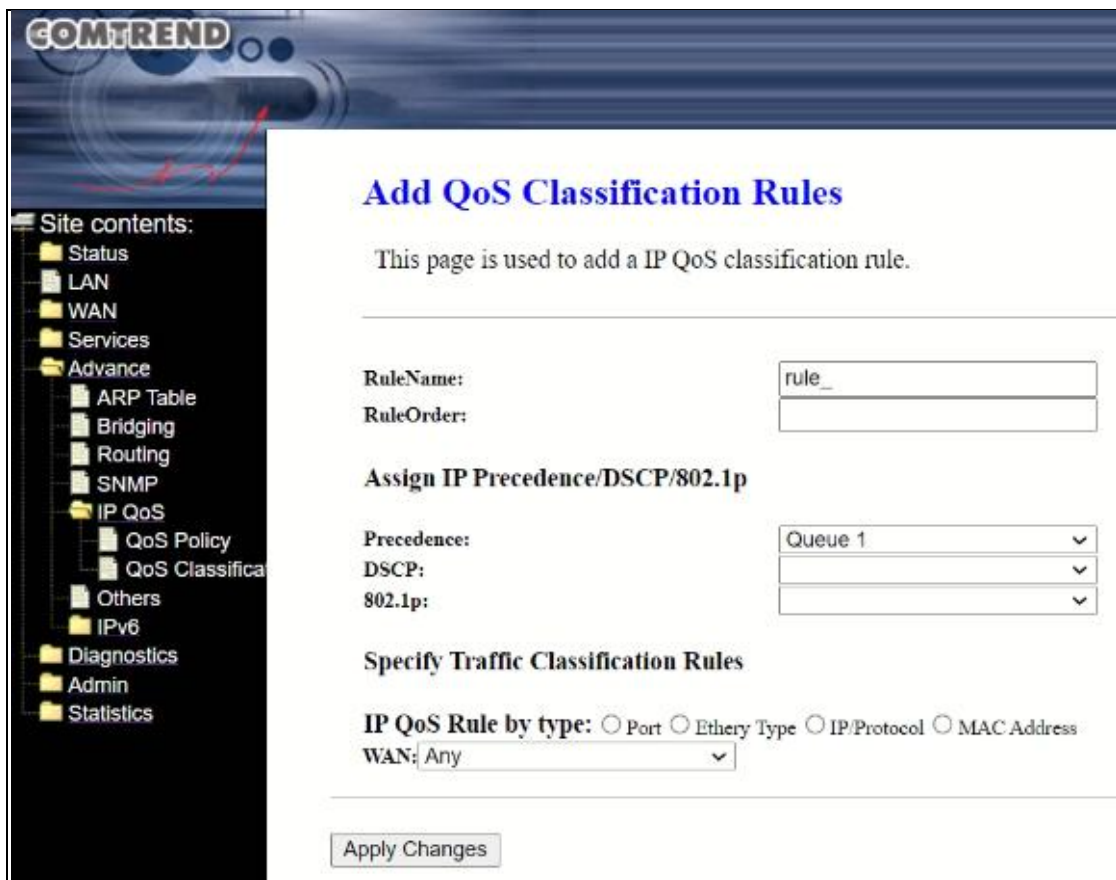
<b>Item</b>	<b>Description</b>
Policy	Select the PRIO (strict-priority) or WRR (Weighted Round Robin) for QoS setting
Q1-Q4	The device supports four different queues, enable/disable each queue by clicking the enable button
User Defined Bandwidth	Enable/disable the total bandwidth setting accord to the total bandwidth limit
Total Bandwidth Limit	The setting of total bandwidth defined by the user

### 8.5.2 QoS Classification

This device provides a control mechanism which serves traffic with different priorities. This allows you to apply the strict priority level and/or mark some fields in the packet for traffic that falls in this classification.



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



After adding a new rule, please click the **Apply Changes** button for the rule to take effect.

Item	Description
Rule Name	The identifier for this Queue entry (defined by the user)
Rule Order	Input the value of the rule order (defined by the user)
Precedence	Select from the drop-down menu to mark the IP precedence bits in the packet which match this classification rule. Select from queue 1-4.
DSCP	Select from the drop-down menu to mark the IP TOS bits in the packet which match this classification rule
802.1p	Select from the drop-down menu to mark the 3-bit user-priority field in the 802.1p header for traffic that falls in this classification. Note that this 802.1 marking is applicable on a given PVC channel only if the VLAN tagging is enabled in that PVC channel.
IP QoS Rule by type	Select from Port, Ethery type, IP/Protocol or MAC address

#### Setting IP QoS rule by port

Item	Description
WAN	Select the uplink WAN interface
Physical Port	Select the incoming physical port and blank indicates that no physical port is specified.

