COMTREND

VR-3047eu

Home Gateway

User Manual

Version A1.0, March 22 2021

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.
- 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:

- 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.
- If this Home Gateway Router cause harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
- 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.
- If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this equipment does not disable the alarm equipment. If you are unsure, consult your telephone company or a qualified installer.

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, 1.5A
USB: 5Vdc, 0.5A

Certification

- CE standard
  EN 55032 / EN 55024 / EN 55035
  EN 300 328
  EN 301 893
  EN 301 489-1 / EN 301 489-17
  ETSI ES 203 021
  EN 60950-1 / EN 62368-1
  EN 50564

Copyright

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
2.1.1 Back Panel 8
2.1.2 Front Panel 10

CHAPTER 3 WEB USER INTERFACE 12
3.1 DEFAULT SETTINGS 12
3.2 IP CONFIGURATION 13
3.3 LOGIN PROCEDURE 15

CHAPTER 4 STATUS 17
4.1 DEVICE 17
4.2 IPV6 18
4.3 LAN PORT 19

CHAPTER 5 LAN 20

CHAPTER 6 WLAN 21
6.1 WLAN0 (5GHZ) – BASIC SETTINGS 21
6.2 WLAN0 (5GHZ) – ADVANCED SETTINGS 22
6.3 WLAN0 (5GHZ) – SECURITY 24
6.4 WLAN0 (5GHZ) – ACCESS CONTROL 25
6.5 WLAN0 (5GHZ) – WPS 26
6.6 WLAN0 (5GHZ) – STATUS 27
6.7 WLAN0 (2.4GHZ) – BASIC SETTINGS 28
6.8 WLAN0 (2.4GHZ) – ADVANCED SETTINGS 29
6.9 WLAN0 (2.4GHZ) – SECURITY 31
6.10 WLAN0 (2.4GHZ) – ACCESS CONTROL 32
6.11 WLAN0 (2.4GHZ) – WPS 33
6.12 WLAN0 (2.4GHZ) – STATUS 34

CHAPTER 7 WAN 35
7.1 WAN MODE 35
7.2 ETHERNET WAN 36
7.3 PTM WAN 37
7.4 ATM WAN 38
7.5 ATM SETTINGS 39
7.6 DSL SETTINGS 40
7.7 3G SETTINGS 41

CHAPTER 8 SERVICES 43
8.1 DHCP 43
8.2 VLAN ON LAN 45
8.3 DNS – DYNAMIC DNS 46
8.4 FIREWALL 47
8.4.1 IP/Port Filtering 47
8.4.2 MAC Filtering 48
8.4.3 Port Forwarding 49
8.4.4 URL Blocking 50
8.4.5 Domain Blocking 51
8.4.6 DMZ 52
8.5 UPNP 53
8.6 RIP 54
8.7 DMS 55
8.8 SAMBA 56

CHAPTER 9 ADVANCED 57
9.1 ARP TABLE 57

9.2 BRIDGING 58
9.3 ROUTING 59
9.4 SNMP 60
9.5 IPQOS 61
9.5.1 QoS Policy *61*
9.5.2 QoS Classification *62*
9.6 OTHERS 64
9.7 IPV6 65
9.7.1 IPv6 ..... *65*
9.7.2 RADVD *66*
9.7.3 DHCPv6 ..... *67*
9.7.3.1 DHCPv6 – DHCP Server (Auto) *68*
9.7.3.2 DHCPv6 – NONE *69*
9.7.3.3 DHCPv6 – DHCP Relay *69*
9.7.3.4 DHCPv6 – DHCP Server (Manual) *70*
9.7.4 MLD Proxy *72*
9.7.5 MLD Snooping *73*
9.7.6 IPv6 Routing *74*
9.7.7 IP/Port Filtering *75*
9.8 DIAGNOSTICS 76
9.8.1 Ping *76*
9.8.2 ATM Loopback *77*
9.8.3 DSL Tone *78*
9.9 IPV6 79
9.9.1 Commit/Reboot *79*
9.9.2 Backup/Restore *80*
9.9.3 System Log *81*
9.9.4 Password *82*
9.9.5 Firmware Upgrade *83*
9.9.6 ACL *84*
9.9.7 Time Zone *85*
9.9.8 TR-069 ..... *86*
9.10 STATISTICS 88
9.10.1 Interface *88*
9.10.2 DSL *89*

APPENDIX A - PIN ASSIGNMENTS 91

APPENDIX B – SPECIFICATIONS 92

APPENDIX C - SSH CLIENT 94

Chapter 1 Introduction

The VR-3047eu makes full use of its dual band Wi-Fi abilities, reaching speeds of up to 300Mbps on the 2.4GHz band and 867Mbps on the 5GHz band. Enjoy a total speed of up to 1200Mbps to eliminate buffering from your HD streams and lag from online games. The two wireless bands are separated in two dedicated Wi-Fi networks, supporting more devices while reducing signal interference, to deliver a stable connection for every wireless device in your home.

Chapter 2 Installation

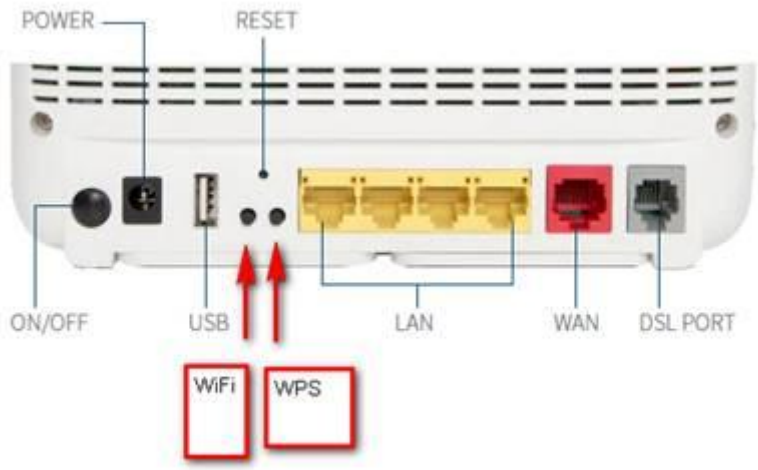
2.1 Hardware Setup

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-3047eu supports the following DSL profiles -
ADSL : ADSL, ADSL 2, ADSL 2+.
VDSL : 8a, 8b, 8c, 8d, 12a, 12b, 17a, 30a and 35b.

WAN PORT
This port is designated to be used for Ethernet WAN functionality only. Use 1000-BASE-T RJ-45 cables to connect to Gigabit WAN server, or 10/100BASE-T RJ-45 cables for standard network usage. This ports is auto-sensing MDI/X; so either straight-through or crossover cable can be used.

LAN (Ethernet) Ports
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 2.1.3 Front Panel for details).

NOTE:	If pressed down for more than 60 seconds, the VR-3047eu 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.

WiFi Button
Press and hold WLAN button more than 2 seconds to enable/disable WiFi.

WPS Button
Press the WPS button to enable WPS which will allow 5 minutes for WiFi connection.

USB Port
This port can be used to connect the router to a storage device. It can only be used for SAMBA(storage) and for a Printer Server. Support for other devices may be added in future firmware upgrades.

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	LED Status	Description
PWR	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 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.
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. If the IP or PPPoE session is dropped due to an idle timeout, the light will remain Blue.
		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.)
DSL	Green	On	xDSL (DSL0) Link is established.
		Off	xDSL (DSL0) Link is established.
		Blink	xDSL (DSL0) Link is training.
WAN	GREEN	On	xDSL Link is established
		Blink	xDSL Link is training or xDSL Link is not established

LAN 1-4	GREEN	On	Ethernet connected
		Off	Ethernet not connected
		Blink	Ethernet is transmitting/receiving
WiFi 2.4G	GREEN	On	(2.4G) Wi-Fi enabled
		Off	(2.4G) Wi-Fi disabled
		Blink	(2.4G) Wi-Fi is transmitting/receiving
WiFi 5G	GREEN	On	(5G) Wi-Fi enabled
		Off	(5G) Wi-Fi disabled
		Blink	(5G) Wi-Fi is transmitting/receiving
WPS	GREEN	On	WPS connection successful. The LED will stay on during 3 minutes
		Off	No WPS association process ongoing
		Slow Blink	WPS connection in progress
		Fast Blink	WPS connection unsuccessful. The LED will keep blinking for 30 sec.
USB	GREEN	On	At least one device is connected to any USB ports
		Off	No device is connected to the any USB ports or a device is connected to any USB port but not active
		Blink	Data TX/RX through at least one of the USB ports

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**)
- User access (username: **user**, password: **user**)
- 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-3047eu powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

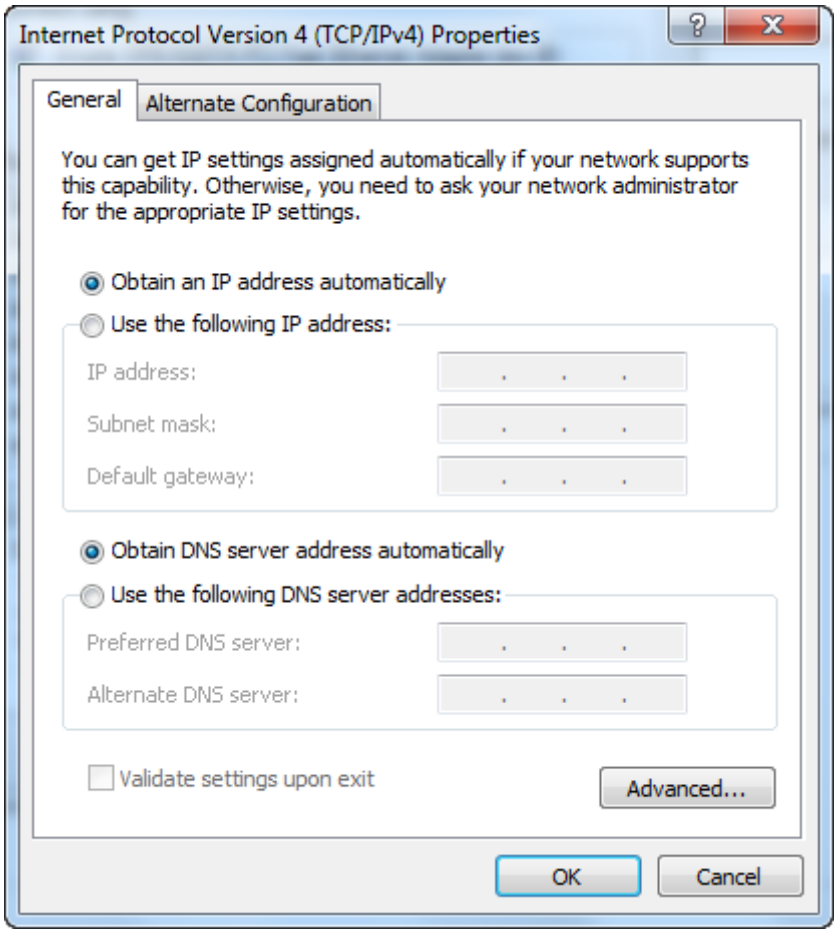
To obtain an IP address from the DCHP server, follow the steps provided below.

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

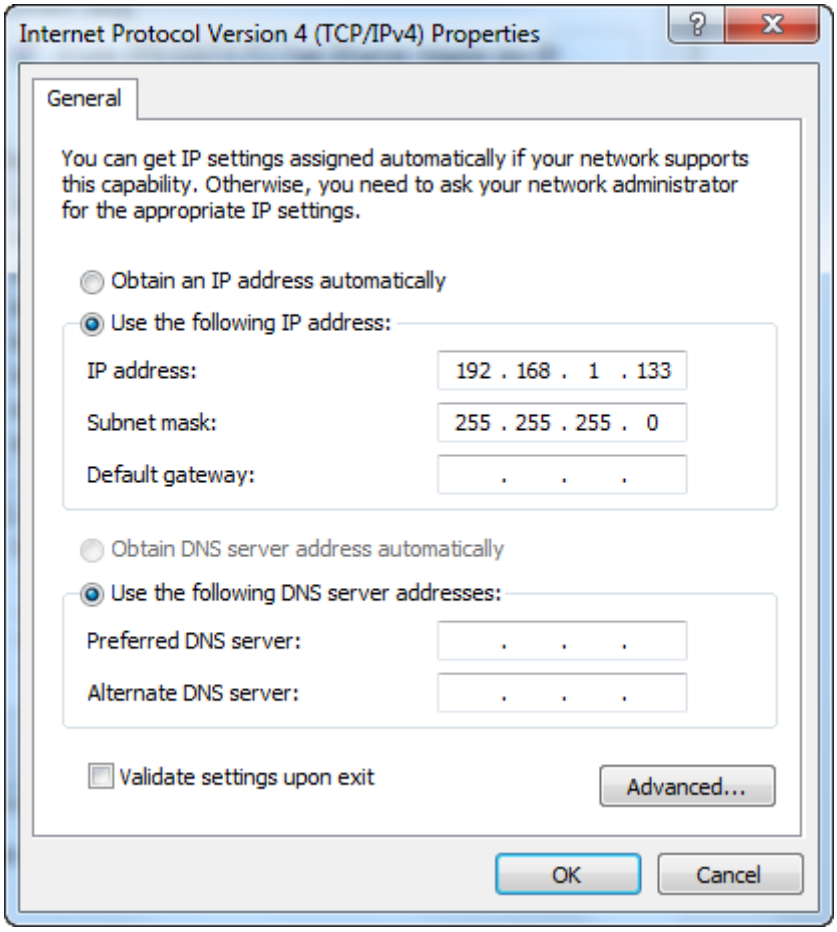
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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.

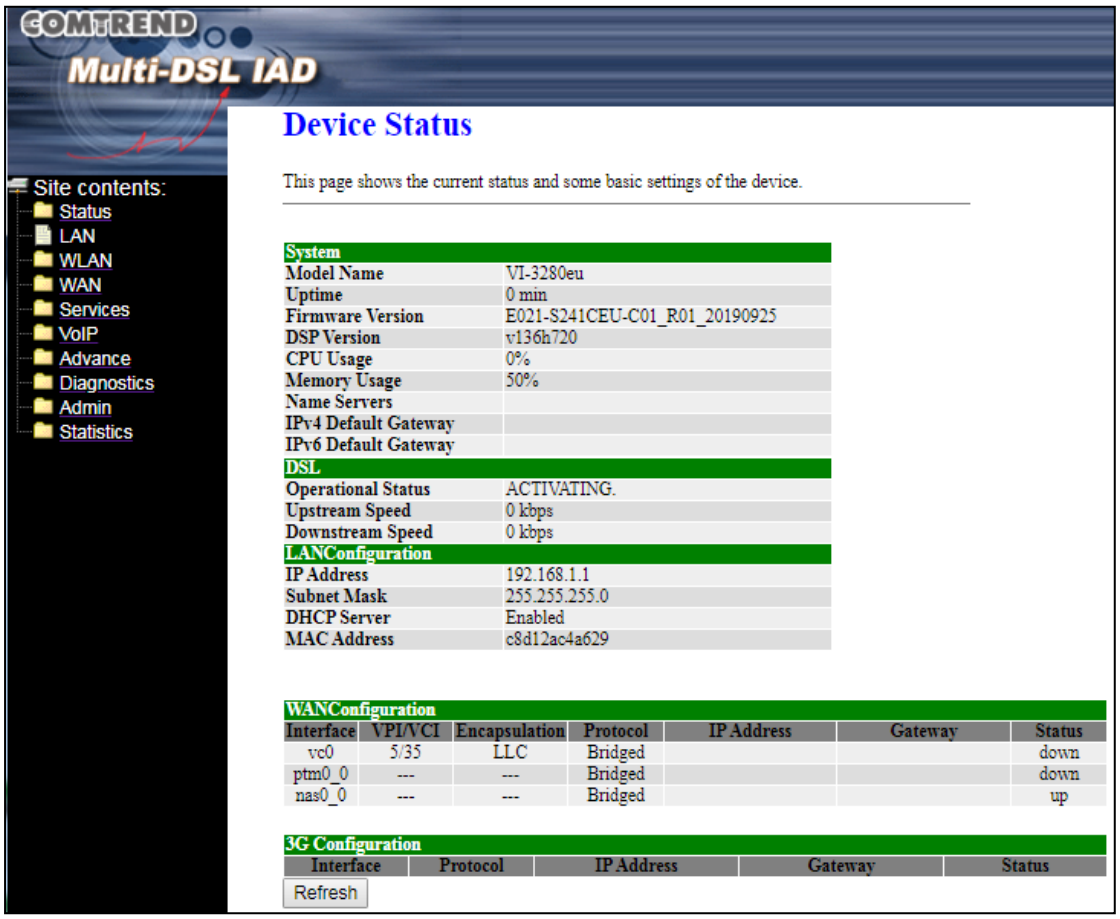
NOTE:	For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device.

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 10.9.4 Password).

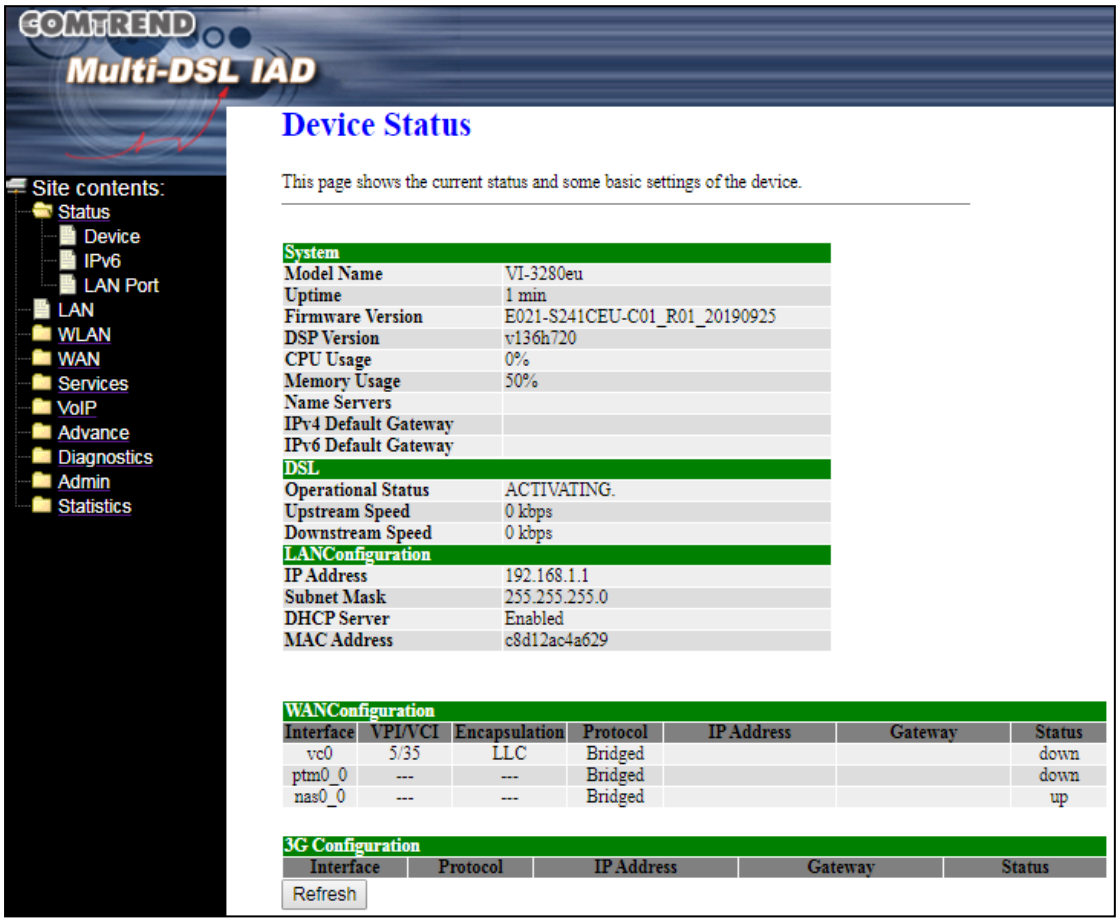
STEP 3: After successfully logging in for the first time, you will reach this screen.



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.