#### Setting IP QoS rule by Ethery type

Item	Description
WAN	Select the uplink WAN interface
Ethernet Type	Select the Ethernet type of packets

### Setting IP QoS rule by port IP/Protocol

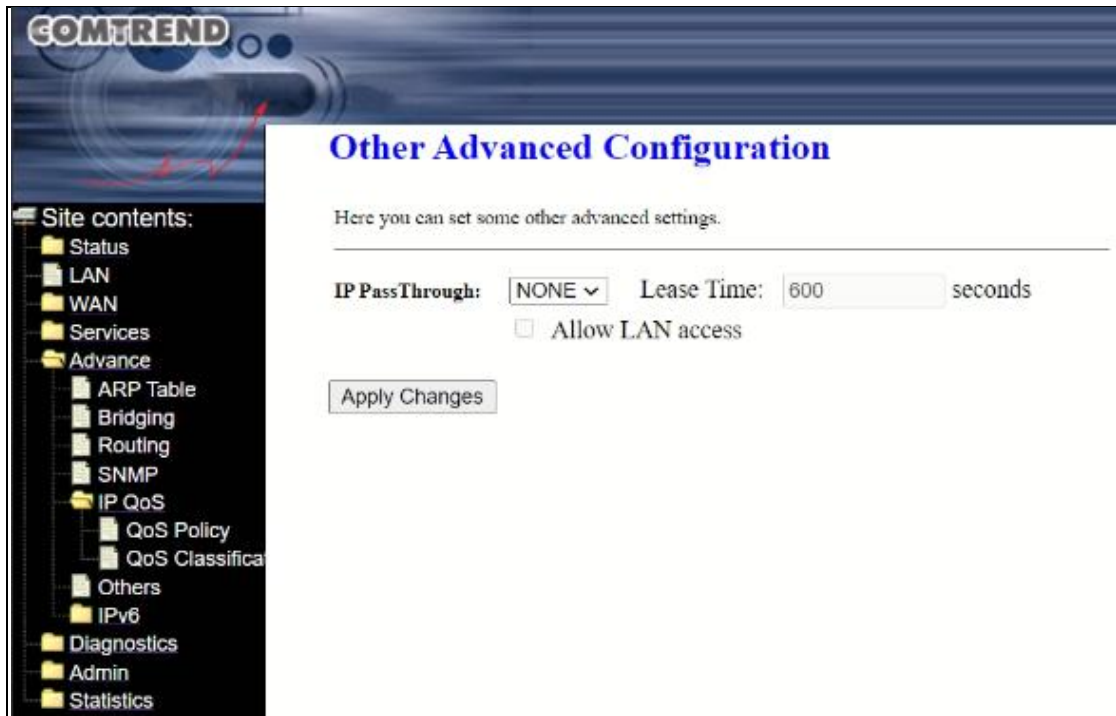
Item	Description
WAN	Select the uplink WAN interface
IP Version	Select IPv4 or IPv6
Protocol	Select from TCP, UDP, ICMP or TCP/UDP. A blank selection indicates that this criterion is not used for classification.
DSCP	Select the DSCP in IP packet
Source IP	Source IP address
Source Mask	Source IP address mask. This field is required if the source IP has been assigned.
Destination IP	Destination IP address
Destination Mask	Destination IP address mask. This field is required if the destination IP has been assigned.
Source Port	Source port number. You cannot configure this field if no protocol has been selected.
Destination Port	Destination port number. You cannot configure this field without selecting the protocol first.

### Setting IP QoS rule by MAC address

Item	Description
WAN	Select the uplink WAN interface
Source MAC	Source MAC address
Destination MAC	Destination MAC address

## 8.6 Others

This page allows you to set the IP PassThrough feature.



Click the **Apply Changes** button for the rule to take effect.

Item	Description
IP Pass Through	Select the IP pass through interface
Lease Time	Input the lease time in seconds for the IP pass through
Allow LAN access	Check the checkbox to enable



## 8.7 IPv6

### 8.7.1 IPv6

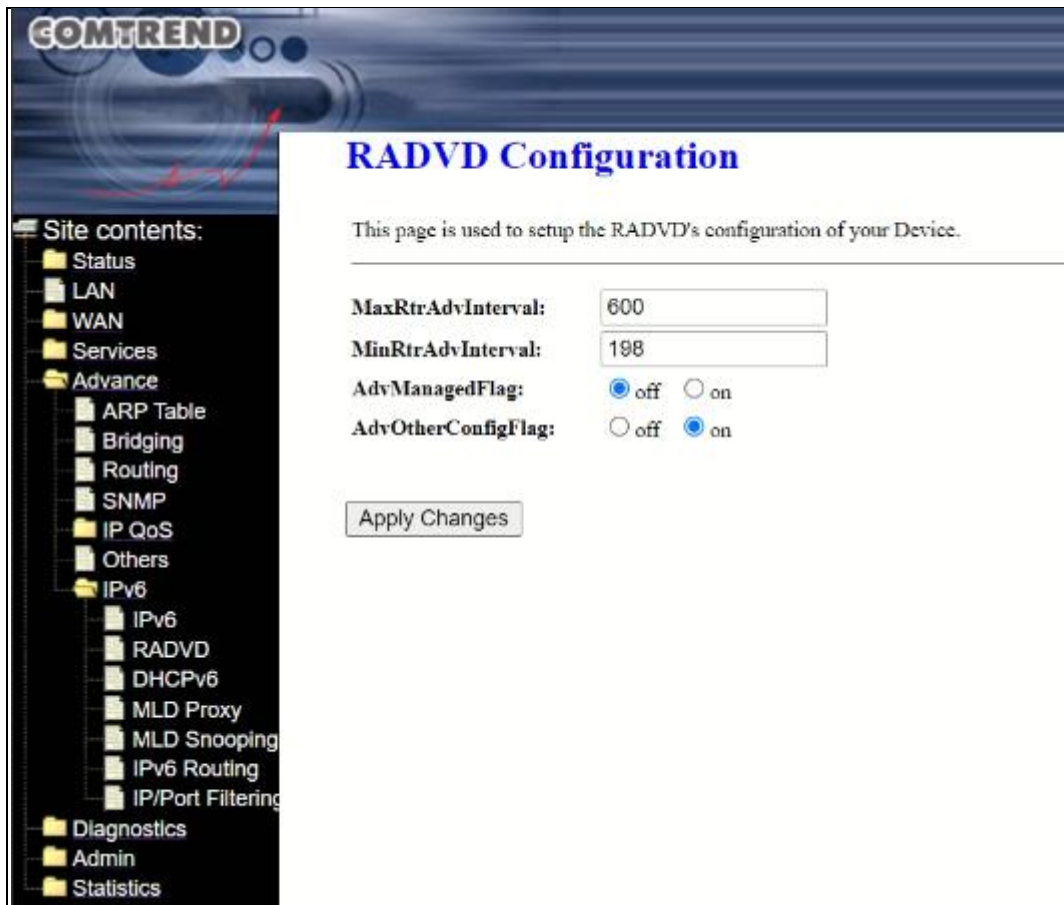
This page can be used to configure IPv6 enable/disable.