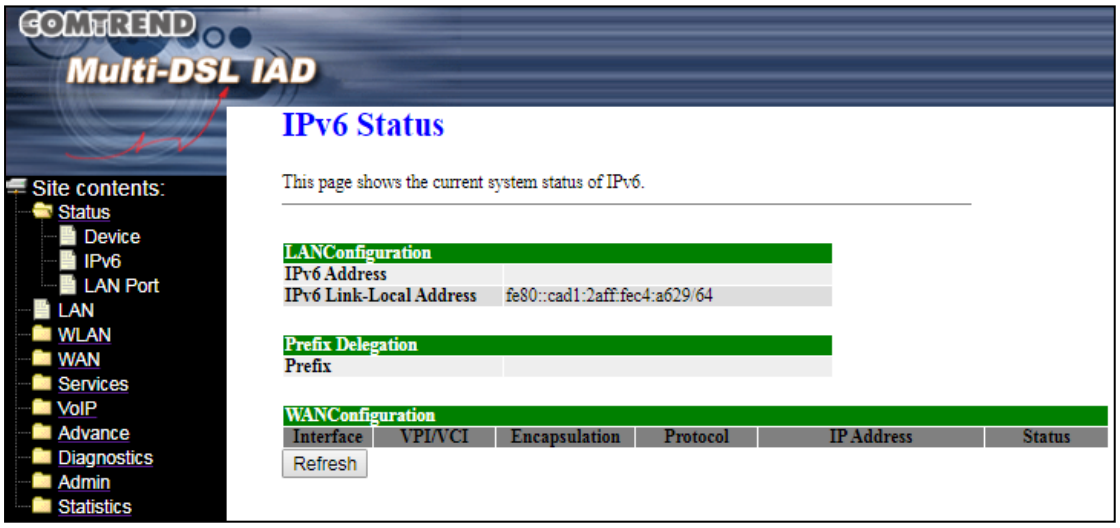


View the DSL, LAN/WAN and 3G settings and other related information.

NOTE: The menu items shown are based upon the configured connection(s) and user account privileges. For example, user account has limited access to configuration modification.

4.2 IPv6

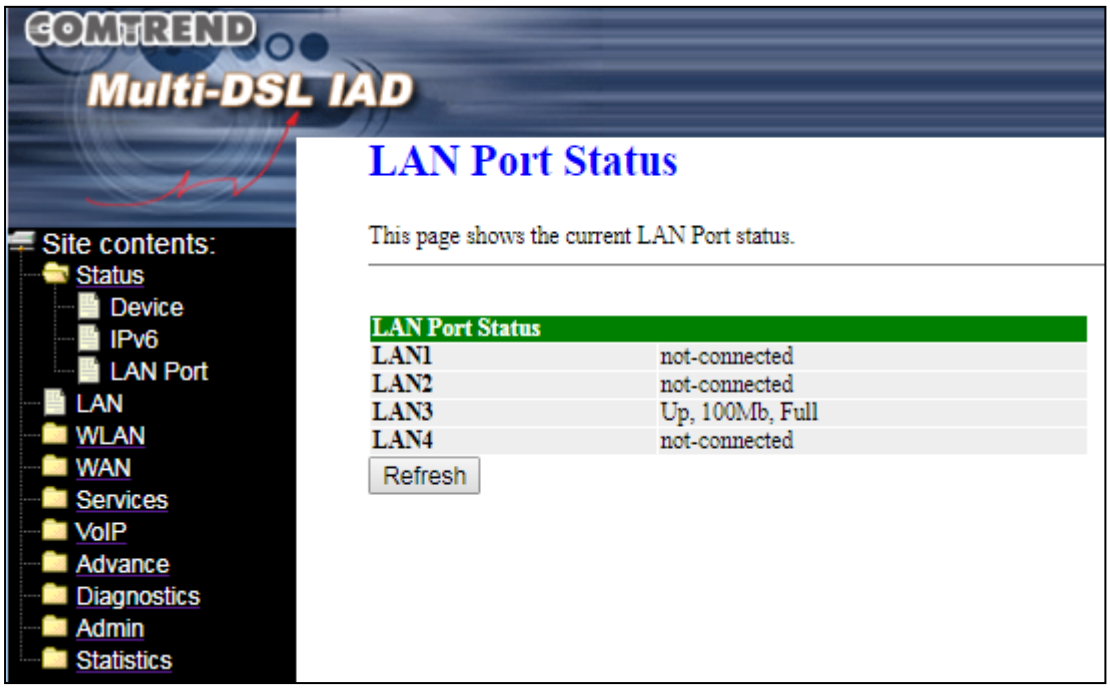
This page shows the current system status of IPv6.



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

4.3 LAN Port

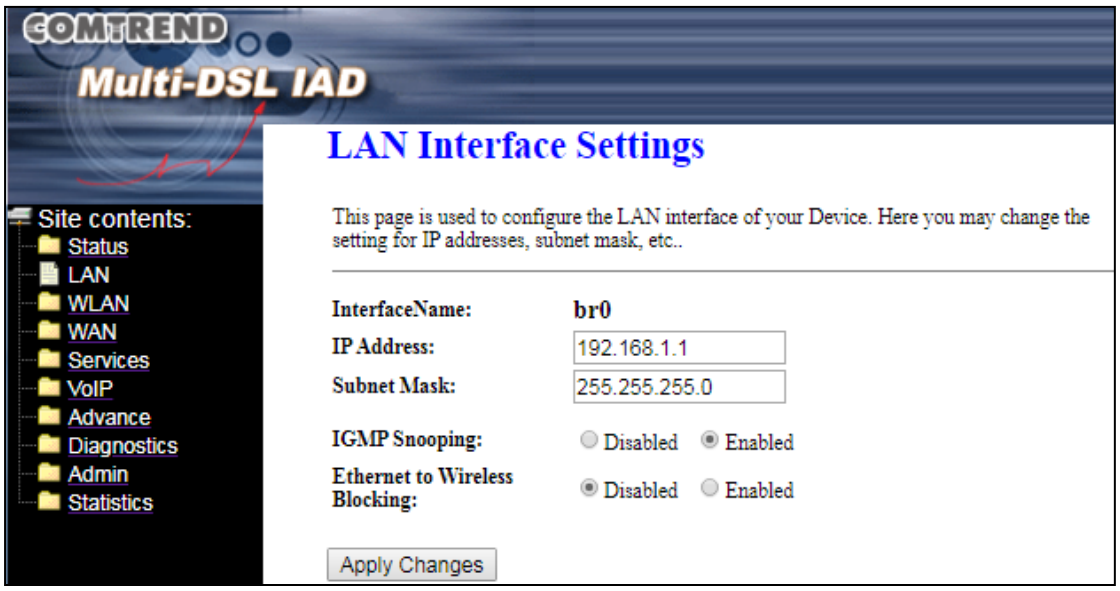
This page shows the current LAN Port status.



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.



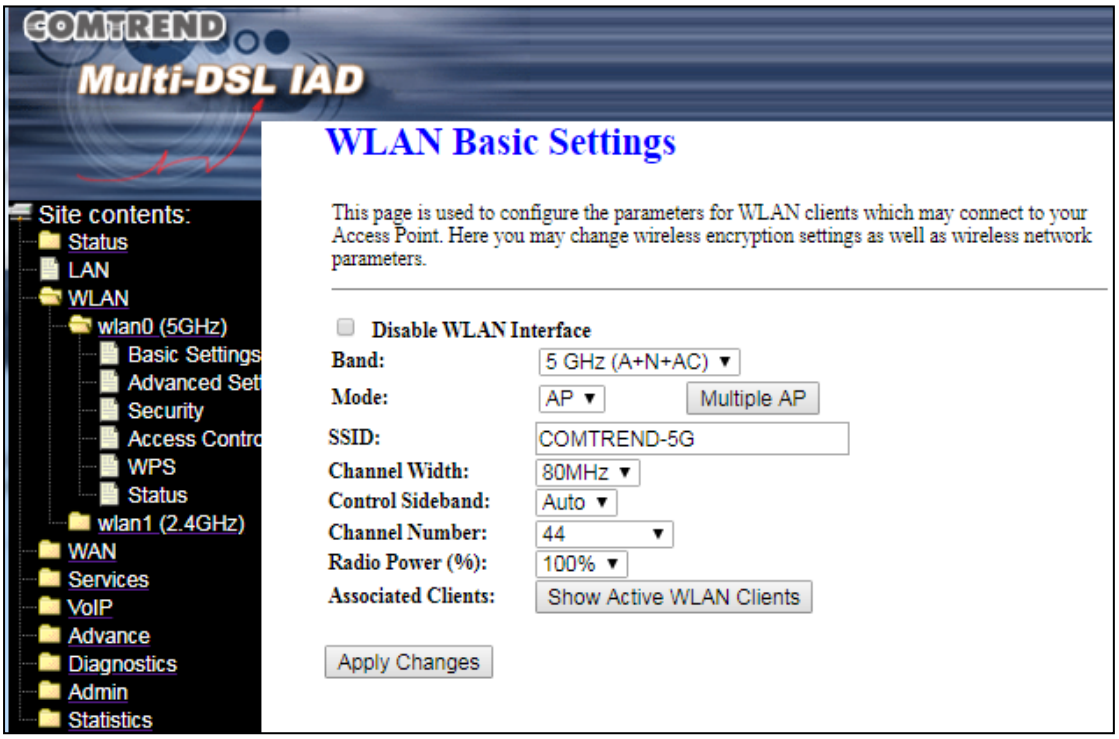
Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Interface Name	The name of the LAN interface
IP Address	The IP address of the LAN interface
Subnet Mask	The subnet mask of the LAN interface
IGMP Snooping	Enable/Disable by selecting the appropriate radio button
Ethernet to Wireless Blocking	Enable/Disable by selecting the appropriate radio button

Chapter 6 WLAN

6.1 wlan0 (5GHz) – Basic Settings

This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

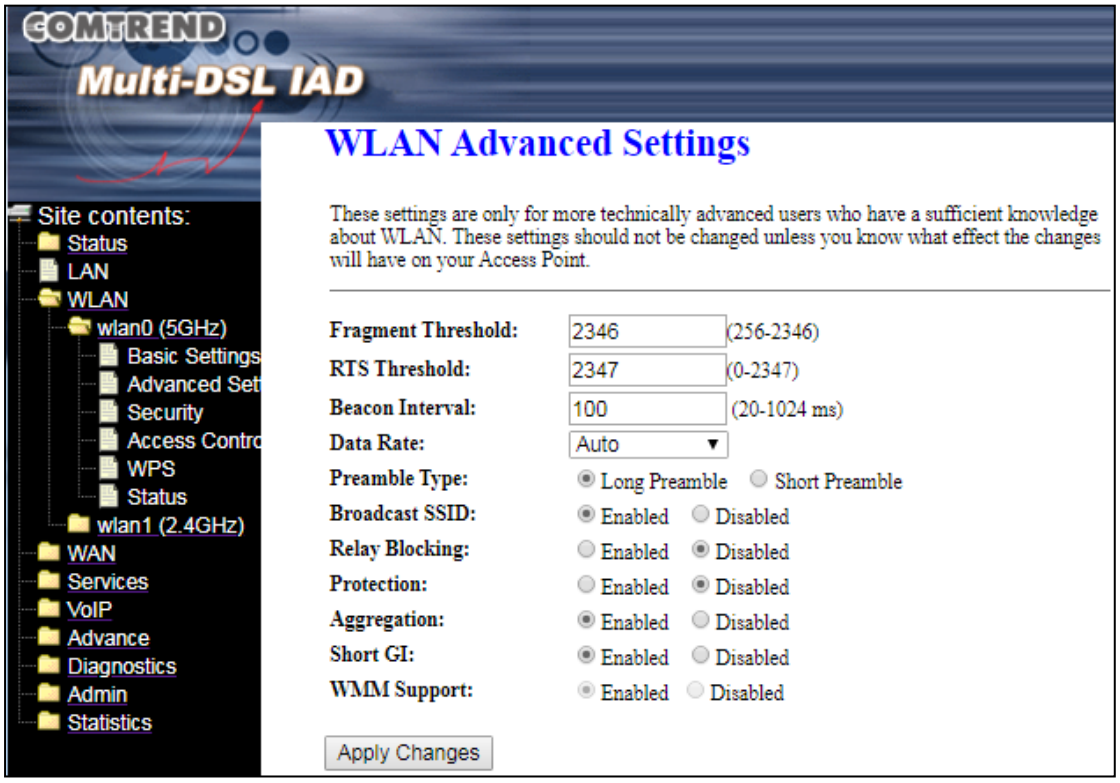


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Disable WLAN Interface	Disable the WLAN interface by ticking the checkbox
Band	Select the band from the drop-down menu
Mode	Select the mode from the drop-down menu
SSID	Lists which SSID of the modem that the stations connect to
Channel Width	Select the channel width from the drop-down menu
Control Sideband	Select from the drop-down menu Displays the control sideband status if channel is on "Auto". Select the desired sideband to adjust the channel list if the current channel is on a specific channel.
Channel Number	Drop-down menu that allows selection of a specific channel
Radio Power	Select the radio power percentage from the drop-down menu
Associated Clients	Click the "Show Active WLAN Client" to show authenticated wireless stations and their status

6.2 wlan0 (5GHz) – Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



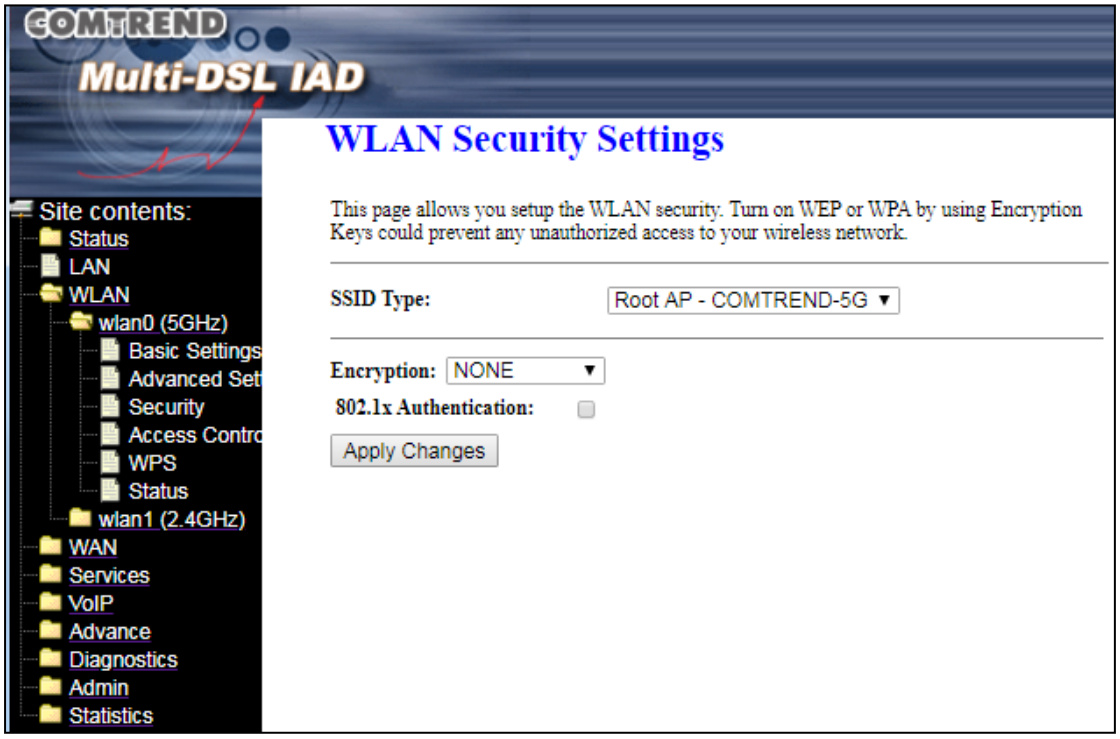
Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance. ***Do not modify the default value if you don't know what it is, default value is 2346.***

Field/Header	Description
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold. ***Do not modify the default value if you don't know what it is, default value is 2347.***
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 20-1024. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). ***Do not modify the default value if you don't know what it is, default value is 100.***
Data Rate	Select from the drop-down menu. The rate of date transmission should be set depending on the speed of your wireless network. The default setting is Auto.
Preamble Type	Select the preamble type depending on your needs. This parameter defines the length of the CRC block sent by the router when communicating to wireless devices. Select a value from the drop-down list. Short Preamble is recommended for networks with high-volume traffic.
Broadcast SSID	Select Disabled to hide the SSID so that a station cannot obtain the SSID through passive scanning. Select Enabled to make the SSID visible so a station can obtain the SSID through passive scanning.
Relay Blocking	When Relay Blocking is enabled, wireless clients will not associate with other wireless clients
Protection	Click to enable or disable the Management Frame Protection
Aggregation	Frame aggregation is a feature of the IEEE 802.11e, 802.11n and 802.11ac wireless LAN standards that increases throughput by sending two or more data frames in a single transmission. Select the enabled or disabled radio button.
Short GI	Enable/Disable use of short guard interval
WMM Support	Helps with different kinds of traffics such as video, voice, and background services

6.3 wlan0 (5GHz) – Security

This page allows you setup the WLAN security. Turning on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

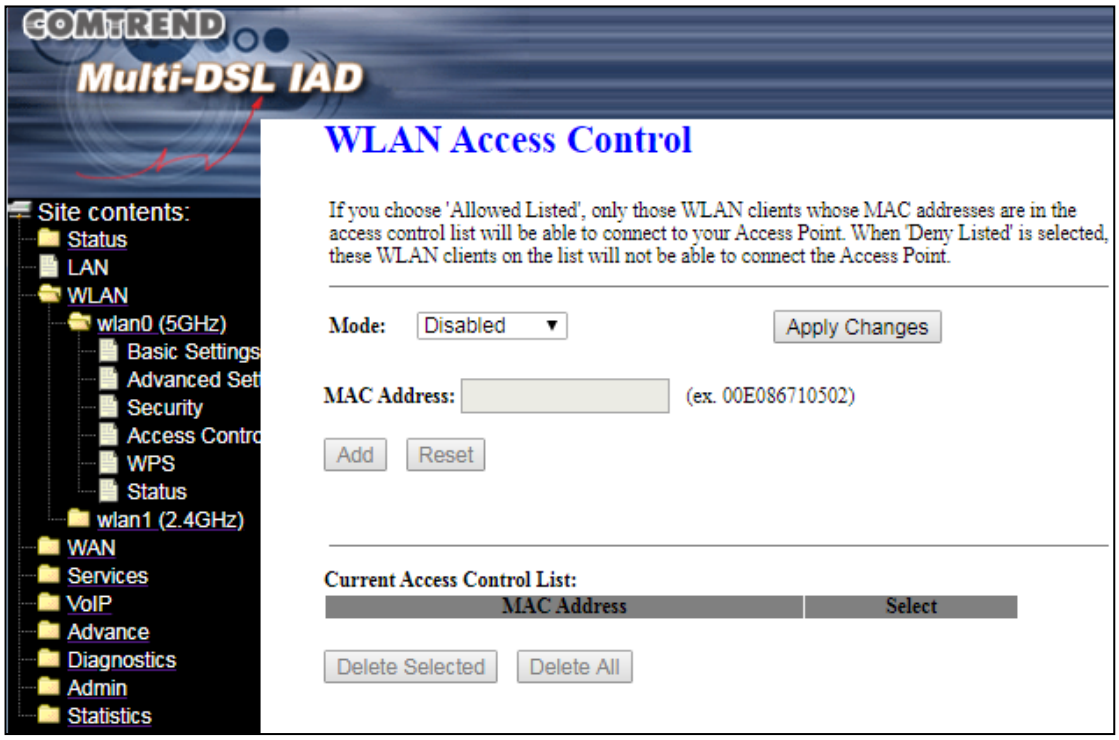


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
SSID Type	Select the service set identifier type from the drop-down menu
Encryption	Select the encryption type from the drop-down menu. They are 4 types of security to be selected. To secure your WLAN, it is strongly recommended to enable this feature. Encryption Types: None, WEP, WPA2, WPA2 Mixed.
802.1x Authentication	Tick the checkbox to enable 802.1x authentication (i.e restrict unauthorized clients from connecting to a LAN through publicly accessible ports)

6.4 wlan0 (5GHz) – Access Control

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

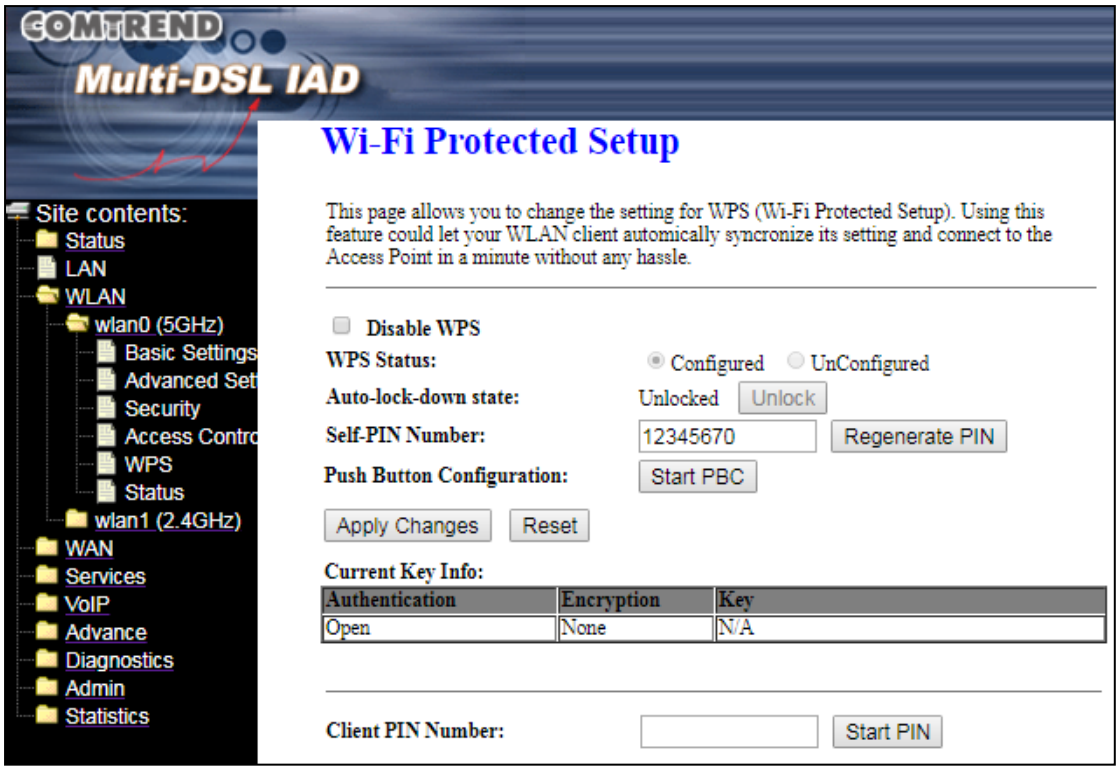


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Mode	Select the mode from the drop-down menu
MAC Address	Please input the MAC address for WLAN access control list

6.5 wlan0 (5GHz) – WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its settings and connect to the Access Point in a minute without any hassle.