Click the **Apply Changes** button for your changes to take effect.

### 8.7.2 RADVD

This page is used to setup the router advertisement daemons (RADVD's) configuration of your Device.



Click the **Apply Changes** button for your changes to take effect.

Item	Description
Max Rtr Adv Interval	The maximum allowed time allowed between sending unsolicited router advertisements from the interface, in seconds
Min Rtr Adv Interval	The minimum allowed time allowed between sending unsolicited router advertisements from the interface, in seconds
Adv Managed Flag	Check the checkbox to turn off or turn on Adv Managed Flag. When turned on, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any address autoconfigured using stateless address autoconfiguration.

<p>Adv Other Config Flag</p>	<p>Check the checkbox to turn off or turn on Adv Other Config Flag. When turned on, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information.</p>
------------------------------	--

### 8.7.3 DHCPv6

This page is used to configure DHCPv6 Server and DHCPv6 Relay. The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol for configuring IPv6 hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network.

IPv6 hosts may automatically generate IP addresses internally using stateless address configuration, or they may be assigned configuration data with DHCPv6.

IPv6 hosts that use stateless autoconfiguration may require information other than an IP address or route. DHCPv6 can be used to acquire this information, even though it is not being used to configure IP addresses.



### 8.7.3.1 DHCPv6 – DHCP Server (Auto)

Set the IPv6 server automatically, the dsl devices will use the prefix and IP address from Prefix Delegation (IAPD) and DNSv6 address from IPv6 WAN.

#### DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

---

**DHCPv6 Mode:**  NONE  DHCPRelay  DHCPServer(Manual)  DHCPServer(Auto)

---

Auto Config by Prefix Delegation for DHCPv6 Server.

Click the **Apply Changes** button for your changes to take effect.

Click the **Show Client** button to display the following.

#### Active DHCPv6 Clients

This table shows the assigned IP address, DUID and time expired for each DHCP leased client.

IP Address	DUID	Expired Time (sec)
NONE	----	----

### 8.7.3.2 DHCPv6 – NONE

If you do not require DHCP Server or DHCP Relay, select the NONE radio button and click the **Apply Changes** button.

#### DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

---

**DHCPv6 Mode:**  NONE  DHCPRelay  DHCPServer(Manual)  DHCPServer(Auto)

---

### 8.7.3.3 DHCPv6 – DHCP Relay

This page is used to configure the upper interface (server link) for DHCPv6 Relay. The DHCPv6 Relay Agent uses Relay forward/Reply messages to relay the messages between servers and clients.

**DHCPv6 Settings**

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

---

DHCPv6 Mode:  NONE  DHCPRelay  DHCPServer(Manual)  DHCPServer(Auto)

---

This page is used to configure the upper interface (server link) for DHCPv6 Relay.

---

Upper Interface: vc0\_0 ▼

**Upper Interface:** Select an interface of the servers for the relay agent.

Click the **Apply Changes** button for your changes to take effect.

**8.7.3.4 DHCPv6 – DHCP Server (Manual)**

Enable the DHCPv6 Server if you are using this device as a DHCPv6 server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

### DHCPv6 Settings

This page is used to configure DHCPv6 Server and DHCPv6 Relay.

---

**DHCPv6 Mode:**  NONE  DHCPRelay  DHCPv6Server(Manual)  DHCPv6Server(Auto)

---

Enable the DHCPv6 Server if you are using this device as a DHCPv6 server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

**IP Pool Range:**  -

**Prefix Length:**

**Valid Lifetime:**  seconds

**Preferred Lifetime:**  seconds

**Renew Time:**  seconds

**Rebind Time:**  seconds

**Client DUID:**

---

**Domain:**

**Domain Search Table:**

Select	Domain
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>	

---

**Name Server IP:**

**Name Server Table:**

Select	Name Server
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>	

Item	Description
IP Pool Range	Set the IP address range allowing the device to allocate to LAN users
Prefix Length	Input the prefix length
Valid Lifetime	Specify how long the prefix remains valid for onlink determination

Preferred Lifetime	Specify how long the prefix generated by stateless autoconfiguration remains preferred
Renew Time	The number of seconds from the time a client gets an address until the client transitions to the RENEWING state.
Rebind Time	The number of seconds from the time a client gets an address until the client transitions to the REBINDING state.
Client DUID	This option specifies the server's DUID identifier. You can use this option to configure an opaque binary blob for your server's identifier.
Domain	Input the domain name of the IPv6 DNS server
Name Server IP	Input the IP address of the IPv6 DNS server

### 8.7.4 MLD Proxy

Multicast Listener Discovery (MLD) Proxy is a component of the internet protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like Internet Group Management Protocol (IGMP) is used in IPv4.



Click the **Apply Changes** button for your changes to take effect.

Item	Description
MLD Proxy	Enable/Disable the MLD proxy on the DSL device
WAN Interface	Select the WAN interface for uplink MLD protocols



### 8.7.5 MLD Snooping

MLD Snooping provides functionality for IPv6 that is similar to IGMP snooping for IPv4, by sending IPv6 multicast traffic only to interested listeners. By listening to and analyzing MLD messages, when VR-3046 enables MLD snooping, it will establish mappings between ports and multicast MAC addresses or multicast IP addresses, and forwards multicast data.



Click the **Apply Changes** button for your changes to take effect.

### 8.7.6 IPv6 Routing

The IPv6 routing page allows you to define a specific route for your internet and network data.



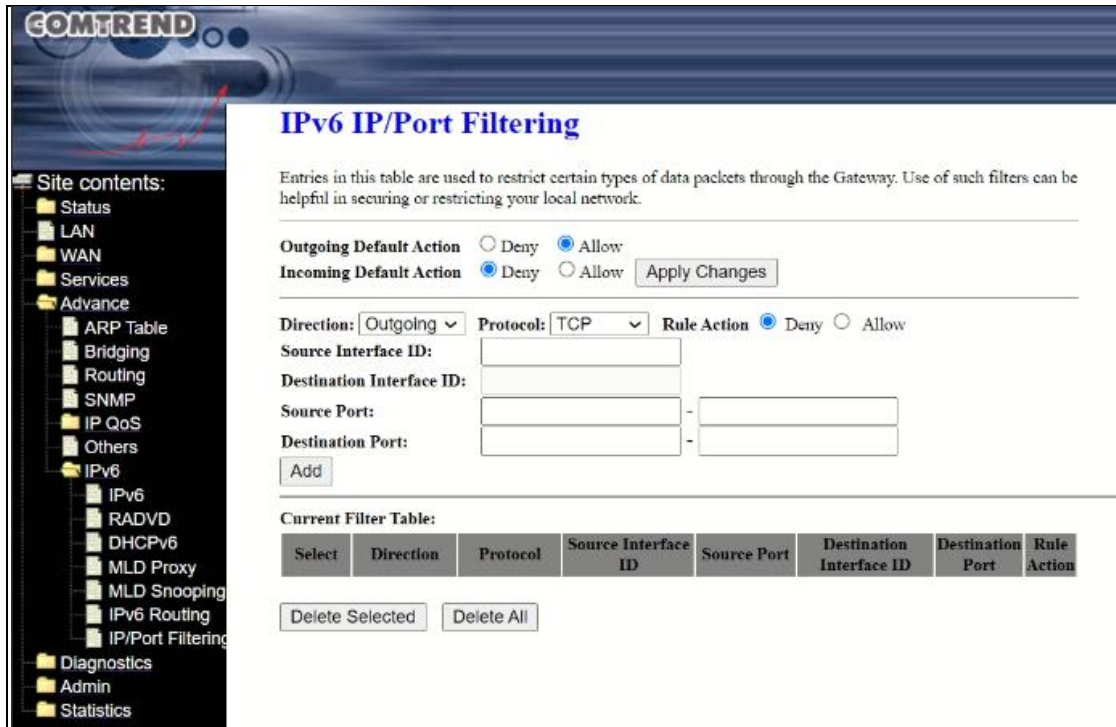
Click the **Add Route** button to add an entry to the static IPv6 route table

Item	Description
Enable	Check the checkbox to enable the route entry
Destination	Input the destination IP address. The destination can be specified as the IPv6 address of a subnet or a specific host in the subnet.
Next Hop	Input the next hop of this destination route
Metric	The metric defines the number of hops between network nodes that data packets travel
Interface	Select the interface from the drop-down menu to which the static IPv6 routing is applied

### 8.7.7 IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Click the **Apply Changes** button for your changes to take effect.