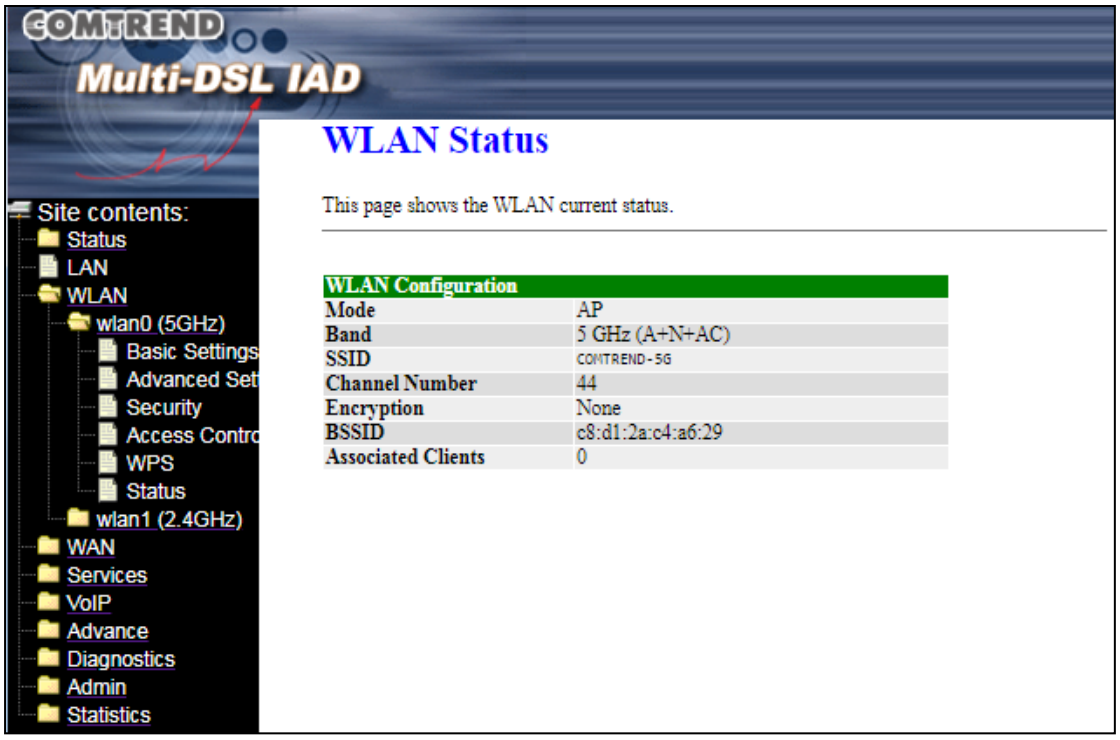
Click the **Apply Changes** button for your changes to take effect.

Click the **Reset** button to reset to the default value.

Field/Header	Description
Disable WPS	Disable WPS by ticking the checkbox
WPS Status	Displays "Configured" or "unConfigured" depending on whether WPS and SSID/security settings for the device have been configured or not, either manually or using the WPS button
Auto-lock-down state	Displays the Auto-lock-down state
Self-PIN Number	This AP itself is the WPS Personal Identification Number
Push Button Configuration	Click "Start PBC" (Push-Button Configuration) to activate the WPS process. WPS will be active for 2 minutes.
Current Key Info	Displays current Wi-Fi Security information
Client PIN Number	Input the wireless client's PIN code here and click "Start PIN" to activate PIN code WPS. Refer to your wireless client's documentation if you are unsure of its PIN code.

6.6 wlan0 (5GHz) – Status

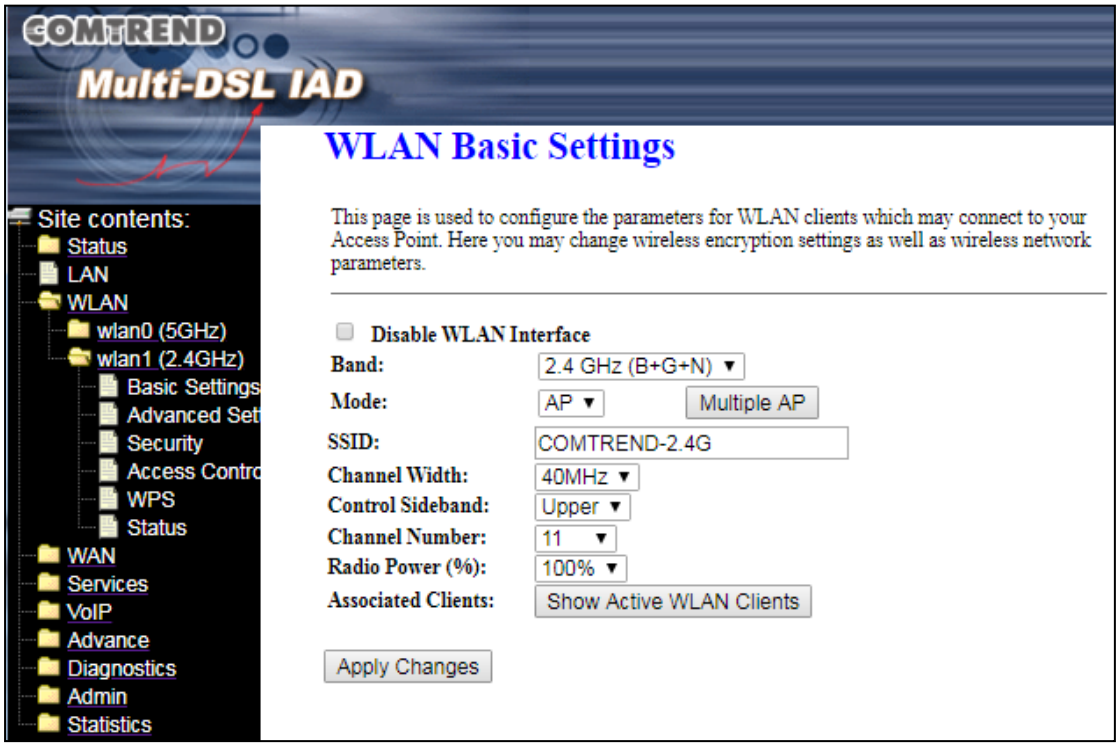
This page shows the WLAN current status.



Field/Header	Description
Mode	Displays the mode for the current WLAN configuration
Band	Displays the band for the current WLAN configuration
SSID	Displays the SSID for the current WLAN configuration
Channel Number	Displays the channel number for the current WLAN configuration
Encryption	Displays the encryption type for the current WLAN configuration
BSSID	Displays the BSSID for the current WLAN configuration
Associated Clients	Display the number of current clients connected to the AP

6.7 wlan0 (2.4GHz) – Basic Settings

This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

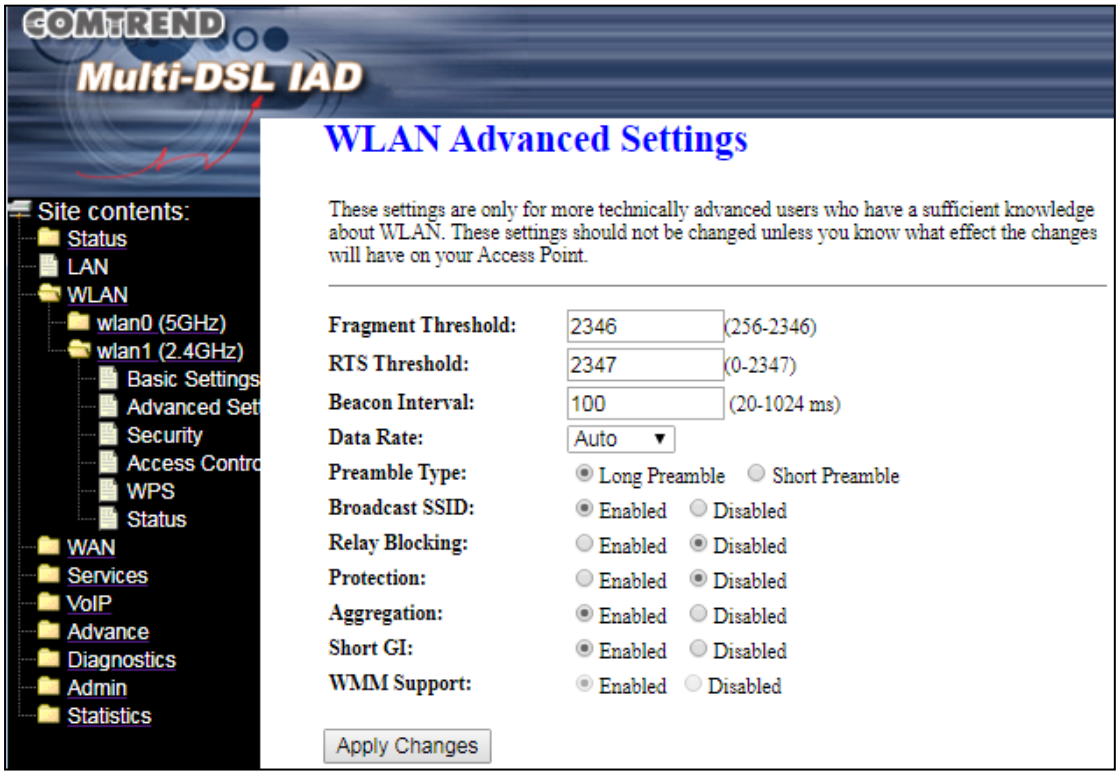


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Disable WLAN Interface	Disable the WLAN interface by ticking the checkbox
Band	Select the band from the drop-down menu
Mode	Select the mode from the drop-down menu
SSID	Lists which SSID of the modem that the stations connect to
Channel Width	Select the channel width from the drop-down menu
Control Sideband	Displays the control sideband status if channel is on "Auto". Select the desired sideband to adjust channel list if the current channel is on a specific channel.
Channel Number	Drop-down menu that allows selection of a specific channel.
Radio Power	Select the radio power percentage from the drop-down menu
Associated Clients	Click the "Show Active WLAN Client" button to show authenticated wireless stations and their status

6.8 wlan0 (2.4GHz) – Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



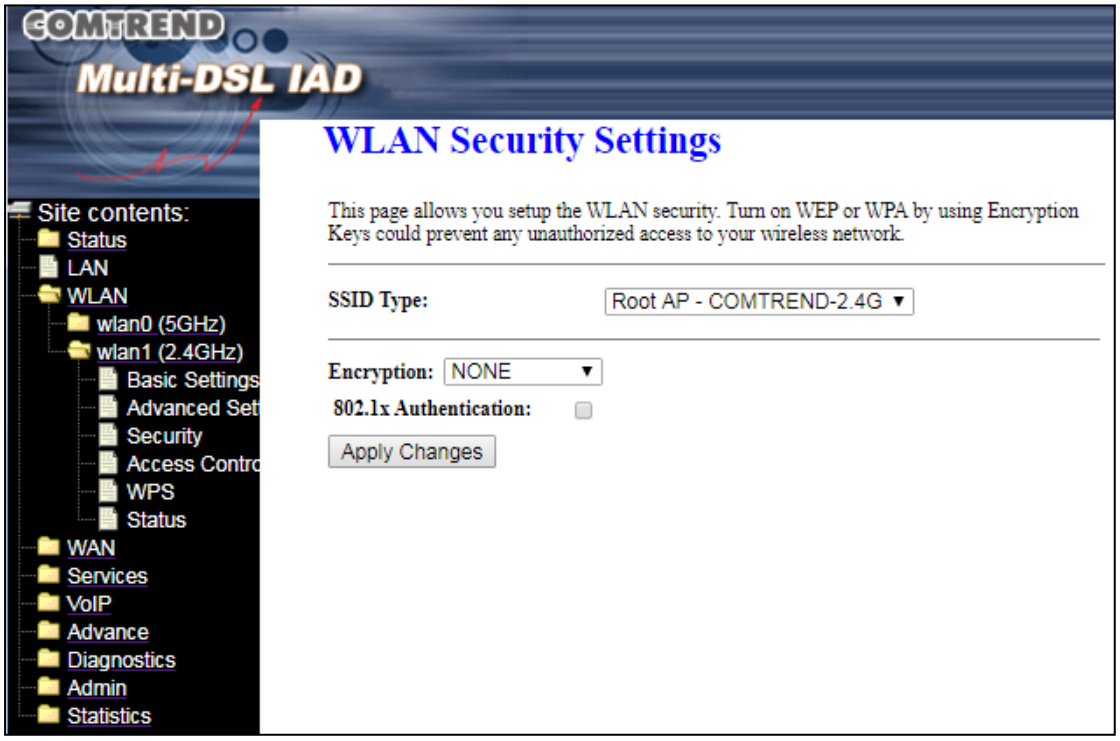
Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance. ***Do not modify the default value if you don't know what it is, default value is 2346.***
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold. ***Do not modify the default value if you don't know what it is, default value is 2347.***

Field/Header	Description
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 2 – 1024. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). ***Do not modify the default value if you don't know what it is, default value is 100.***
Data Rate	Select the data rate from the drop-down menu. The rate of date transmission should be set depending on the speed of your wireless network. The default setting is Auto.
Preamble Type	Select the preamble type depending on your needs. This parameter defines the length of the CRC block sent by the router when communicating to wireless devices. Select a value from the drop-down list. Short Preamble is recommended for networks with high-volume traffic.
Broadcast SSID	Select Disabled to hide the SSID such that a station cannot obtain the SSID through passive scanning. Select Enabled to make the SSID visible so a station can obtain the SSID through passive scanning.
Relay Blocking	When Relay Blocking is enabled, wireless clients will not associate with other wireless clients.
Protection	Click to enable or disable the Management Frame Protection
Aggregation	Frame aggregation is a feature of the IEEE 802.11e, 802.11n and 802.11ac wireless LAN standards that increases throughput by sending two or more data frames in a single transmission. Select the enabled or disabled radio button.
Short GI	Enable/Disable use of short guard interval
WMM Support	Helps with different kind of traffics such as video, voice, and background services

6.9 wlan0 (2.4GHz) – Security

This page allows you setup the WLAN security. Turning on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

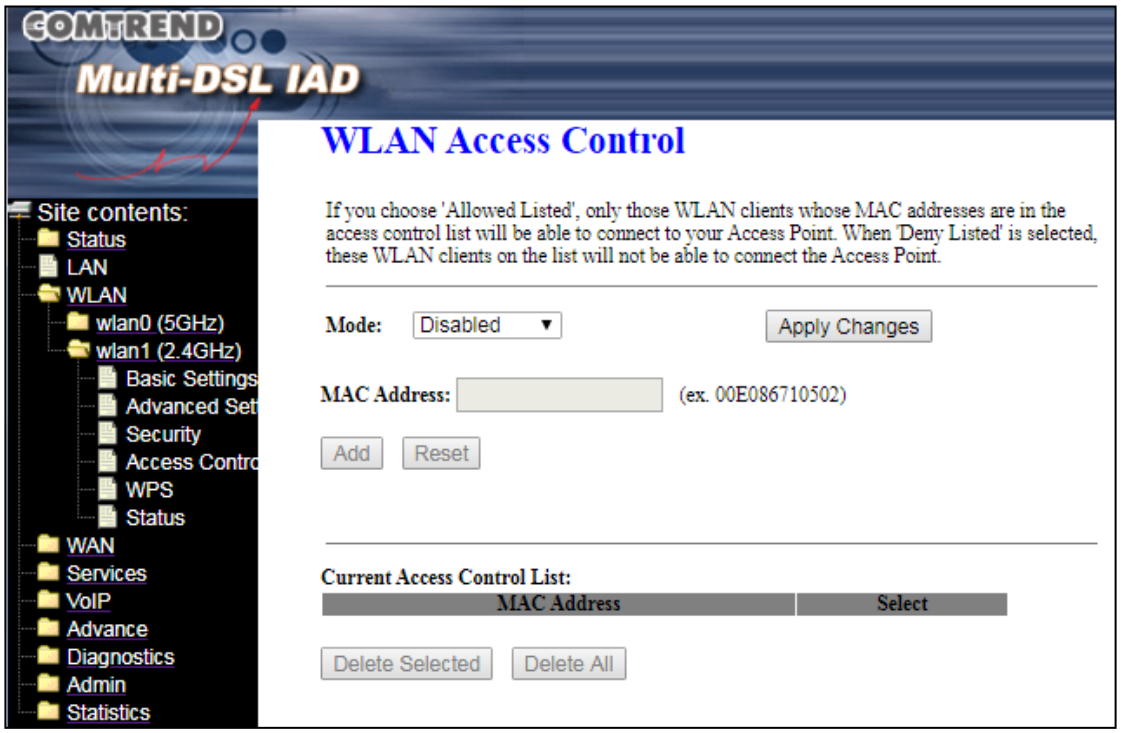


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
SSID Type	Select the SSID type from the drop-down menu
Encryption	Select the encryption type from the drop-down menu. They are 4 types of security to be selected. To secure your WLAN, it is strongly recommended to enable this feature. Encryption Type: None, WEP, WPA2, WPA2 Mixed.
802.1x Authentication	Tick the checkbox to enable 802.1x authentication (i.e. restrict unauthorized clients from connecting to a LAN through publicly accessible ports)

6.10 wlan0 (2.4GHz) – Access Control

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

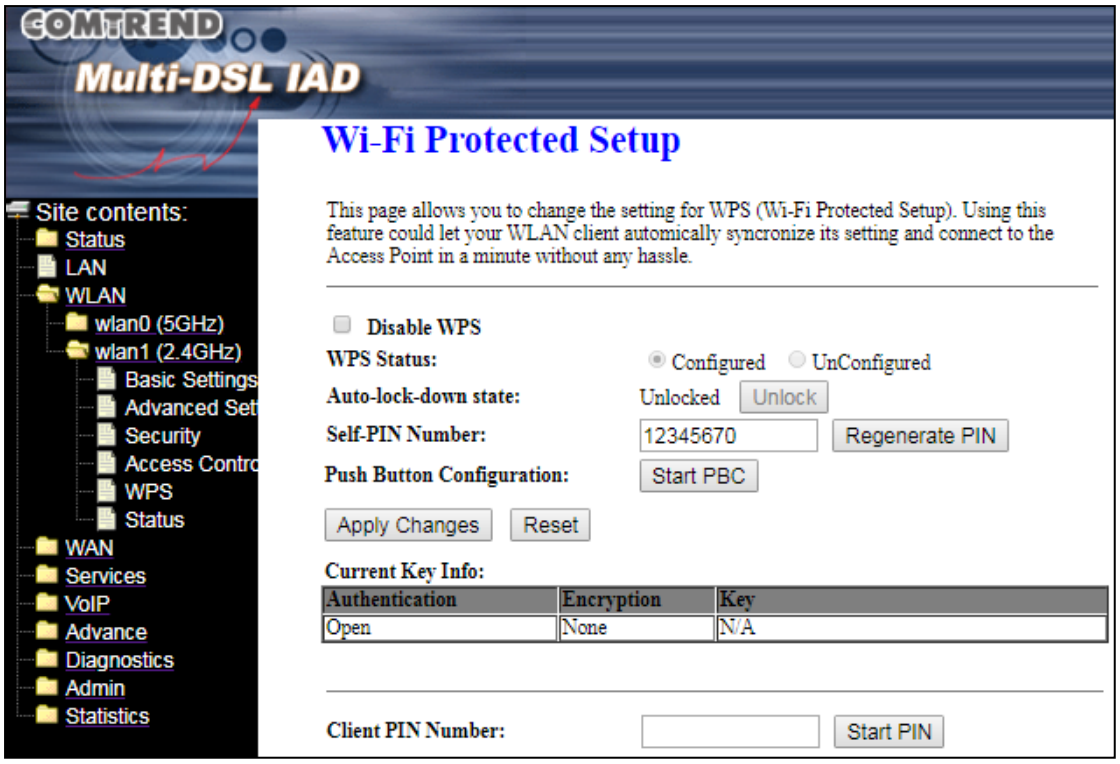


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Mode	Select the mode from the drop-down menu
MAC Address	Input the Client MAC address to be allowed/denied (based on your mode selection)

6.11 wlan0 (2.4GHz) – WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its settings and connect to the Access Point in a minute without any hassle.