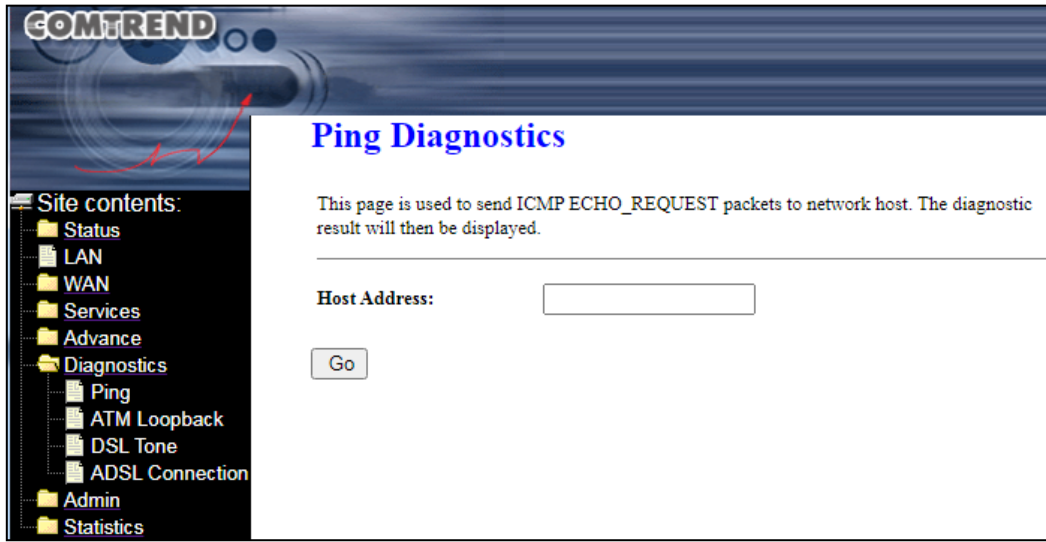
Item	Description
Outgoing Default Action	Specify the default action on the LAN to WAN forwarding path
Incoming Default Action	Specify the default action on the WAN to LAN forwarding path
Direction	Select the traffic forwarding direction from the drop-down menu
Protocol	Select the protocol from the drop-down menu
Rule Action	Deny/Allow the rule action feature
Source Interface ID	The IPv6 interface address assigned to the traffic on which filtering is applied. The format should look like "x:x:x:x".
Destination Interface ID	The IPv6 interface address assigned to the traffic on which filtering is applied. The format should look like "x:x:x:x".

Source Port	Input the starting and ending source port numbers
Destination Port	Input the starting and ending destination port numbers

## Chapter 9 Diagnostics

### 9.1 Ping

This page is used to send ICMP ECHO\_REQUEST packets to network host. The diagnostic result will then be displayed.



Input the address you want to ping and click the **Go** button.

Please see the test result below for reference.

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes

64 bytes from 192.168.1.1: icmp_seq=0
64 bytes from 192.168.1.1: icmp_seq=1
64 bytes from 192.168.1.1: icmp_seq=2