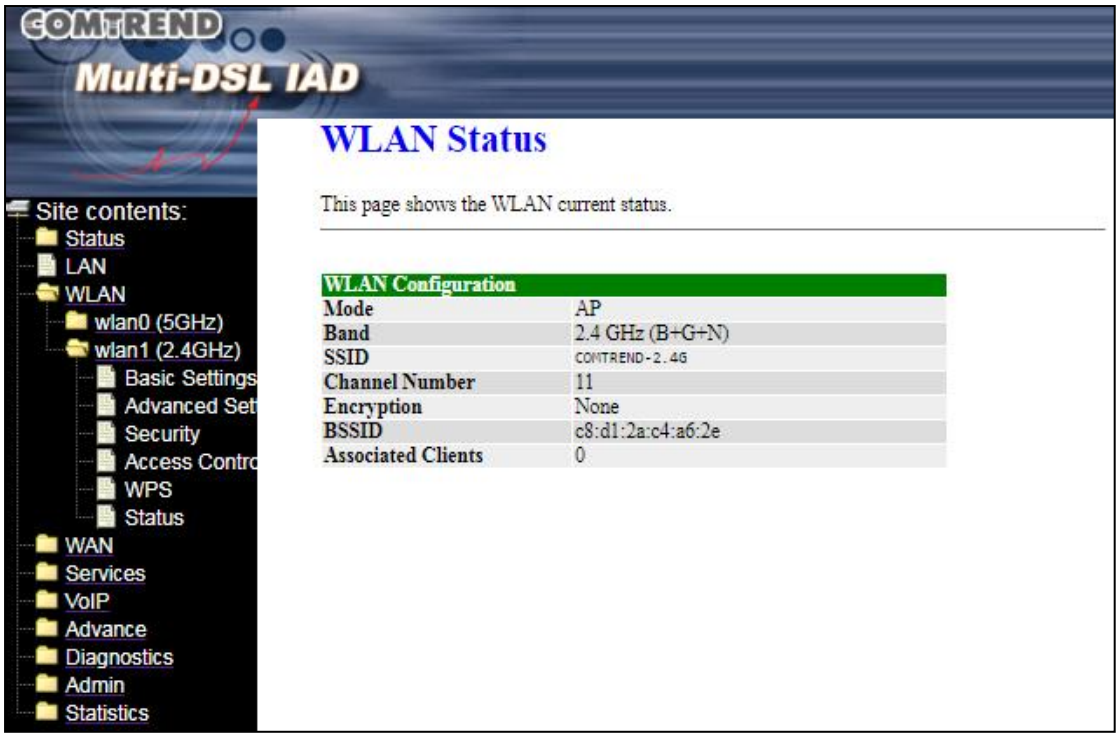
Click the **Apply Changes** button for your changes to take effect.

Click the **Reset** button to reset to default value.

Field/Header	Description
Disable WPS	Disable WPS by ticking the checkbox
WPS Status	Displays "Configured" or "unConfigured" depending on whether WPS and SSID/security settings for the device have been configured or not, either manually or using the WPS button
Auto-lock-down state	Displays the Auto-lock-down state
Self-PIN Number	This AP itself is the WPS Personal Identification Number
Push Button Configuration	Click "Start PBC" (Push-Button Configuration) to activate WPS process. WPS will be active for 2 minutes.
Current Key Info	Displays the current Wi-Fi Security information
Client PIN Number	Input the wireless client's PIN code here and click "Start PIN" to activate PIN code WPS. Refer to your wireless client's documentation if you are unsure of its PIN code.

6.12 wlan0 (2.4GHz) – Status

This page shows the WLAN current status.

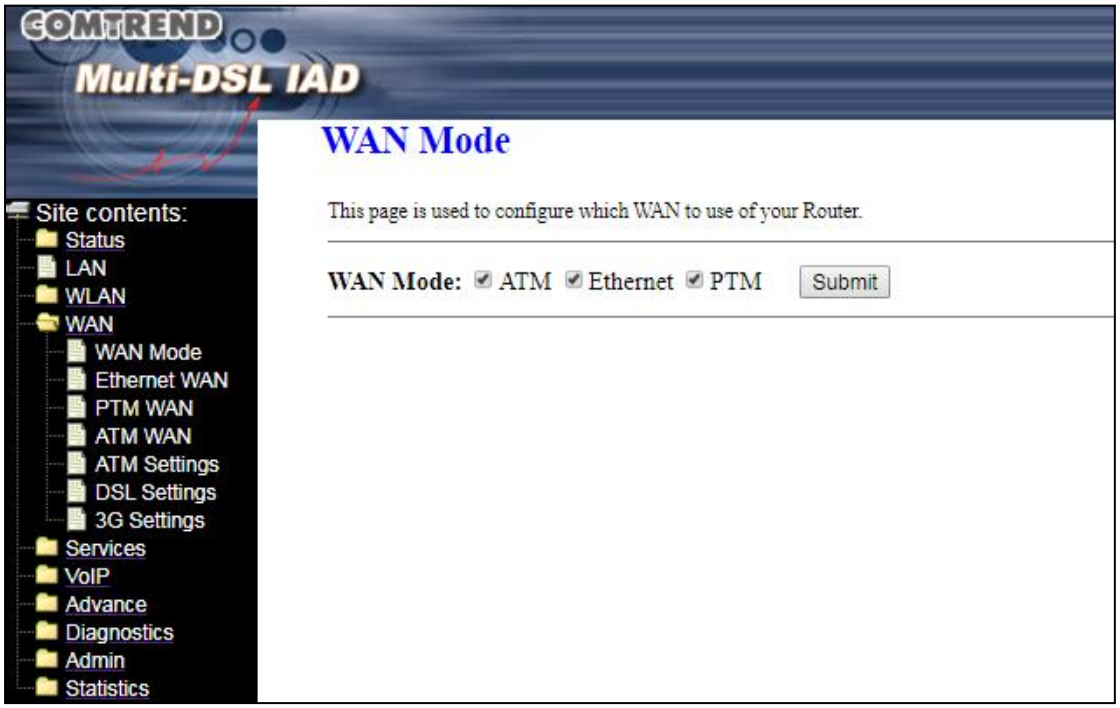


Field/Header	Description
Mode	Displays the mode for the current WLAN configuration
Band	Displays the band for the current WLAN configuration
SSID	Displays the SSID for the current WLAN configuration
Channel Number	Displays the channel number for the current WLAN configuration
Encryption	Displays the encryption type for the current WLAN configuration
BSSID	Displays the BSSID for the current WLAN configuration
Associated Clients	Displays the number of current clients connected to the AP

Chapter 7 WAN

7.1 WAN Mode

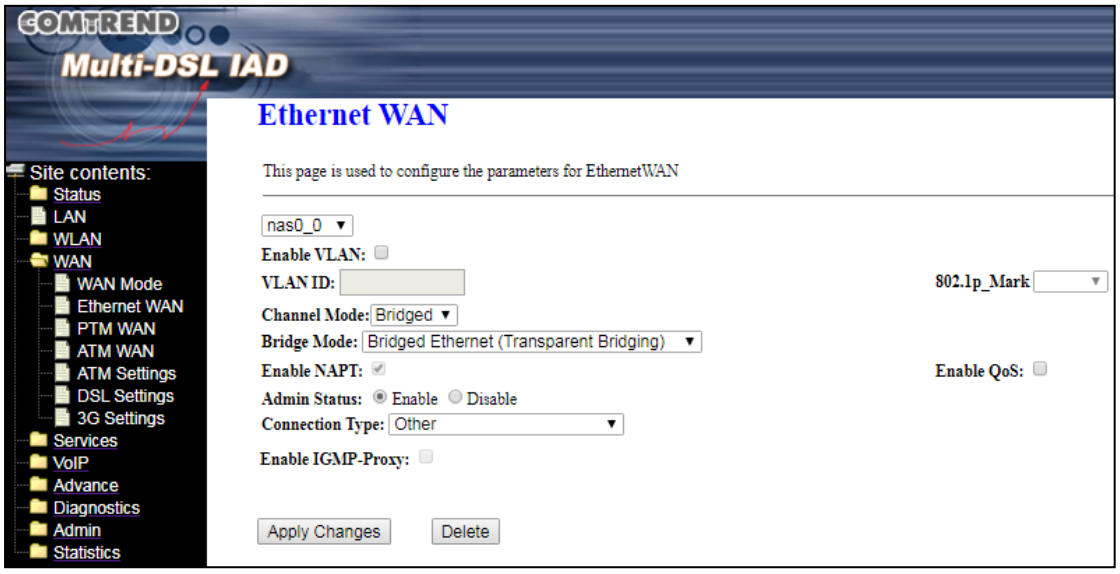
This page is used to configure which WAN to use of your Router.



Tick the checkbox ☑ to select the WAN mode.

7.2 Ethernet WAN

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

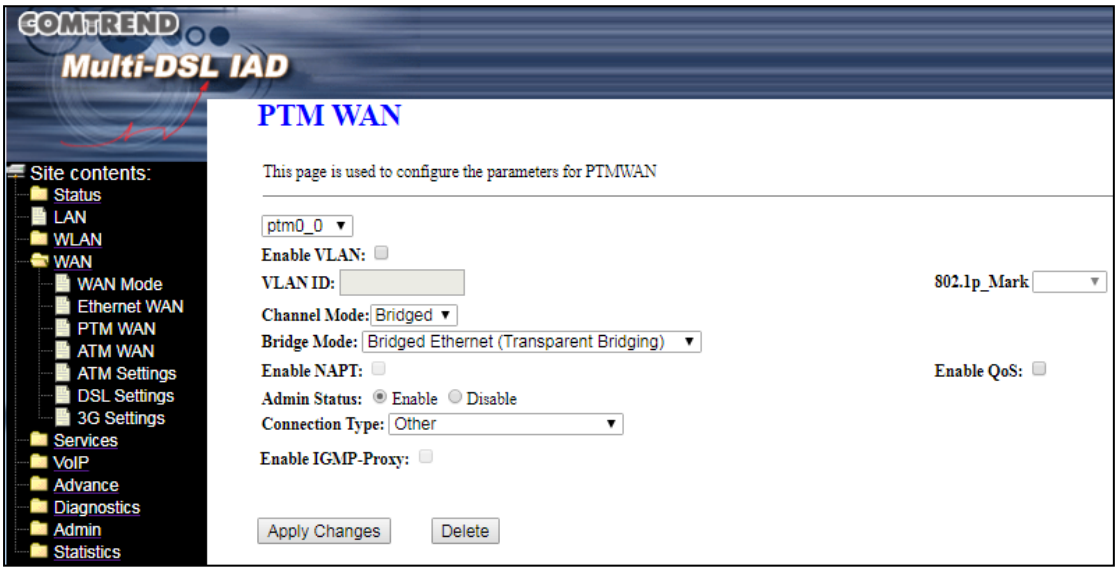


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Enable VLAN	Tick the checkbox to enable VLAN
VLAN ID	Input the VLAN ID
Channel Mode	Select the channel mode from the drop-down menu
Bridge Mode	Select the bridge mode from the drop-down menu
Enable NAPT	Tick the checkbox to enable NAPT
Admin Status	Tick the checkbox to enable or disable this WAN interface
Connection Type	Select the connection type from the drop-down menu
Enable IGMP-Proxy	Tick the checkbox to enable IGMP-Proxy
802.1p_Mark	Select the connection type from the drop-down menu
Enable QoS	Tick the checkbox to enable QoS

7.3 PTM WAN

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

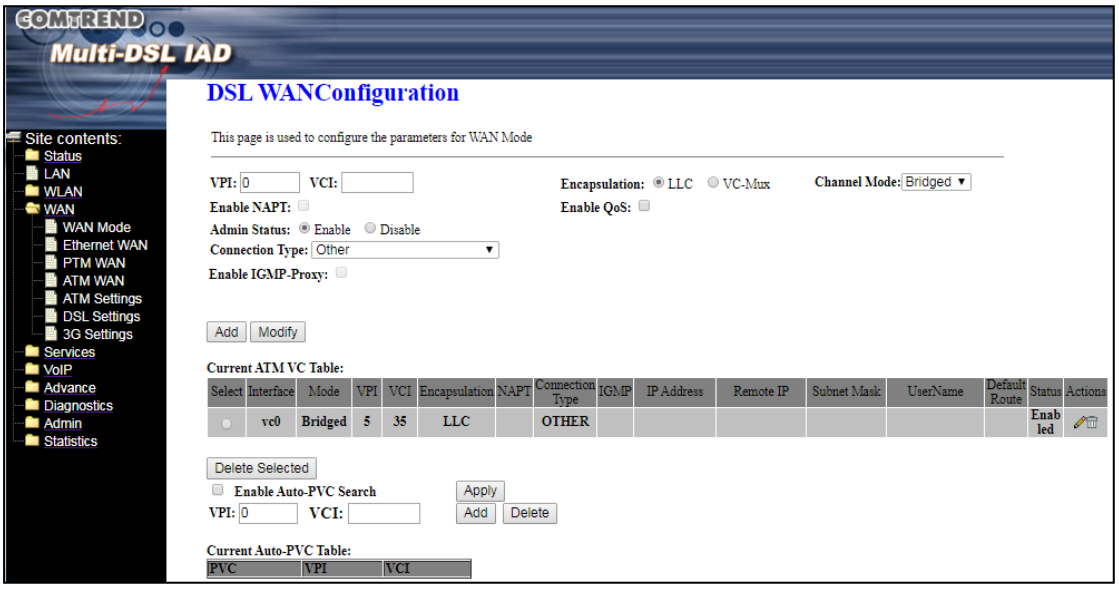


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Enable VLAN	Tick the checkbox to enable VLAN
VLAN ID	Input the VLAN ID
Channel Mode	Select the channel mode from the drop-down menu. **Bridged** – Select this option to use the device as an AP **IPoE** – Select this option if you are connected to the Internet through a cable modem line **PPPoE** – Select this option if you are connected to the Internet through a DSL line **DS-Lite** – Select this option if you are connected to the DS-Lite server **6rd** - Select this option if you are connected to the 6rd server
Bridge Mode	Select the bridge mode from the drop-down menu
Enable NAPT	Tick the checkbox to enable NAPT
Admin Status	Tick the checkbox to enable or disable this WAN interface
Connection Type	Select the connection type from the drop-down menu
Enable IGMP-Proxy	Tick the checkbox to enable IGMP-Proxy
802.1p_Mark	Select the connection type from the drop-down menu
Enable QoS	Tick the checkbox to enable QoS

7.4 ATM WAN

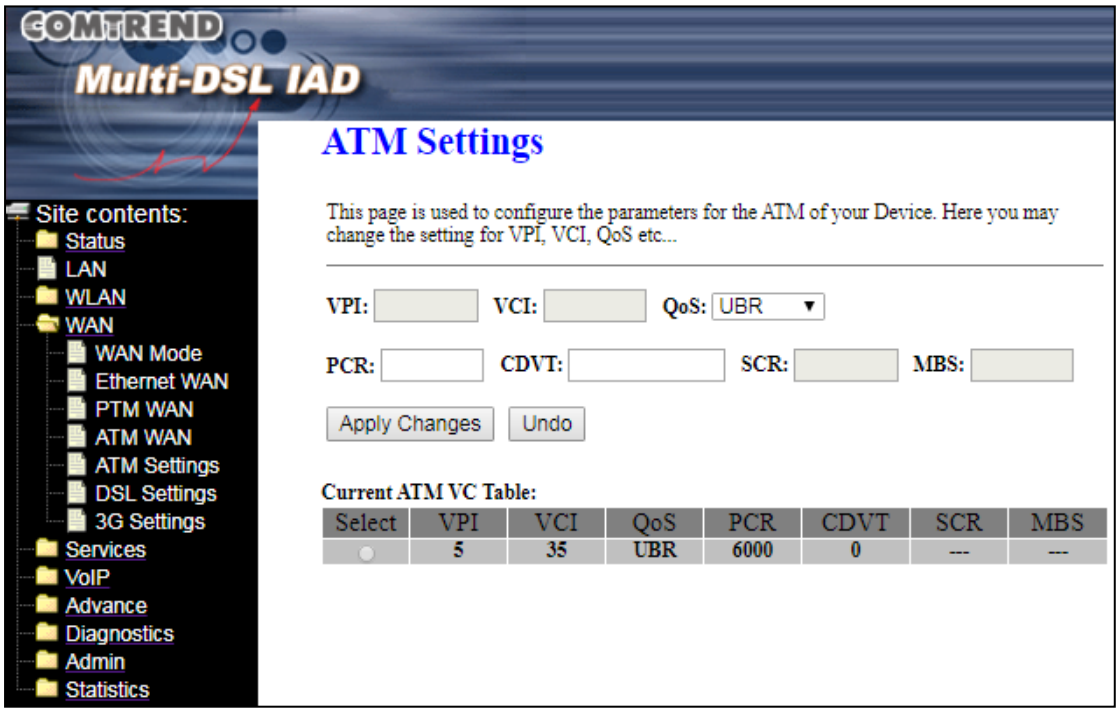
This page is used to configure the parameters for WAN Mode. Your ISP determines the Internet access type that you should use.



Field/Header	Description
VPI/VCI	Input the VPI and VCI values provided by the ISP
Enable NAPT	Tick the checkbox to enable NAPT
Admin Status	Tick the checkbox to enable or disable this WAN interface
Connection Type	Select the connection type from the drop-down menu
Enable IGMP-Proxy	Tick the checkbox to enable IGMP-Proxy
Encapsulation	Select the encapsulation type determined by the ISP
Enable QoS	Tick the checkbox to enable QoS
Channel Mode	Select the channel mode from the drop-down menu. **Bridged** – Select this option to use the device as an AP **IPoE** – Select this option if you are connected to the Internet through a cable modem line **PPPoE** – Select this option if you are connected to the Internet through a DSL line **DS-Lite** – Select this option if you are connected to the DS-Lite server **6rd** - Select this option if you are connected to the 6rd server

7.5 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.

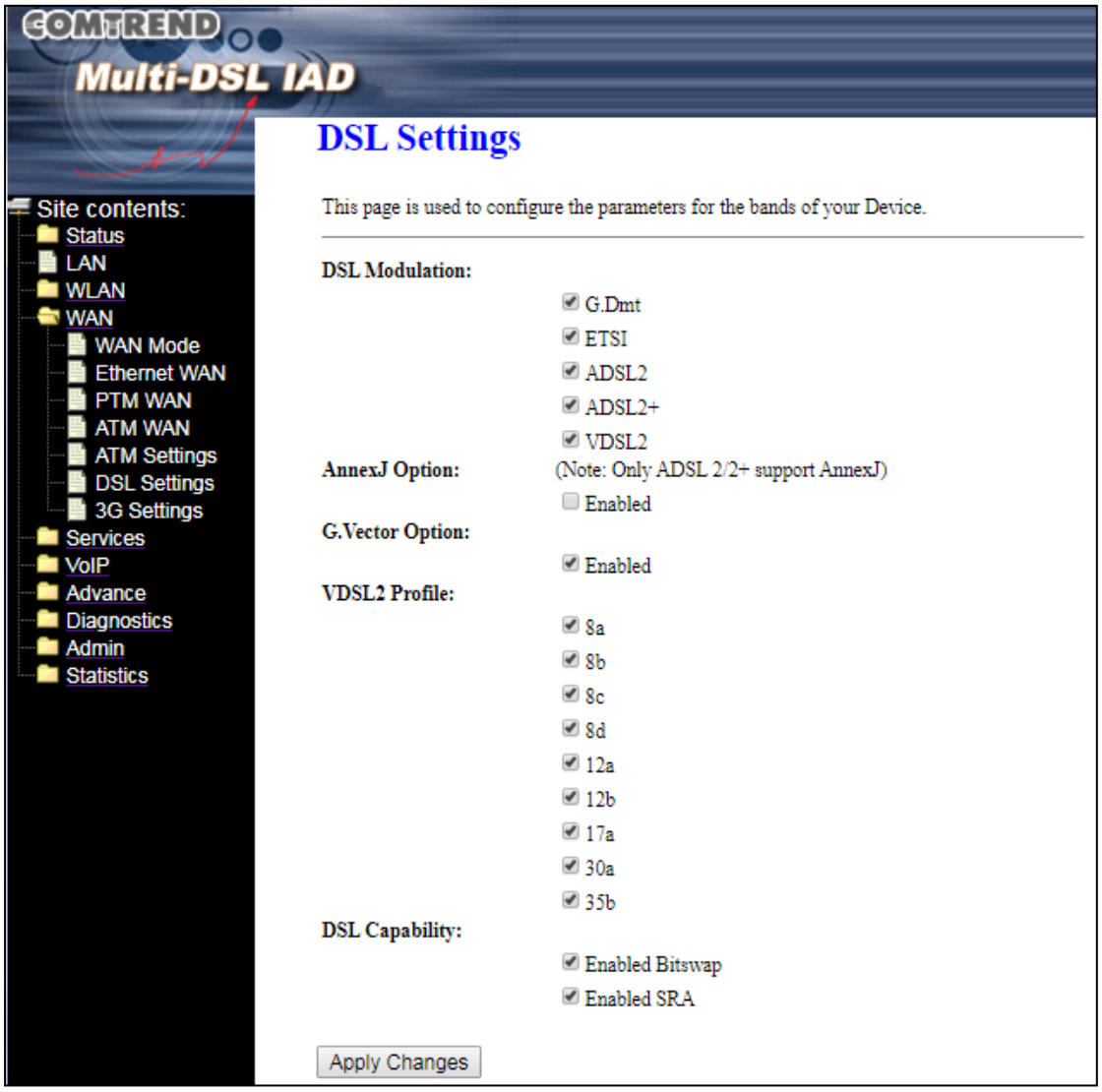


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
QoS	Select 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

7.6 DSL Settings

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

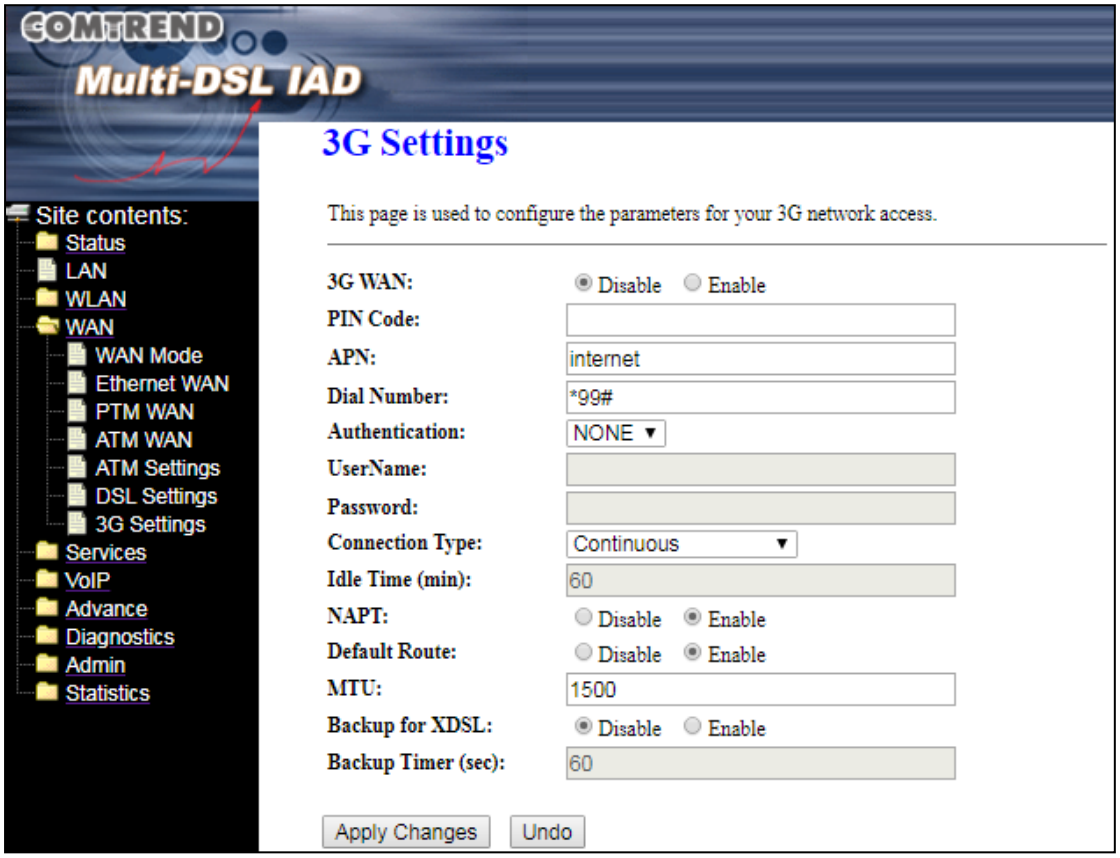


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
DSL Modulation	Tick the checkbox to select DSL modulation
AnnexJ Option	Tick the checkbox to enable Annex J
G.Vector Option	Tick the checkbox to enable G.Vector
VDSL2 Profile	Tick the checkbox to select VDSL profile
DSL Capability	Enables Bitswap and Seamless Rate Adaptation

7.7 3G Settings

This page is used to configure the parameters for your 3G network access.



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

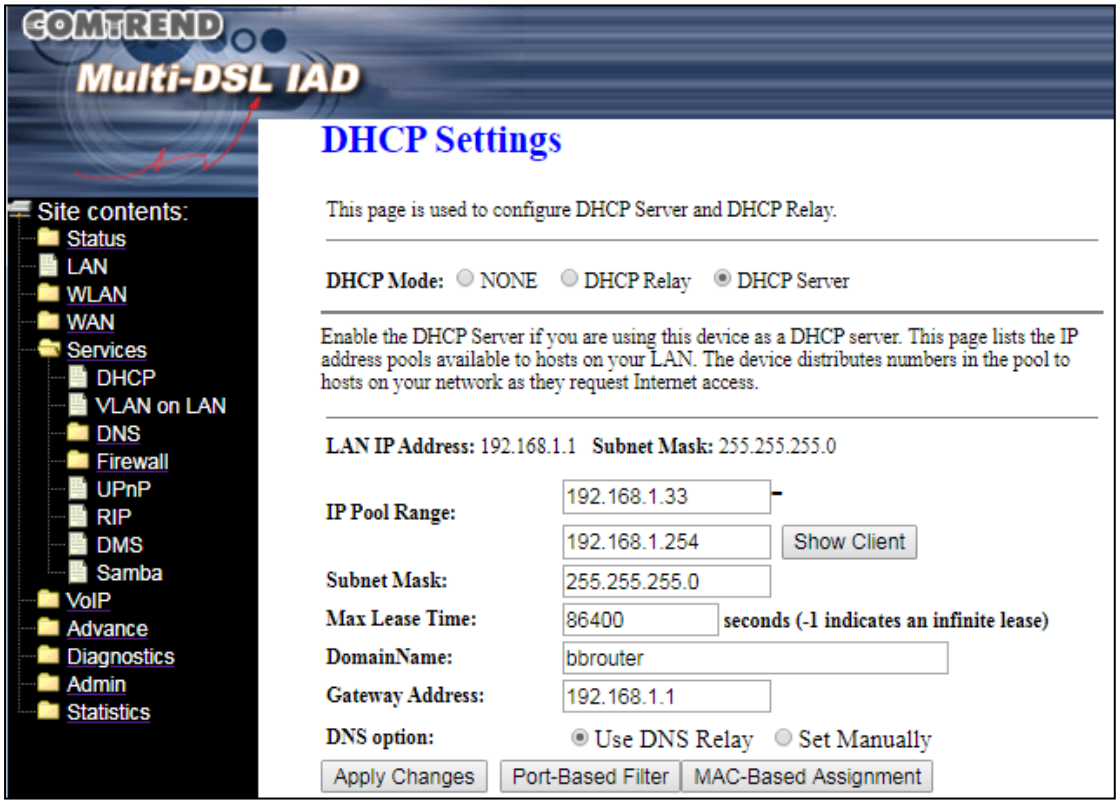
Field/Header	Description
3G WAN	Select the required radio button to enable or disable 3G WAN
PIN Code	Input the SIM card PIN code
APN	Input APN(Access Point Name) provided by your service provider
Dial Number	Input the dial number of the 3G/4G network
Authentication	Select the authentication type from the drop-down menu
User Name	Input the user name if Authentication is enabled
Password	Input the password if Authentication is enabled
Connection Type	Select the connection type from the drop-down menu
Idle Time (min)	Input idle time value if connection type is Connect on Demand
NAPT	Enable/disable Network Address Port Translation by selecting the radio button
Default Route	Enable/disable default route by selecting the radio button
MTU	Fixed Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards.

Field/Header	Description
Backup for XDSL	Select the required radio button to enable or disable XDSL backup
Backup Timer (sec)	Input backup timer value if Backup for XDSL is enabled

Chapter 8 Services

8.1 DHCP

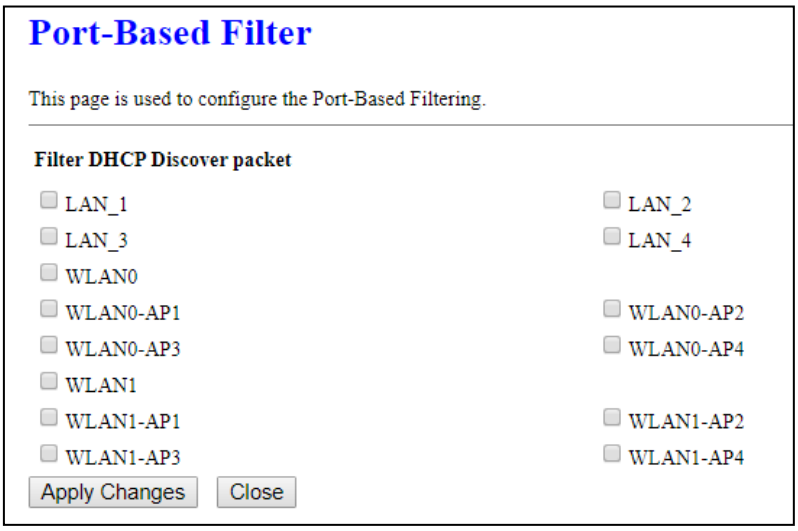
This page is used to configure DHCP Server and DHCP Relay. Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.



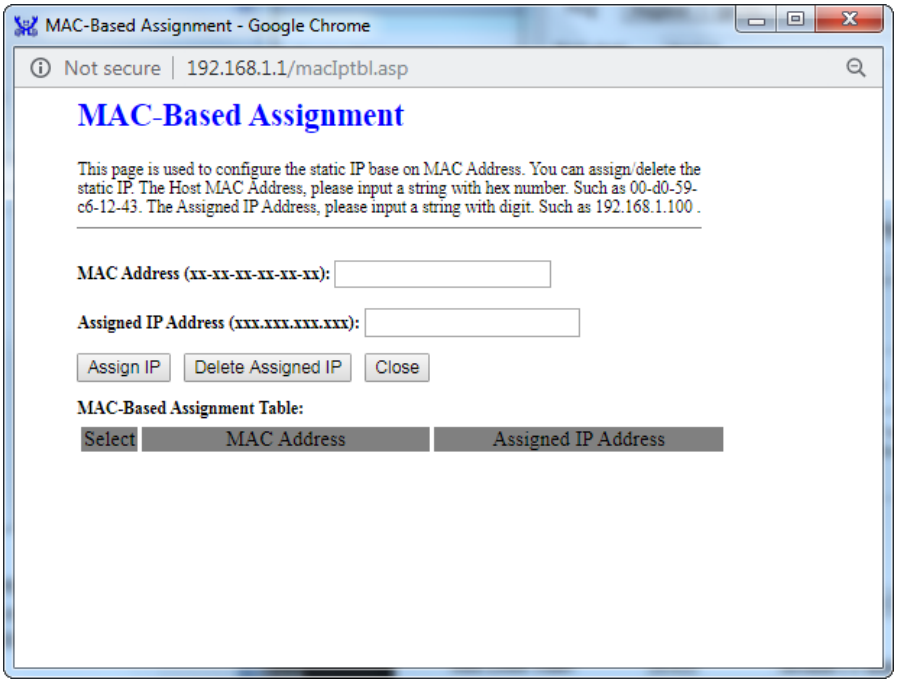
Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
LAN IP Address/Subnet Mask	Displays the IP address and Subnet Mask for the LAN port
IP Pool Range	Input the start IP address and end IP address for DHCP server
Subnet Mask	Input the subnet mask
Max Lease Time	Input the lease time
Domain Name	Input the Domain name
Gateway Address	Input the Default Gateway IP address
DNS option	Select the required DNS option radio button

Click the **Port-Based Filter** button to configure the Port-Based Filtering.

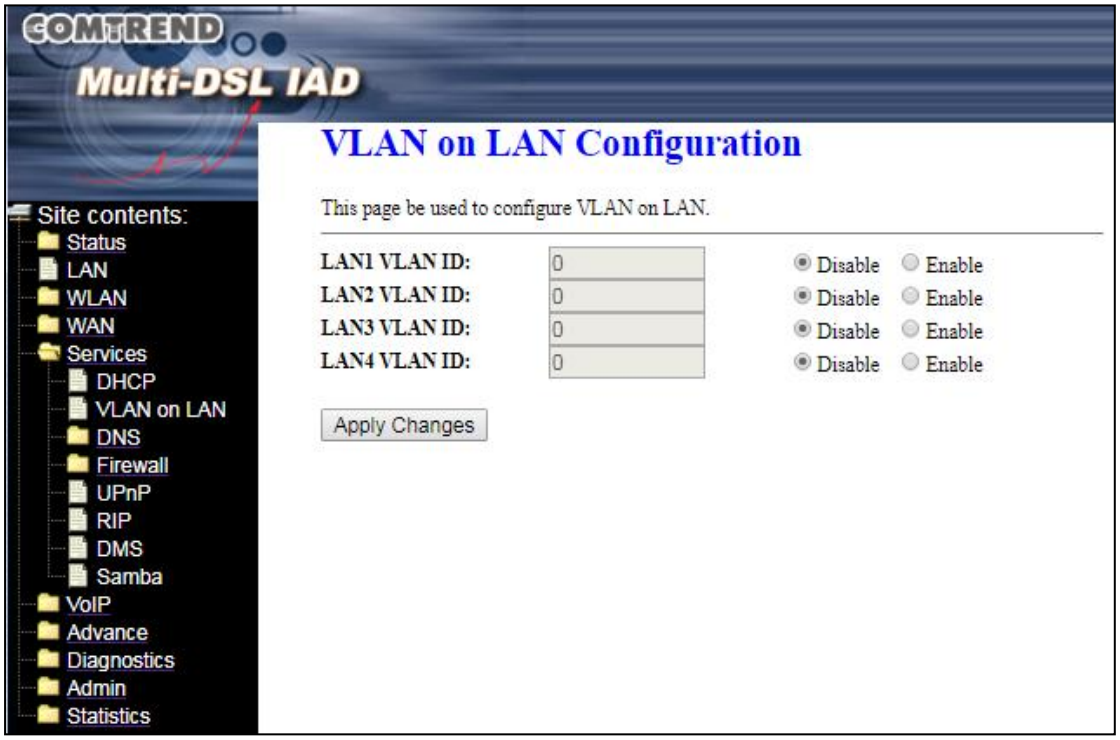


Click the **MAC-Based Assignment** to configure the static IP base on MAC Address. You can assign/delete the static IP. For the Host MAC Address, please input a string with hex numbers. Such as 00-d0-59-c6-12-43. For the Assigned IP Address, please input a string with digits. Such as 192.168.1.100



8.2 VLAN on LAN

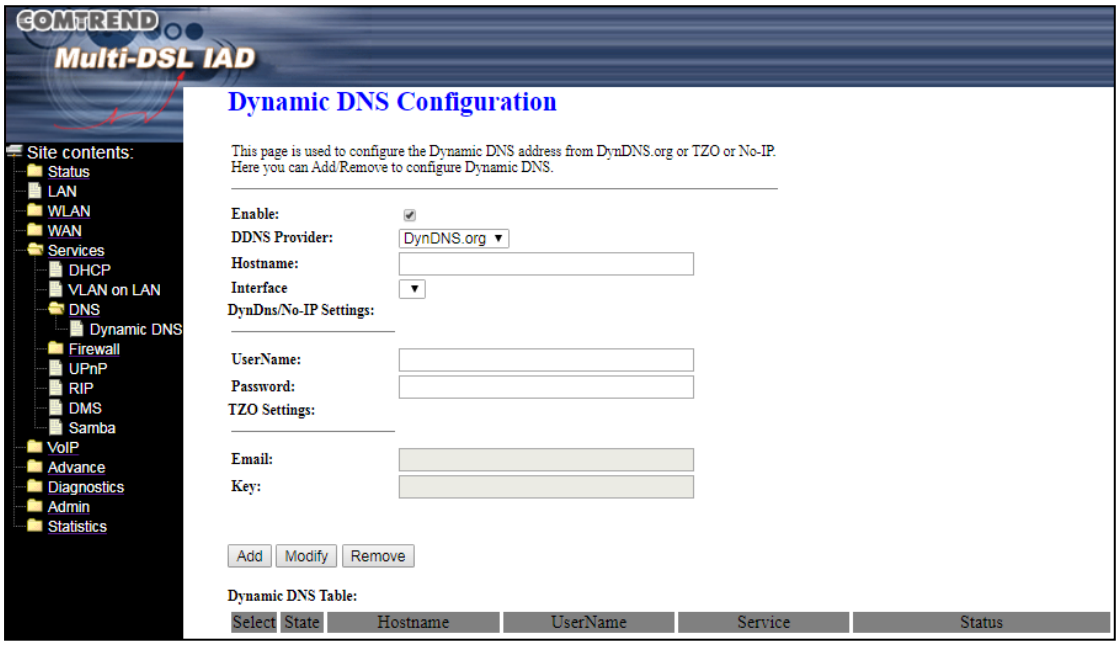
This page can be used to configure VLAN on LAN.