--- ping statistics ---
3 packets transmitted, 3 packets received.
```

Back

## 9.2 ATM Loopback

Connectivity verification is supported by the use of the ATM OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Item	Description
Select PVC	Select the PVC channel you want to do the loop-back diagnostic
Flow Type	The ATM OAM flow type. The selection can be an F5 segment or F5 End-to-End
Loopback Location ID	The loopback location ID field of the loop-back cell

Click the **Go!** button to see the result.

**ATM Loopback Diagnostic Results**

Repetitions Count: 5

Repetitions Timeout: 1000 ms

Success Response Count: 0

Failure Response Count: 5

Average Response Time: 0 ms

Minimum Response Time: 0 ms

Maximum Response Time: 0 ms

## 9.3 DSL Tone

DSL Tone Diagnostics. Only ADSL2/ADSL2+/VDSL2 support this function.

Click the **Start** button to run the DSL diagnostic.

**DSL Tone Diagnostics**

DSL Tone Diagnostics. Only ADSL2/ADSL2+/VDSL2 support this function.

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					

## 9.4 ADSL Connection

The Device is capable of testing your connection. The individual tests are listed below. If a test displays a fail status, click 'Go' button again to make sure the fail status is consistent.



Click the **Go** button to run an ADSL connection check.



## Chapter 10 Admin

### 10.1 Commit/Reboot

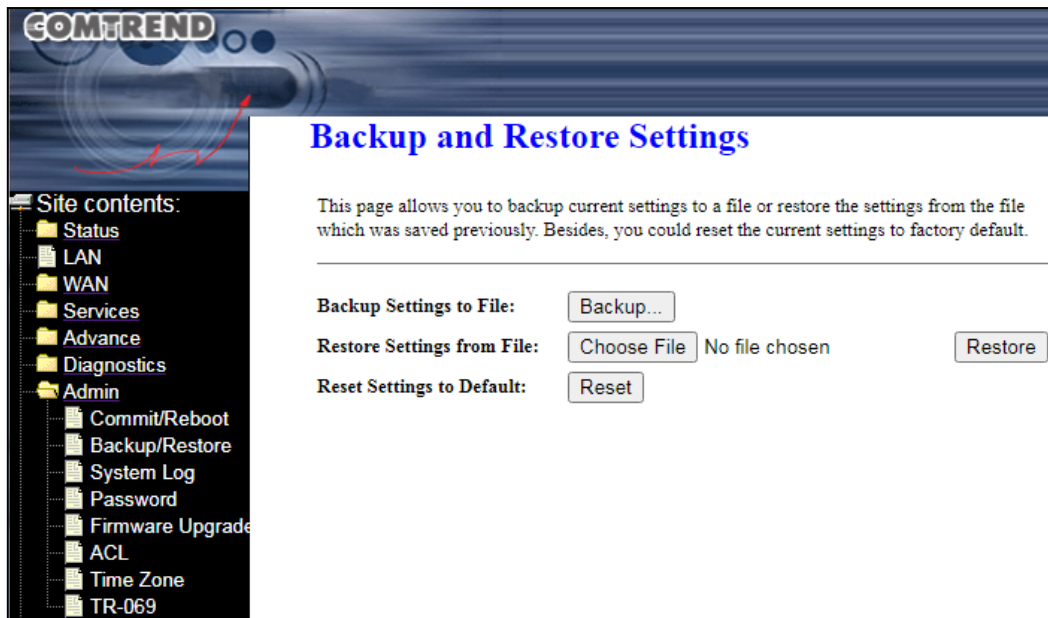
This page is used to commit changes to system memory and reboot your system.



Click the **Commit and Reboot** button to commit changes to system memory and reboot your system.

## 10.2 Backup/Restore

This page allows you to backup current settings to a file or restore the settings from a file which was saved previously. Besides, you could reset the current settings to factory default.



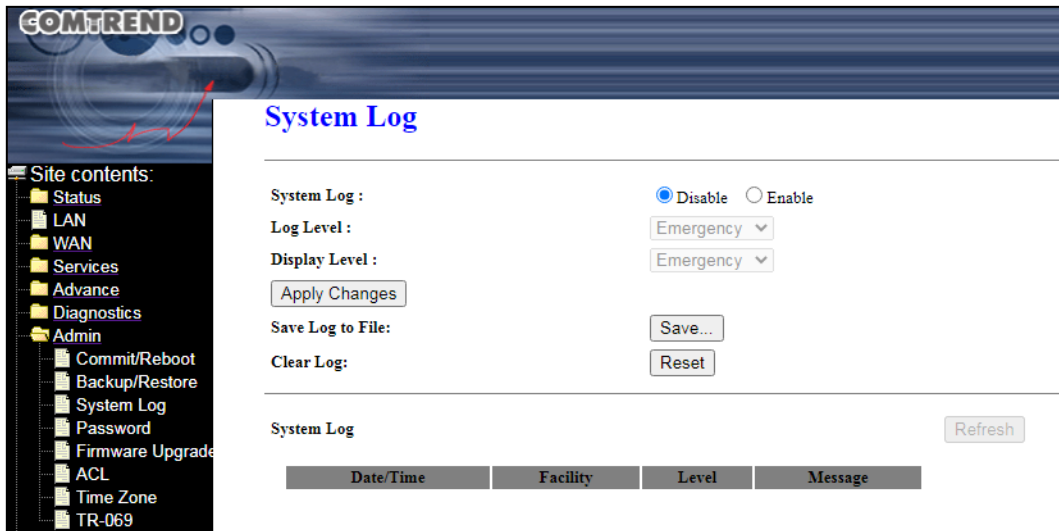
Click the **Backup** button to backup your settings to a file.

To restore settings from a file, click the **Choose File** button to select the file, then click the **Restore** button.

To reset settings to their default values, click the **Reset** button.

## 10.3 System Log

This page is used to configure DHCPv6 Server and DHCPv6 Relay.



Click the **Apply Changes** button for your changes to take effect.

Click the **Save** button to save the log to a file.

Click the **Reset** button to clear the log.

Item	Description
System Log	Enable/disable the system log feature
Log Level	Select the log levels to be recorded from the drop-down menu
Display Level	Select the different log levels to be displayed from the drop-down menu

## 10.4 Password

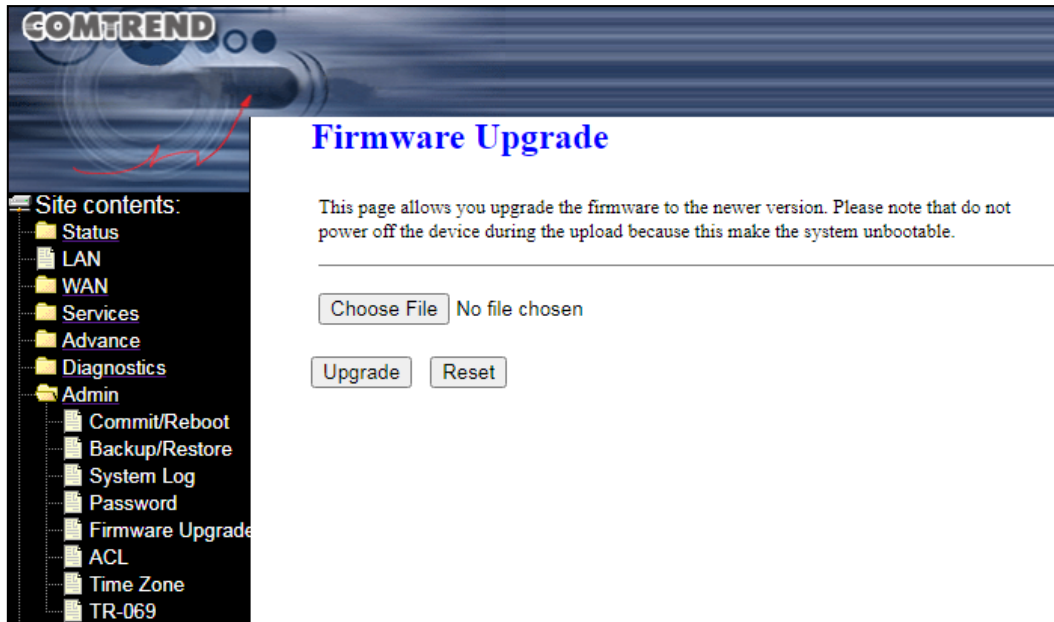
This page is used to set the account to access the web server of your Device. Empty user name and password will disable the protection.

Click the **Apply Changes** button for your changes to take effect.

Item	Description
User Name	Select from the drop-down menu
Old Password	Input the old password
New Password	Input the new password
Confirmed Password	Confirm the new password by inputting it again

## 10.5 Firmware Upgrade

This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.



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

**STEP 2:** Click the **Choose File** button to locate the image file.

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

**Important:** Do not turn off the device or push the reset button while this procedure is in process.

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

## 10.6 ACL

This page is used to configure the IP Address for Access Control List. If ACL is enabled, only the IP address in the ACL Table can access CPE. Here you can add/delete the IP Address.

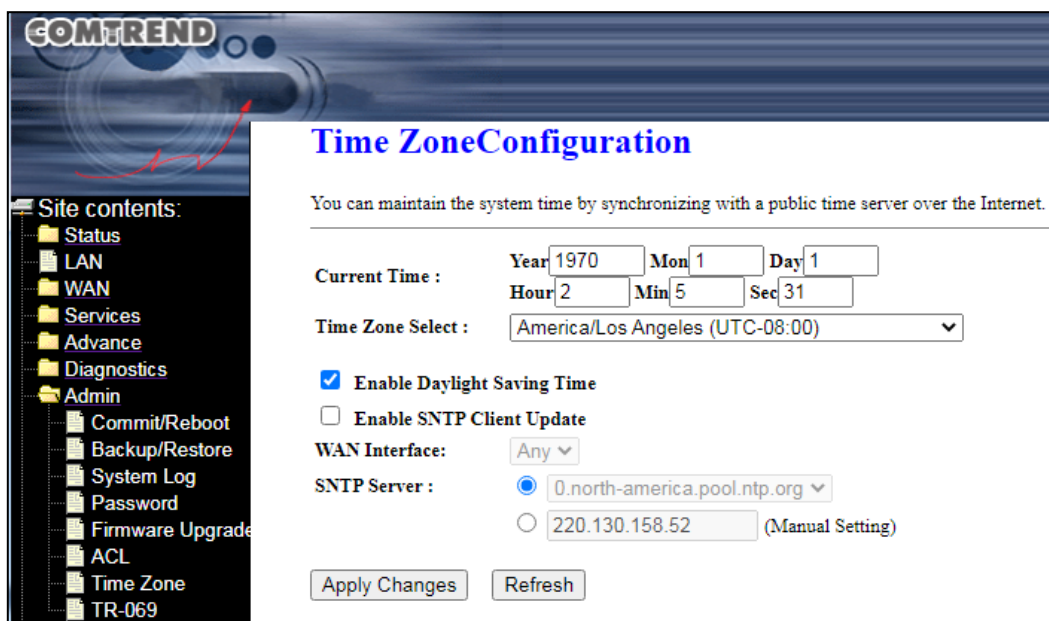
Click the **Apply Changes** button for your changes to take effect.

Item	Description
ACL Capability	Check the checkbox to enable or disable the ACL feature
Enable	Check the checkbox to enable ACL entry
Interface	Select the required interface domain (LAN or WAN) from the drop-down menu
IP Address	Input the IP address that allow access to this device

Subnet Mask	Input the subnet mask that allow access to this device
Service Name / LAN	Select the service type that allow access to this device

## 10.7 Time Zone

You can maintain the system time by synchronizing with a public time server over the Internet.



Click the **Apply Changes** button for your changes to take effect.

Item	Description
Current Time	Input the current date and time of the specified time zone. You can set the current time by yourself or configure by SNTP
Time Zone Select	Select the time zone for your region
Enable Daylight Saving Time	Check the checkbox to enable daylight saving time
Enable SNTP Client Update	Check the checkbox to enable SNTP (Simple Network Time Protocol) client to update the system clock

WAN Interface	Select the WAN interface from the drop-down menu
SNTP Server	Select SNTP server or manually input the SNTP server IP address



## 10.8 TR-069

This page is used to configure the TR-069 CPE. TR-069 is a protocol for communication between a CPE and the Auto-Configuration Server (ACS).

Here you may change the setting for the ACS's parameters.

**TR-069 Configuration**

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

**TR069 Daemon:**  Enabled  Disabled

**Enable CWMP Parameter:**  Enabled  Disabled

**ACS:**

URL:

User Name:

Password:

Periodic Inform:  Disabled  Enabled

Periodic Inform Interval:

**Connection Request:**

User Name:

Password:

Path:

Port:

**Certificate Management:**

CPE Certificate:

CPE Certificate Password:

CPE Certificate:  No file chosen

CA Certificate:  No file chosen

Item	Description
TR069 Daemon	Enable/Disable TR-069 feature
Enable CWMP Parameter	Enable/Disable CWMP parameter feature

<b>ACS</b>	
URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
UserName	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
Periodic Inform	Enable/Disable the periodic inform feature
Periodic Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method
<b>Connection Request</b>	
UserName	Username used to authenticate an ACS making a Connection Request to the CPE
Password	Password used to authenticate an ACS making a Connection Request to the CPE
Path	The Path of the TR069 connection request URL
Port	The Port of the TR-069 connection request URL
<b>STUN Setting</b>	
STUN	Enable/Disable the STUN feature
STUN Server Address	Input the STUN server IP address
STUN Server Port	Input the STUN Server port number

STUN Server User	Username used to authenticate with STU server
STUN Server Password	Password used to authenticate with STU server
<b>Certificate Management</b>	
CPE Certificate Password	Input the Certificate Password
CPE Certificate	Click the <b>Choose File</b> button to select the required file. Then, click the <b>Upload</b> button.
CA Certificate	Click the <b>Choose File</b> button to select the required file. Then, click the <b>Upload</b> button.

## Chapter 11 Statistics

### 11.1 Interface

This page shows the packet statistics for transmission and reception regarding to network interface.

**Interface Statistics**

This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
LAN	19114	0	0	15023	0	0

Refresh    Reset Statistics

Click the **Refresh** button to reload the page.

Click the **Reset Statistics** button reset the page.

Item	Description
Interface	Interface name
Rx pkt	Number of Received packets
Rx err	Number of Received packets with errors
Rx drop	Number of Received dropped packets
Tx pkt	Number of Transmitted packets
Tx err	Number of Transmitted packets with errors
Tx drop	Number of Transmitted dropped packets

## 11.2 DSL

This page shows the DSL statistics.