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

8.3 DNS – 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.

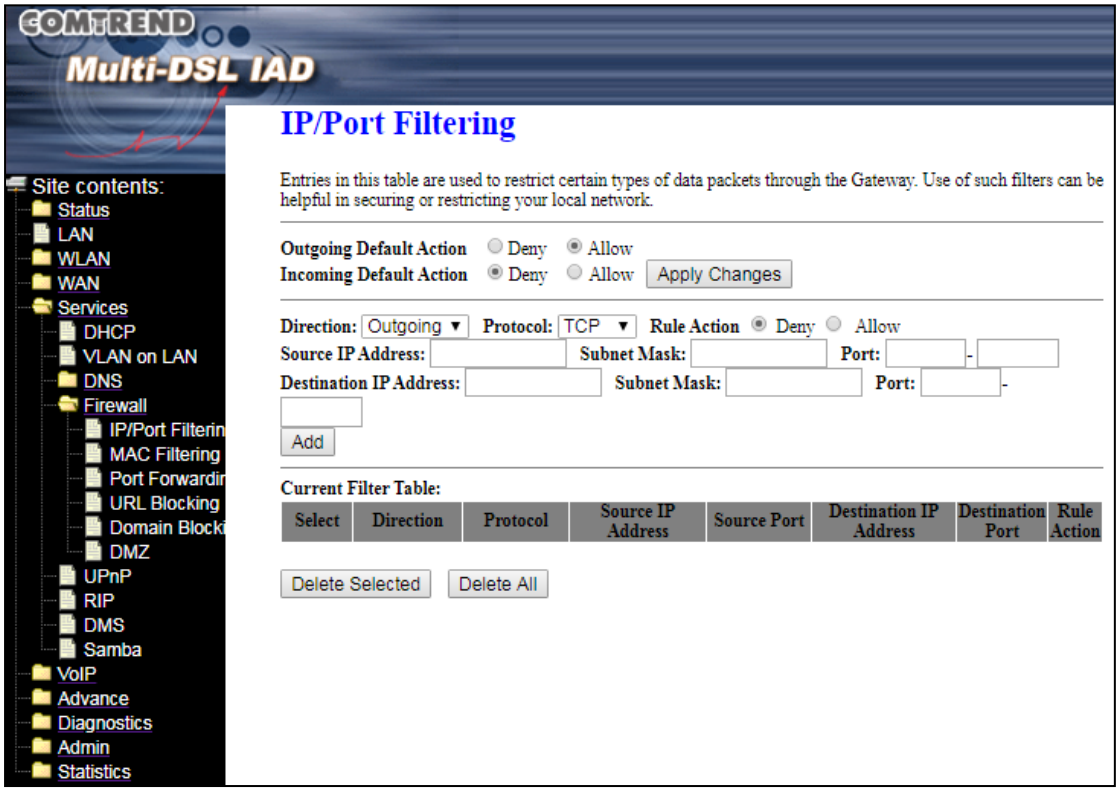


Field/Header	Description
Enable	Tick the checkbox to enable Dynamic DNS
DDNS Provider	Select from the drop-down menu
Hostname	Input the DDNS HostName
Interface	Select the interface from the drop-down menu
DynDns/No-IP Settings	
UserName	Input the username
Password	Input the password
TZO Settings	
Email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

8.4 Firewall

8.4.1 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.



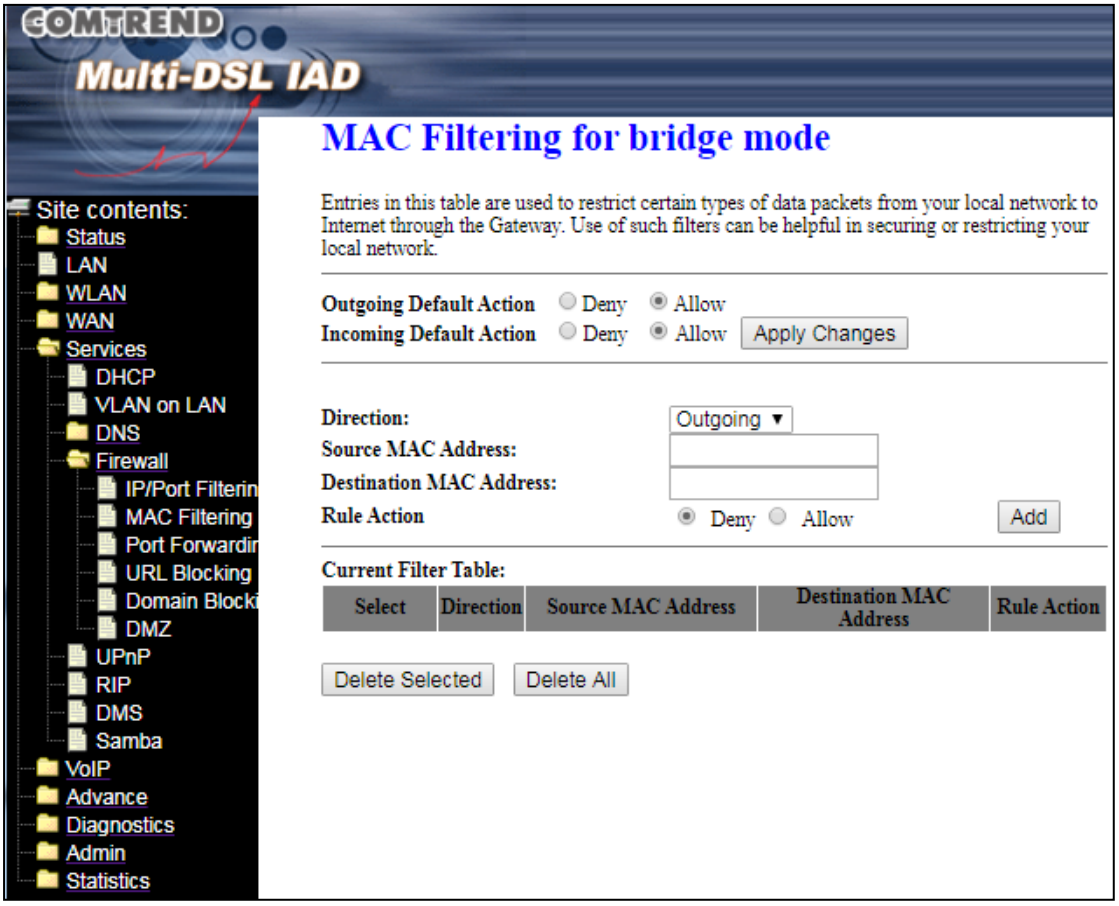
Click the **Apply Changes** button for your changes to take effect.

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

Field/Header	Description
Outgoing Default Action	Select the Deny/Allow radio button depending on your requirements
Incoming Default Action	Select the Deny/Allow radio button depending on your requirements
Direction	Select the direction from the drop-down menu
Protocol	Select the protocol from the drop-down menu
Rule Action	Select the Deny/Allow radio button depending on your requirements
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

8.4.2 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.



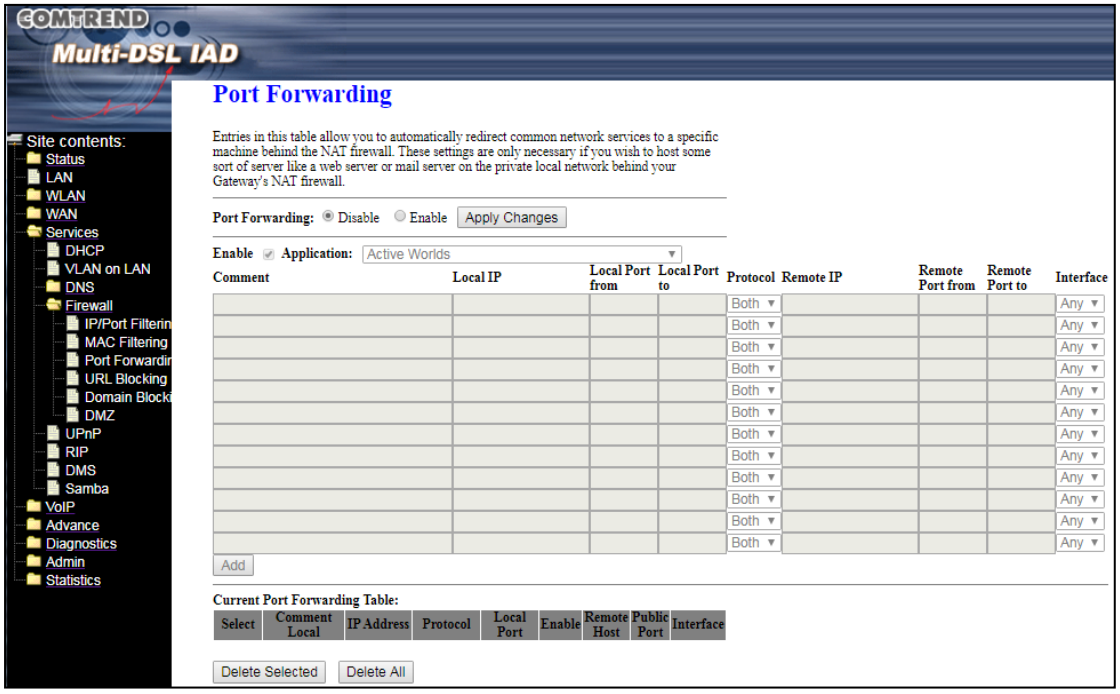
Click the **Apply Changes** button for your changes to take effect.

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

Field/Header	Description
Outgoing Default Action	Select the Deny/Allow radio button depending on your requirements
Incoming Default Action	Select the Deny/Allow radio button depending on your requirements
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	Select the Deny/Allow radio button depending on your requirements

8.4.3 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.

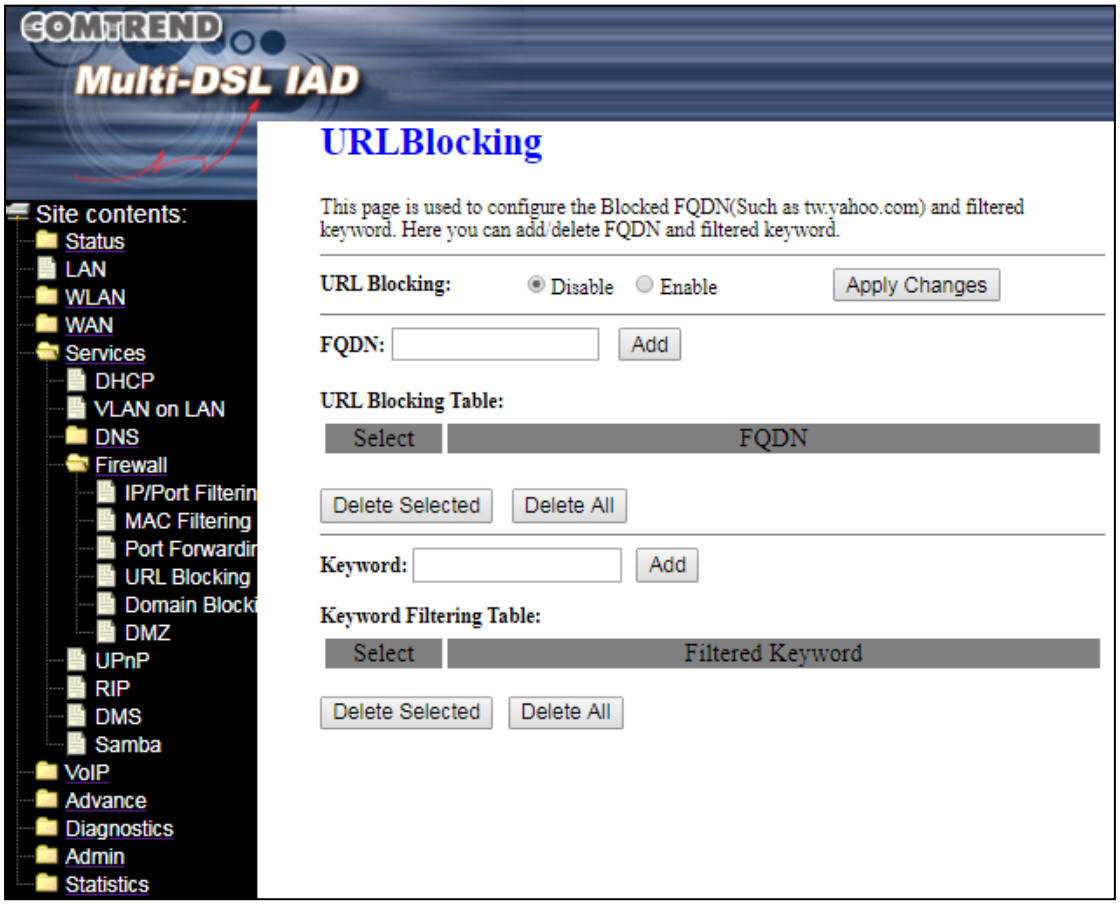


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Port Forwarding	Enable or disable Port Forwarding by selecting the appropriate radio button
Enable	Tick 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 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

8.4.4 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.

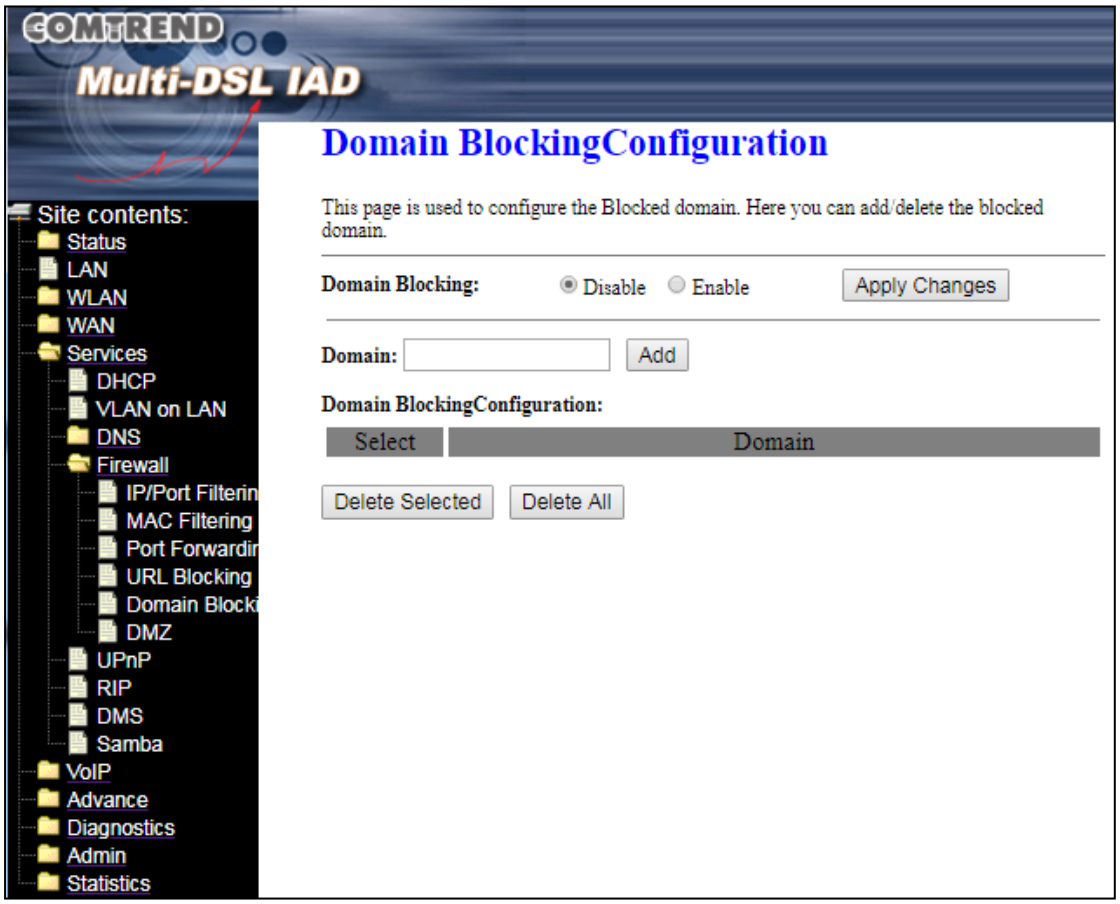


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
URL Blocking	Select the Disable/Enable radio button depending on your requirements
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	Display the Keyword filtering entries

8.4.5 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.

Field/Header	Description
Domain Blocking	Select the Disable/Enable radio button depending on your requirements
Domain	Input the domain

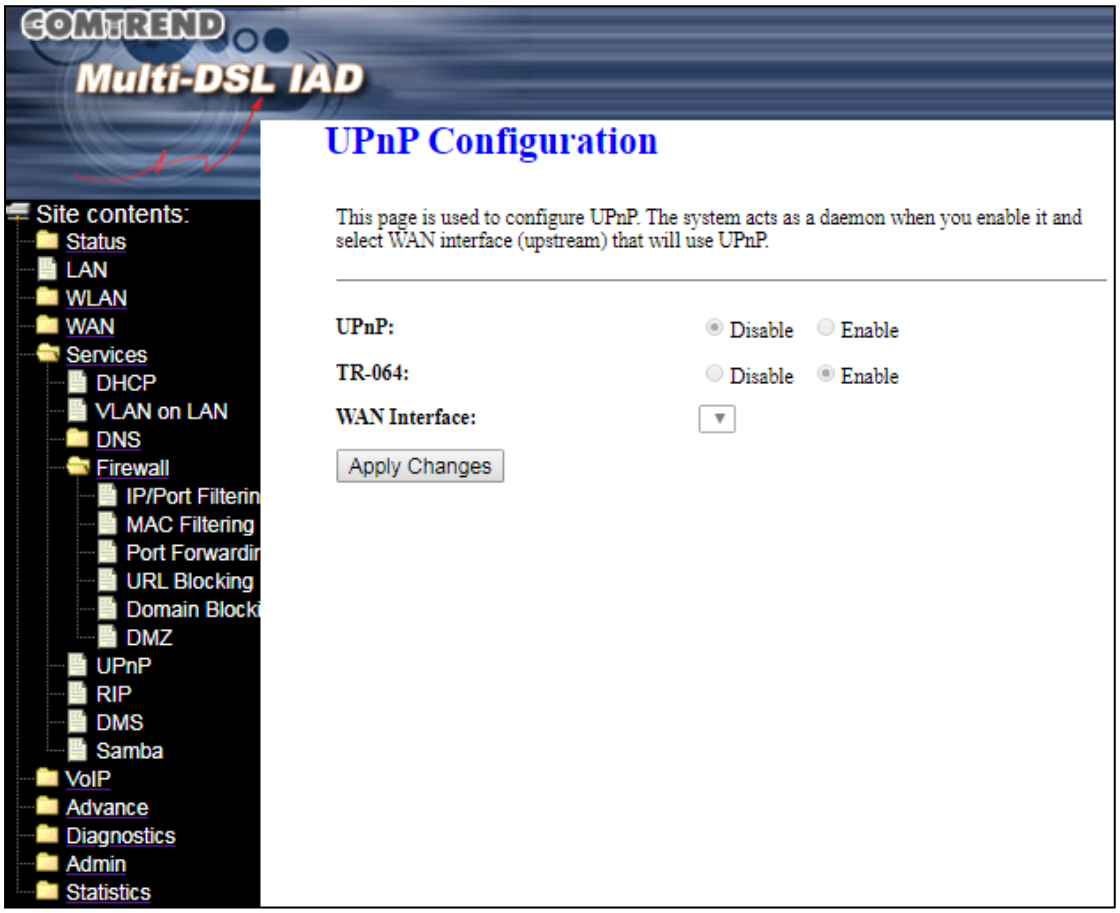
8.4.6 DMZ

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.

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

8.5 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.