**DSL Statistics**

Mode	
TPS-TC	
Latency	
Status	ACTIVATING.
Power Level	L0
Uptime	
G.Vector	Off

	Downstream	Upstream
Trellis	Off	Off
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	0.0
Attainable Rate (Kbps)	0	0
G.INP	Off	Off
Rate (Kbps)	0	0
R (number of check bytes in RS code word)	0	
N (RS codeword size)	0	0
L (number of bits in DMT frame)	0	0
S (RS code word size in DMT frame)	0.00	
D (interleaver depth)	0	
Delay (msec)	0.00	
INP (DMT frame)	0.000	0.000
FEC errors	0	0
OH Frame	0	0
OH Frame errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	7962	0
Total LOSS	--	--
Last Link Rate	0	0
Full Init	0	
Failed Full Init	0	
Synchronized time(Second)		
Synchronized number	0	

Item	Description
Mode	Displays the xDSL type
TPS-TC	Displays PTM or ATM

Latency	Displays Fast or Interleave
Status	Lists the status of the DSL link
Power Level	Link output power state
Uptime	Establishes the connection time
G.Vector	On or Off
<b>Downstream/Upstream</b>	
Trellis	Trellis On/Off
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain
G.INP	On or Off
Rate (Kbps)	Current sync rates downstream/upstream
R (number of check bytes in RS code word)	Number of redundancy bytes in the RS codeword
N (RS codeword size)	RS codeword size
L (number of bits in DMT frame)	Number of bits transmitted in each data symbol
S (RS code word size in DMT frame)	Number of data symbols the RS codeword spans
D (interleaver depth)	The interleaver depth
Delay (msec)	The delay in milliseconds (msec)
INP (DMT frame)	DMT symbol
FEC errors	Total number FEC errors
OH Frame	Total number of OH frames
OH Frame errors	Number of OH frames received with errors
Total ES	Total Number of Errored Seconds

Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds
Total LOSS	Total Number of LOSS
Last Link Rate	Last connection rate
Full Init	Number of Full Init
Failed Full Init	Number of Failed Full Init
Synchronized time(Second)	Number of Synchronized time(Second)
Synchronized number	Number of Synchronized number

## Appendix A - Pin Assignments

### Giga ETHERNET Ports (RJ45)

Pin	Name	Description
1	BI_DA+	Bi-directional pair A +
2	BI_DA-	Bi-directional pair A -
3	BI_DB+	Bi-directional pair B +
4	BI_DC+	Bi-directional pair C +
5	BI_DC-	Bi-directional pair C -
6	BI_DB-	Bi-directional pair B -
7	BI_DD+	Bi-directional pair D +
8	BI_DD-	Bi-directional pair D -



## Appendix B – Specifications

HARDWARE SPECIFICATIONS	
Main CPU	RTL8685FB
Line Driver	RTL8275-VS
Flash	NAND Flash: 128M Byte
RAM	DDR2: 128M Byte
Interfaces	A / VDSL (35b) x 1 Gigabit Ethernet LAN x 1
LED Indicators	Power, GE, DSL, Internet
Button	Power Switch, Reset button
Power Input	12DVC/1A, 100-240ACV, 50/60Hz
ADVANCED FEATURES	
Safe & Secure Connections	Stateful Firewall (with DoS protection) and NAT/PAT
Management Function	TR-069 (TR-181(in future), TR-369(in future)), HTTP, HTTPS, TELNET, SSH
ENVIRONMENT	
Temperature	Operating: 0°C ~ 40°C (32°F ~104°F) Storage: -40°C ~ 70°C (-40°F ~158°F)
Humidity (Non-condensing)	Operating: 10 ~ 90% RH, non-condensing Storage: 5 ~ 90% RH, non-condensing

## Appendix C - SSH Client

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

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

To access the ssh client you must first enable SSH access for the LAN or WAN from the Admin → ACL in the web user interface.

To access the router using the Linux ssh client

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

For WAN access, type: `ssh -l root WAN IP address`

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

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

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

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

## Appendix D – Wall Mounting

To wall mount this device, use the dimensions below to identify and mark correct screw positions on the selected location.