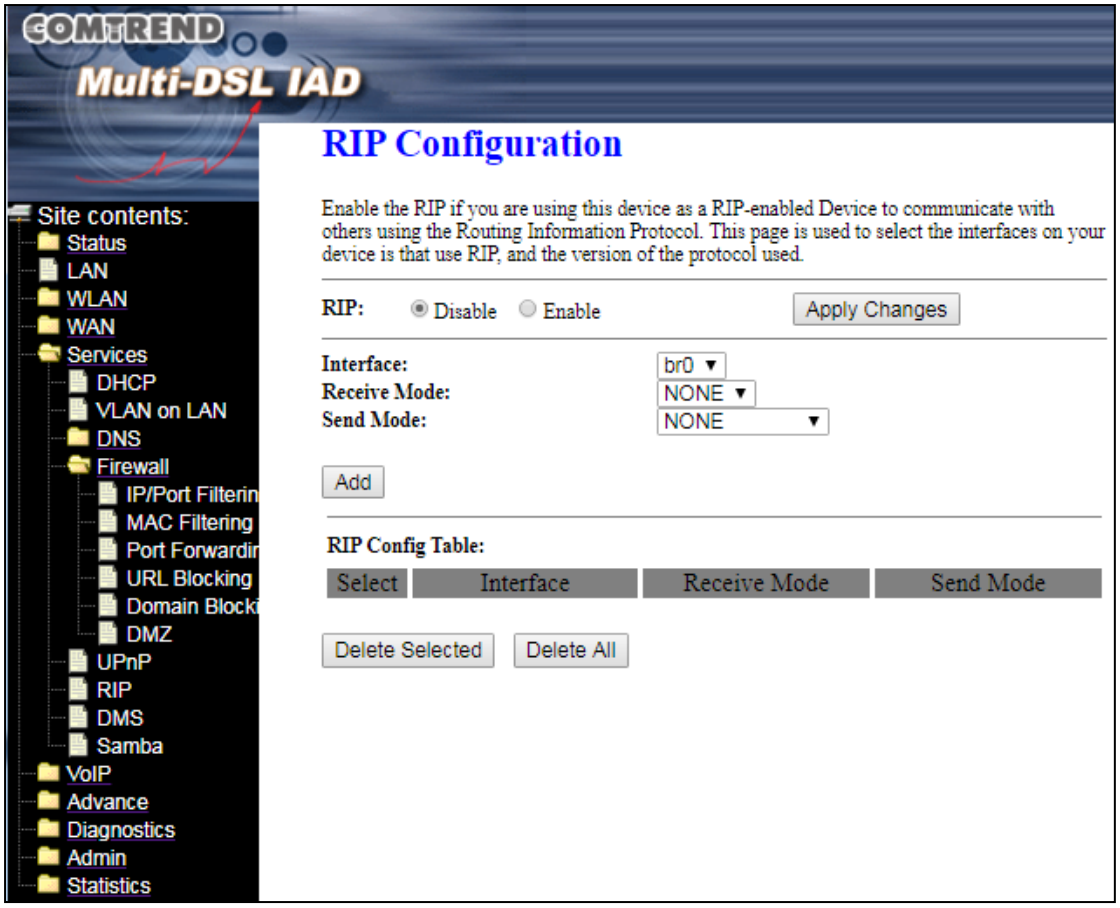


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
UPnP	Select the Disable/Enable radio button depending on your requirements
TR-064	Select the Disable/Enable radio button depending on your requirements
WAN Interface	Select the WAN interface from the drop-down menu

8.6 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 is that use RIP, and the version of the protocol used.

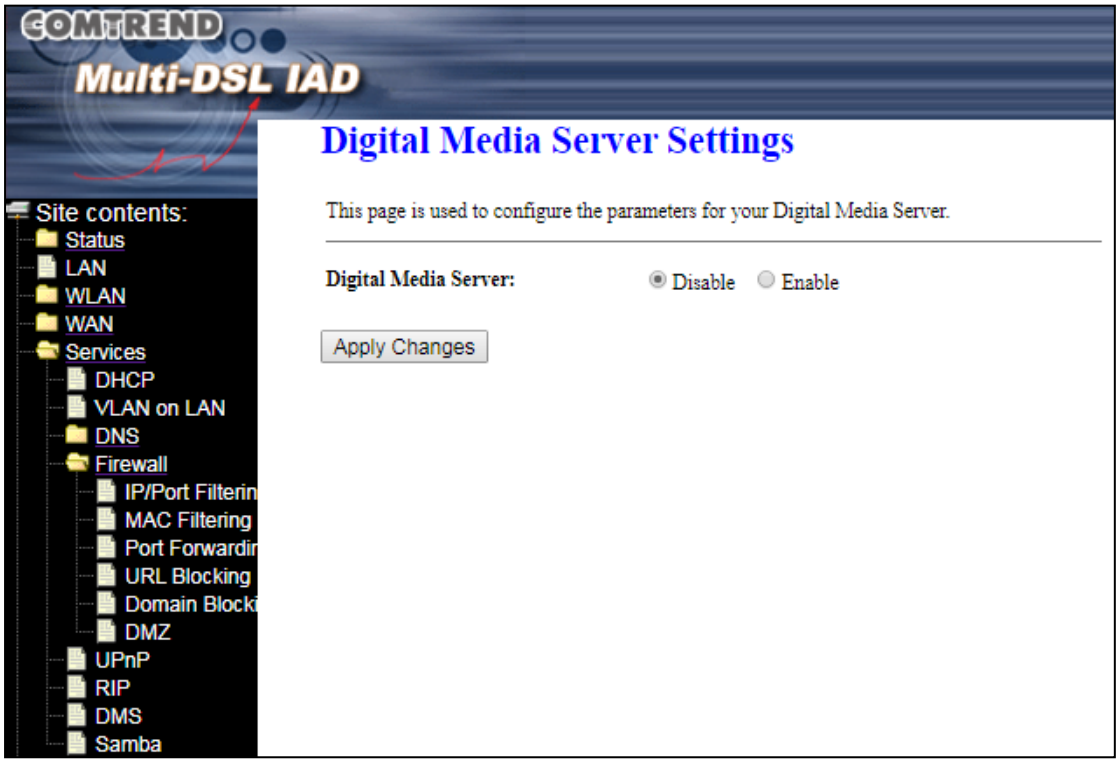


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
RIP	Select the Enable/Disable radio button depending on your requirements
Interface	Select from the drop-down menu
Receive Mode	Select from the drop-down menu
Send Mode	Select from the drop-down menu

8.7 DMS

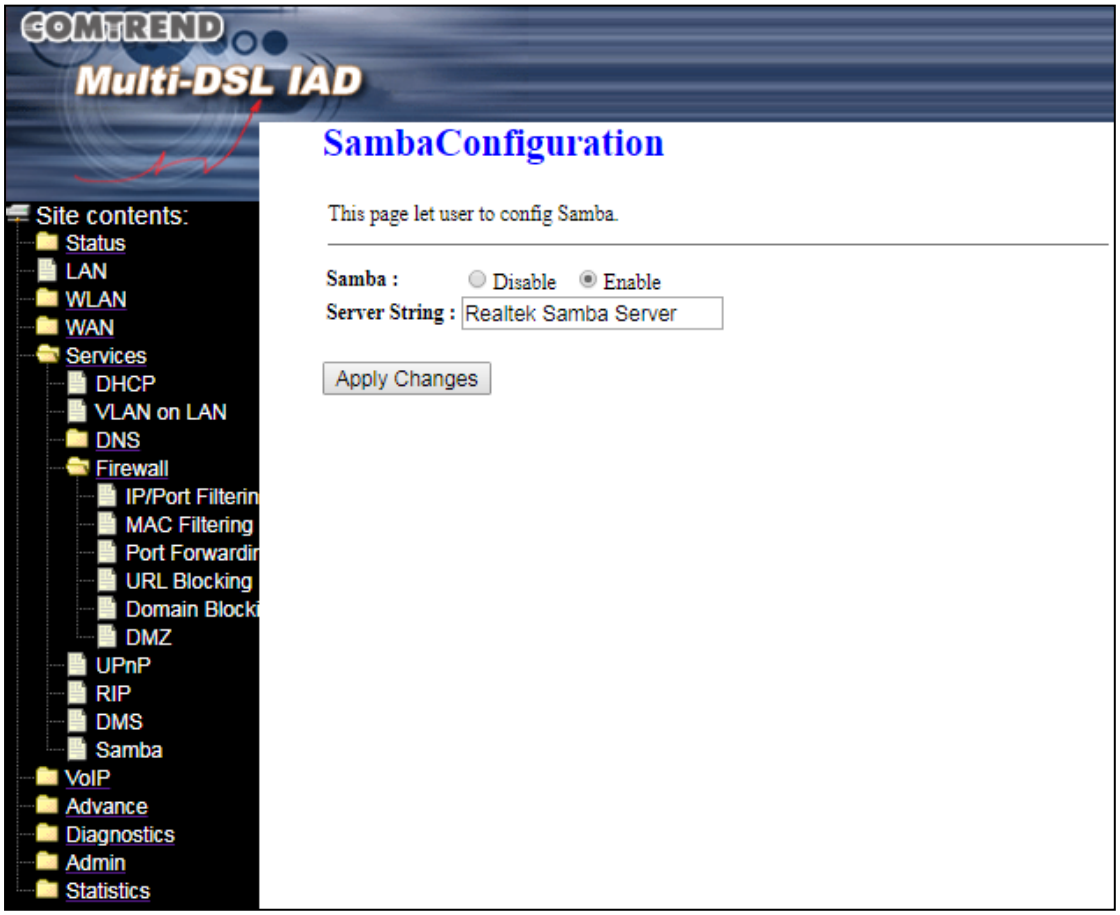
This page is used to configure the parameters for your Digital Media Server. It allows users to share digital media, like pictures, music and video, to other LAN devices from the digital media server.



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

8.8 Samba

This page lets users configure Samba. It allows you to use Storage devices with modems for easy access.

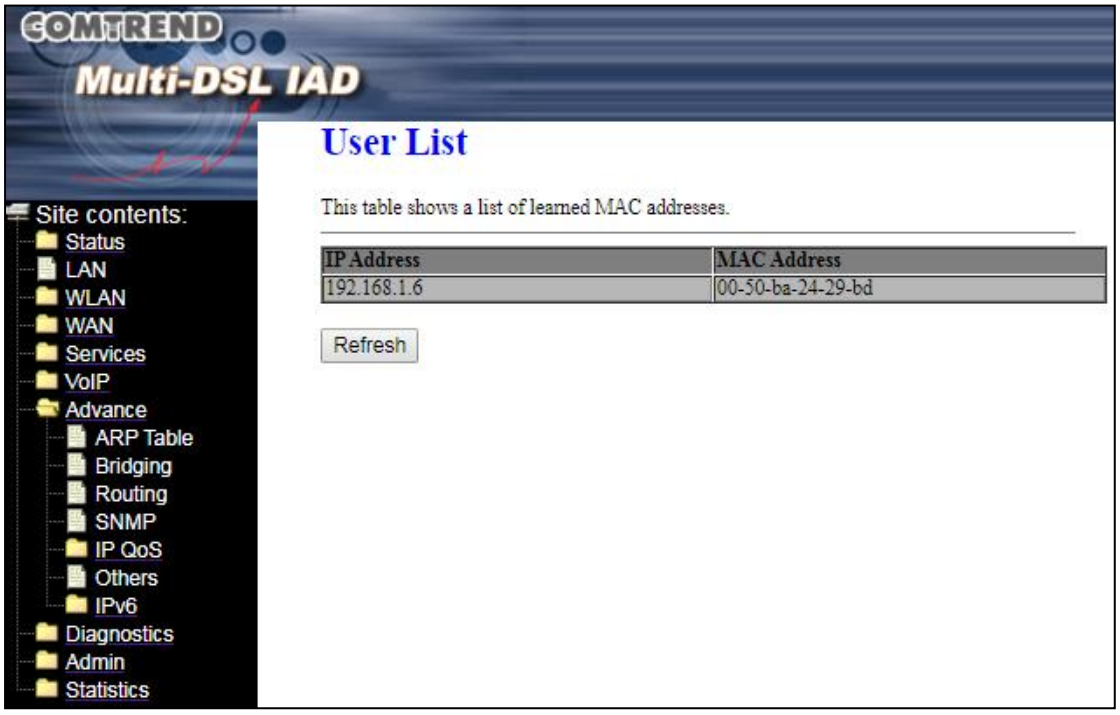


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Samba	Select the Disable/Enable radio button depending on your requirements
Server String	Input description of the Samba Server

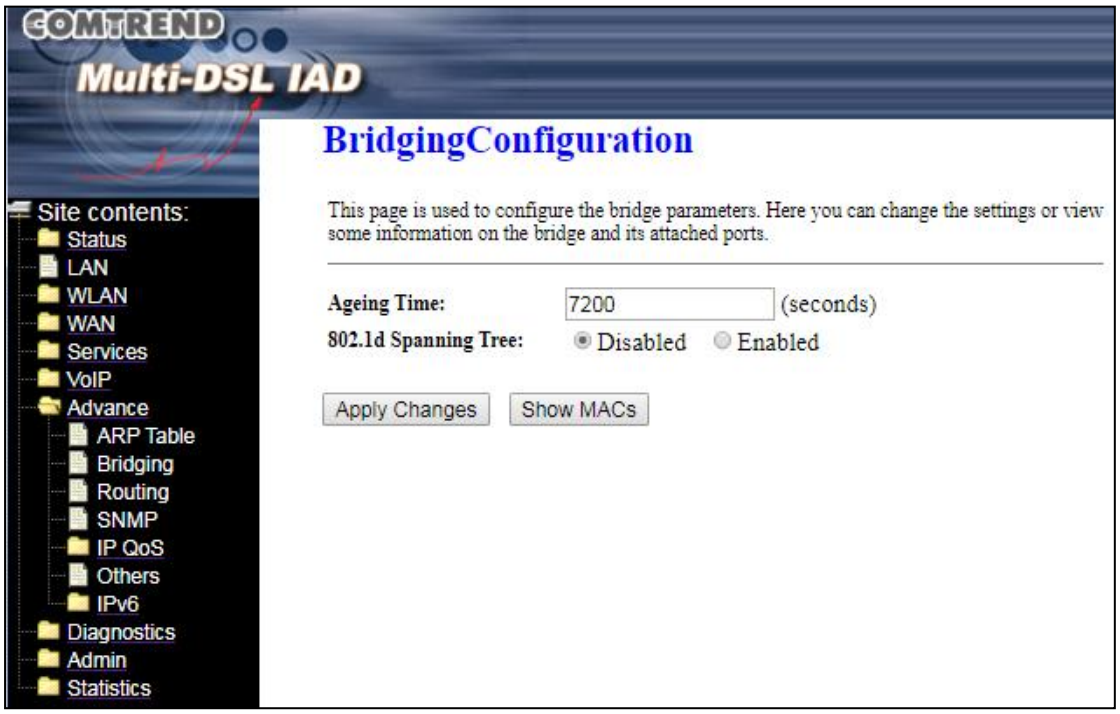
9.1 ARP Table

This table shows a list of learned MAC addresses.



9.2 Bridging

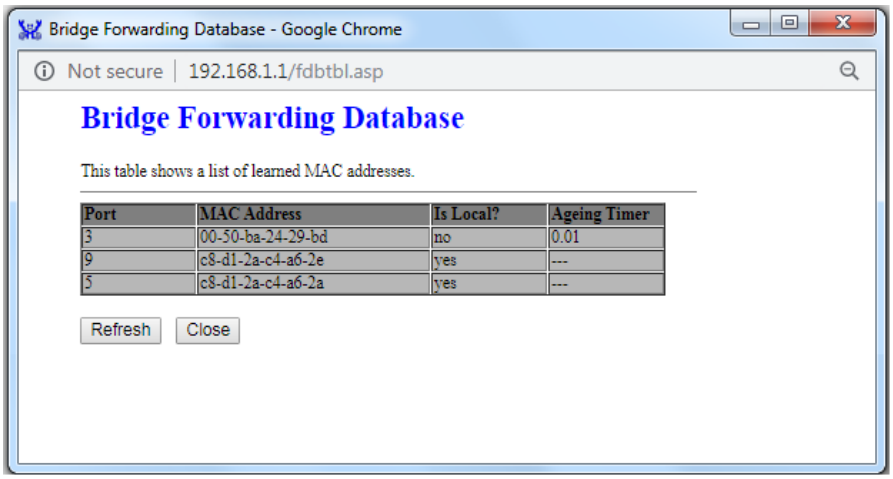
This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.



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

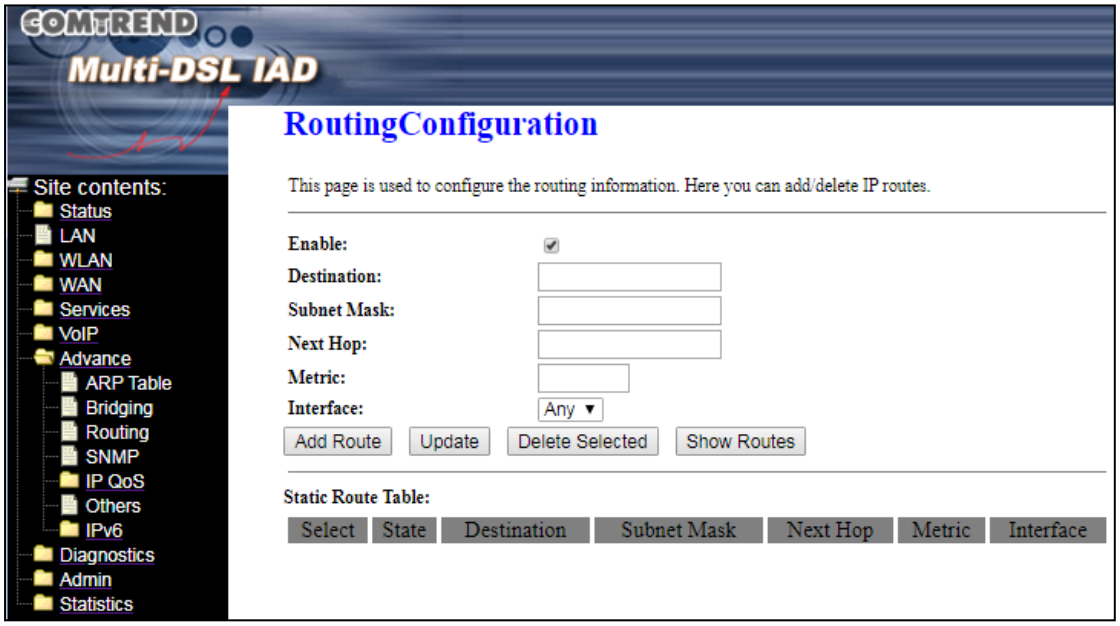
Field/Header	Description
Ageing Time	Configure the STP ageing time
802.1d Spanning Tree	Select the Disable/Enable radio button depending on your requirements

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



9.3 Routing

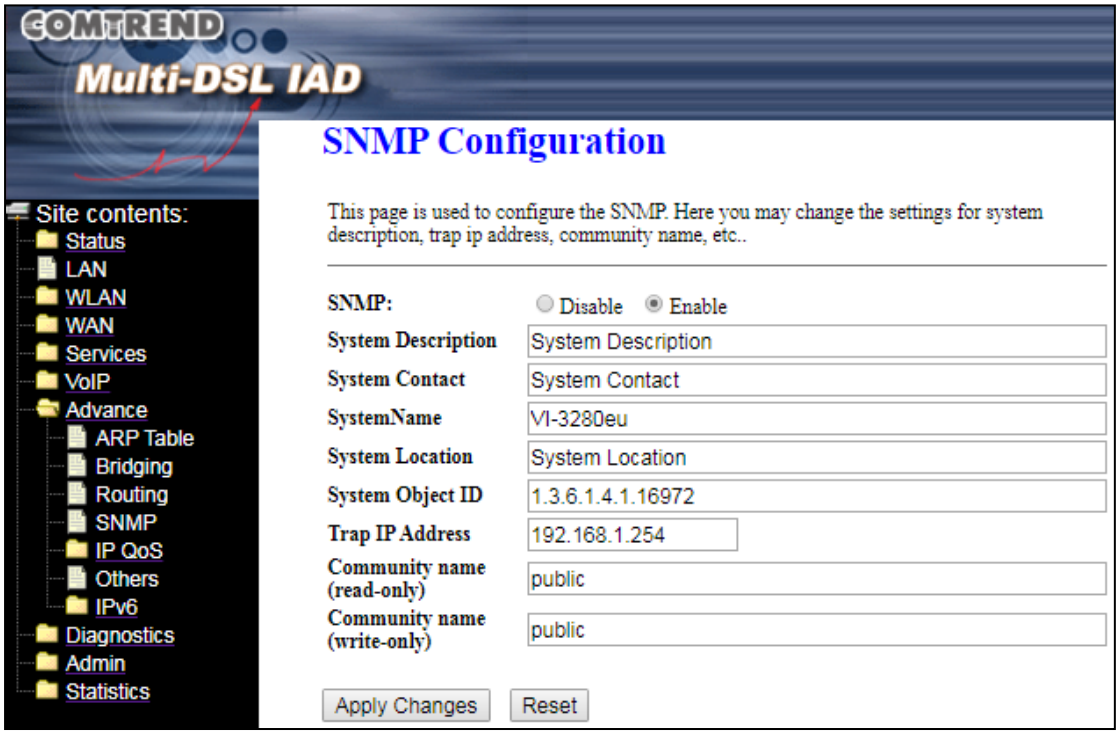
This page is used to configure the routing information. Here you can add/delete IP routes.



Field/Header	Description
Enable	Tick the checkbox to enable
Destination	Input the destination IP address
Subnet Mask	Input the Subnet Mask
Next Hop	Input the next hop of routing
Metric	Input The metric value of routing
Interface	Select the required interface from the drop-down menu

9.4 SNMP

This page is used to configure the SNMP. Here 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.

Field/Header	Description
SNMP	Select the Disable/Enable radio button depending on your requirements
System Description	Input the system description of the device
System Contact	Input the contact 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)	Input the read-only Community name
Community name (write-only)	Input the Read/Write Community name

9.5 IPQoS

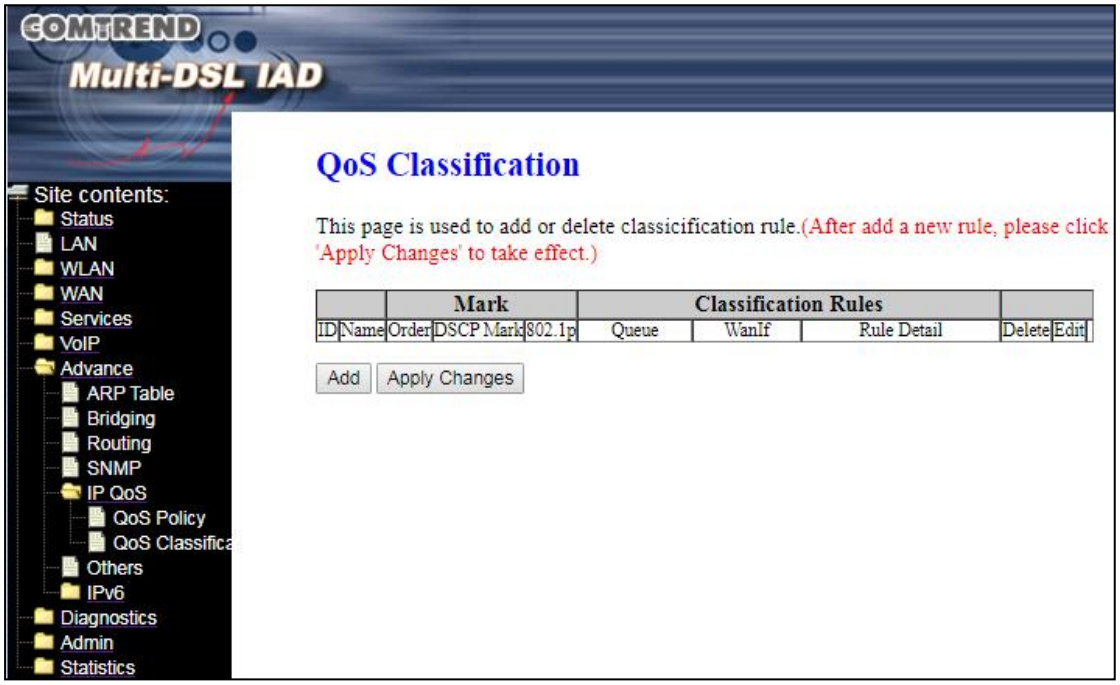
9.5.1 QoS Policy

This page is used to configure the QoS policy and Queue. If you select PRIO of policy, the lower numbers imply greater precedence. If you select WRR of policy, please input the weight of this queue. Default is 40:30:20:10.

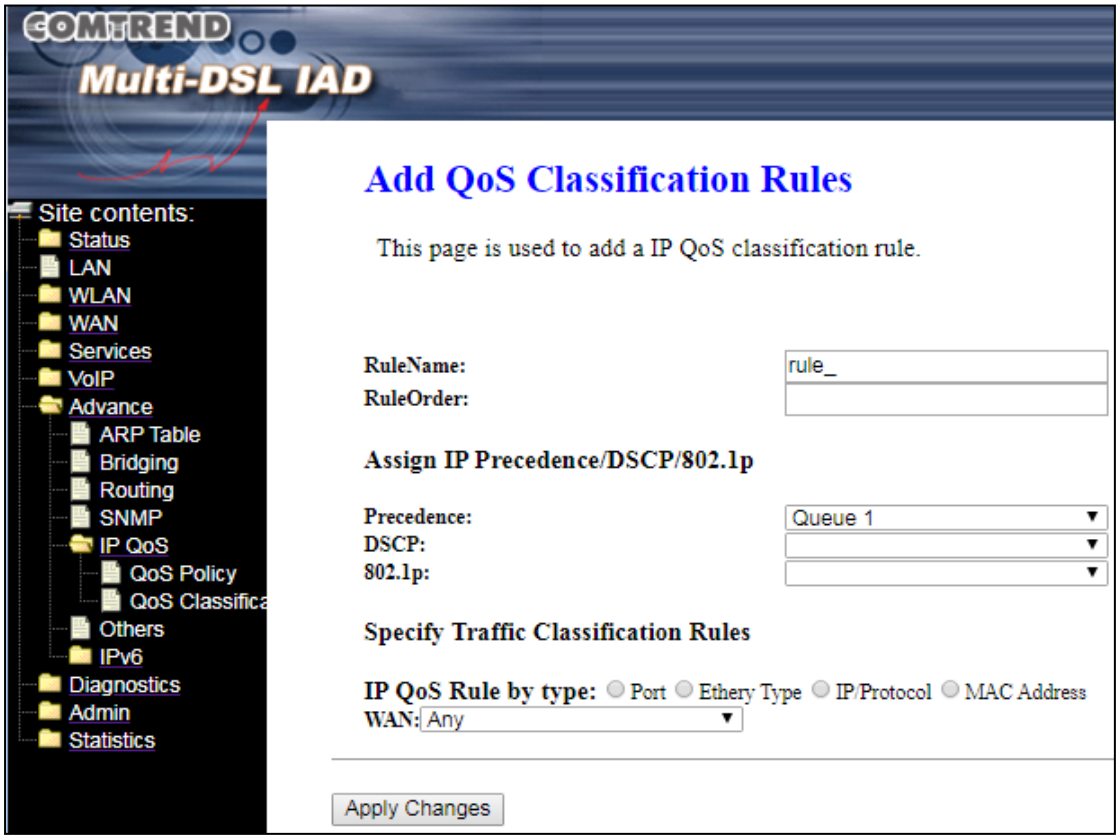
After configuration, please click the **Apply Changes** button.

9.5.2 QoS Classification

This page is used to add or delete classification rule.
(After adding a new rule, please click 'Apply Changes' for the rule to take effect.)



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



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

Field/Header	Description
Rule Name	The identifier for this Queue entry
Rule Order	Input the value of the rule order
Precedence	Select from the drop-down menu
DSCP	Select from the drop-down menu
802.1p	Select from the drop-down menu
IP QoS Rule by type	Select the required radio button
WAN	Select from the drop-down menu

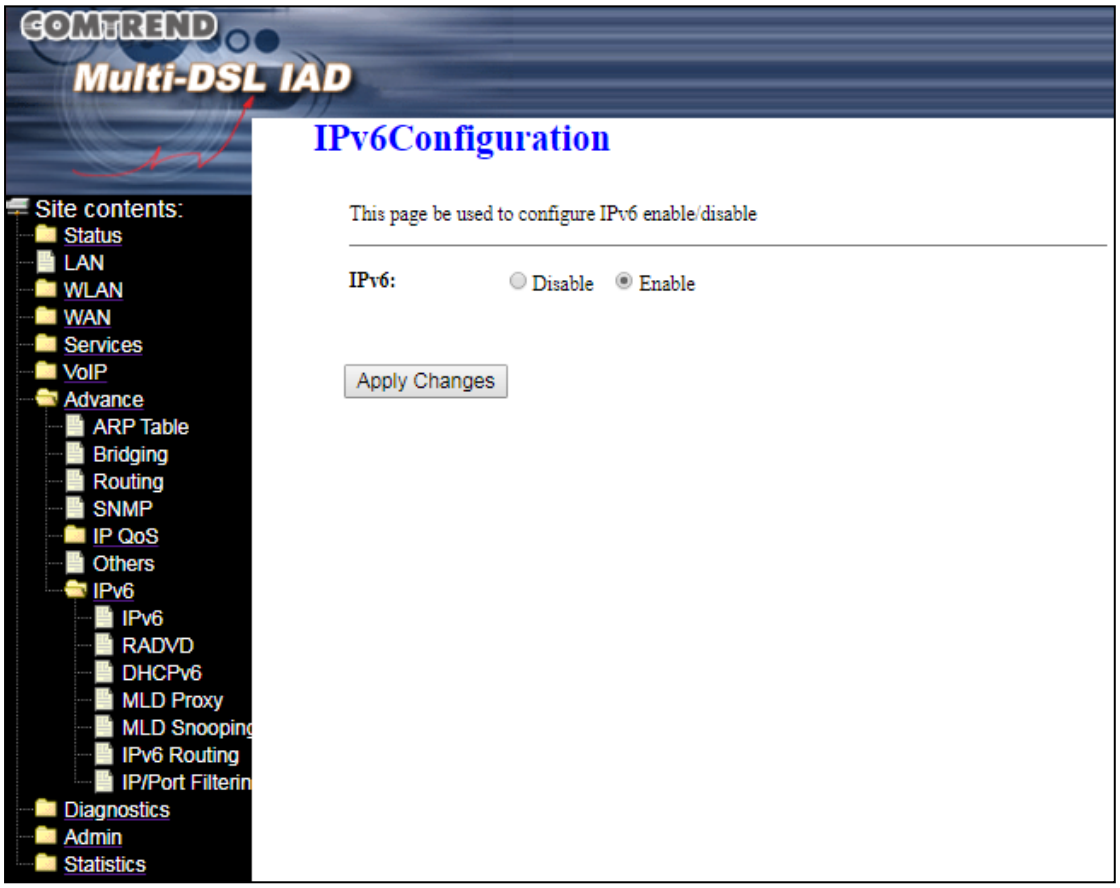
9.6 Others

This function is not supported on this firmware release.

9.7 IPv6

9.7.1 IPv6

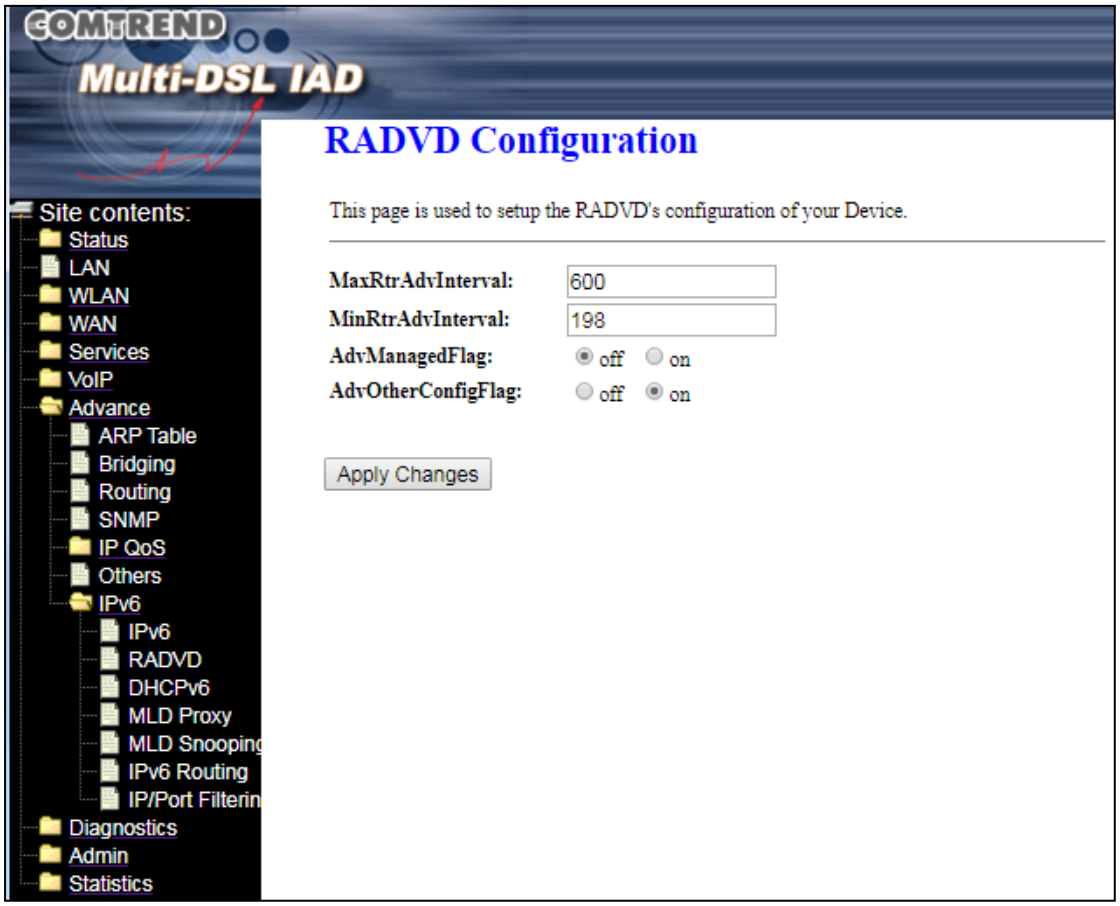
This page can be used to configure IPv6 enable/disable.



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

9.7.2 RADVD

This page is used to setup the RADVD's configuration of your Device.

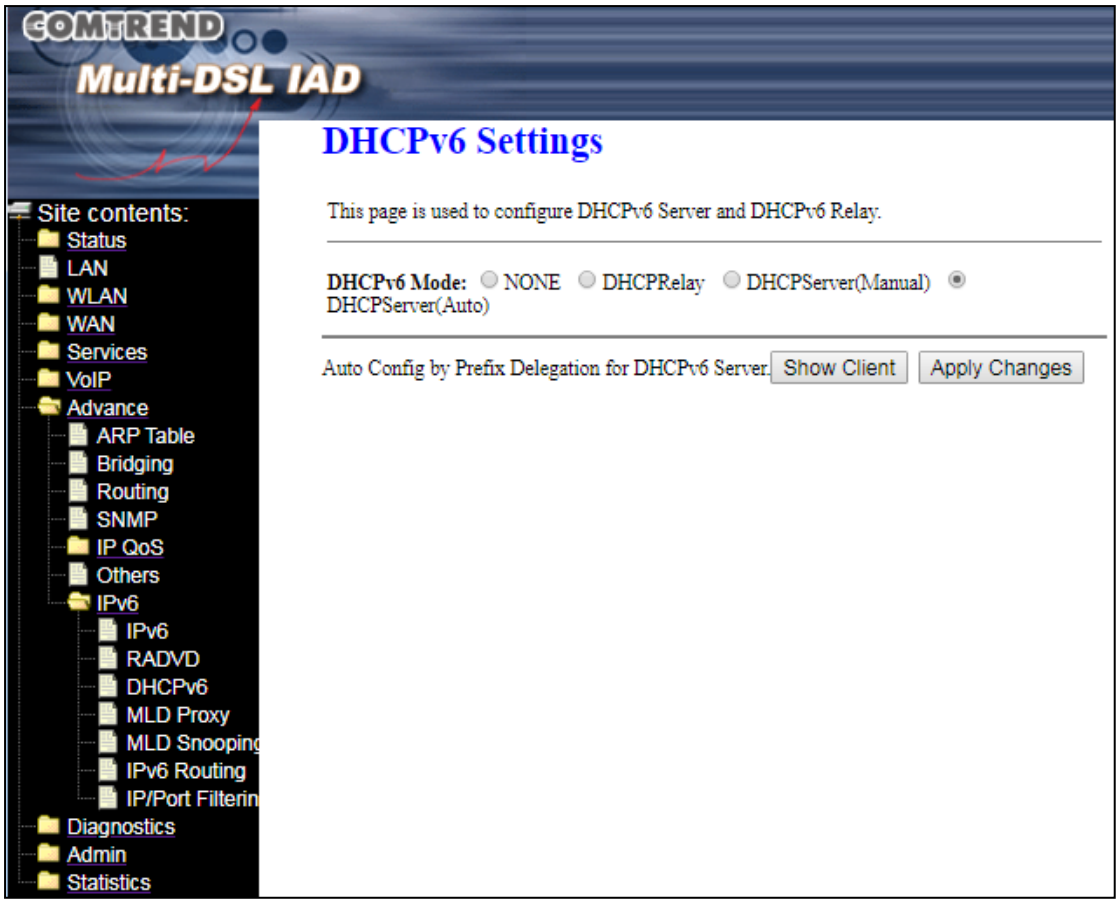


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Max Rtr Adv Interval	Input the Max Rtr Adv Interval
Min Rtr Adv Interval	Input the Min Rtr Adv Interval
Adv Managed Flag	Tick the checkbox to turn off or turn on Adv Managed Flag
Adv Other Config Flag	Tick the checkbox to turn off or turn on Adv Other Config Flag

9.7.3 DHCPv6

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

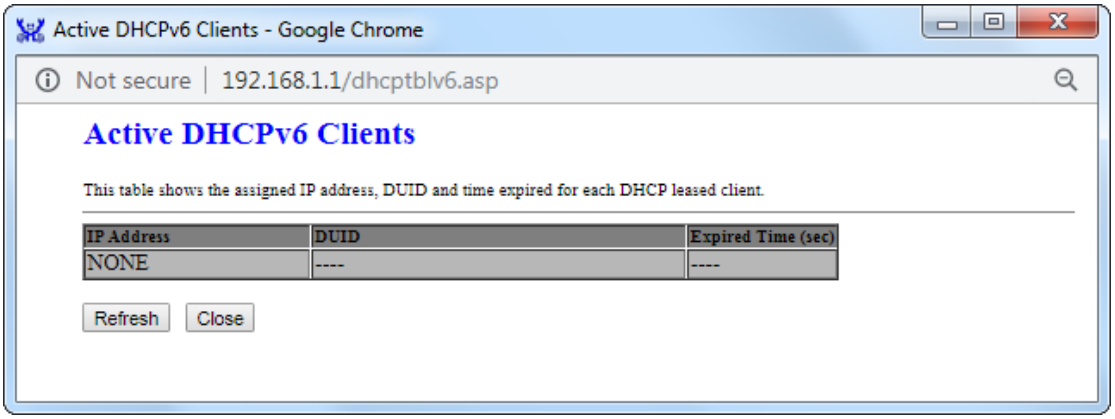


9.7.3.1 DHCPv6 – DHCP Server (Auto)

This is the default setting.

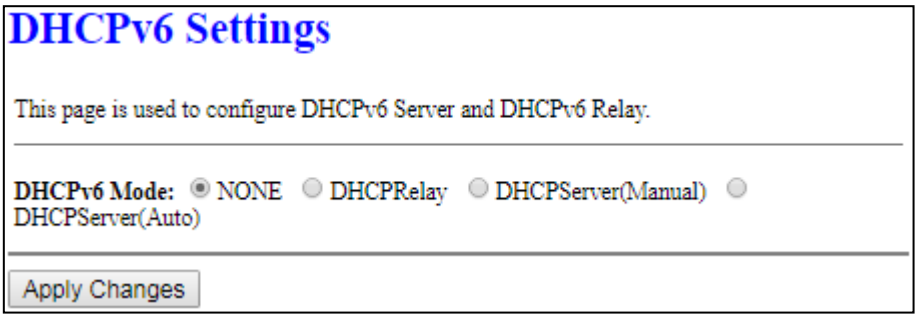
Click the **Apply Changes** button for your changes to take effect.

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



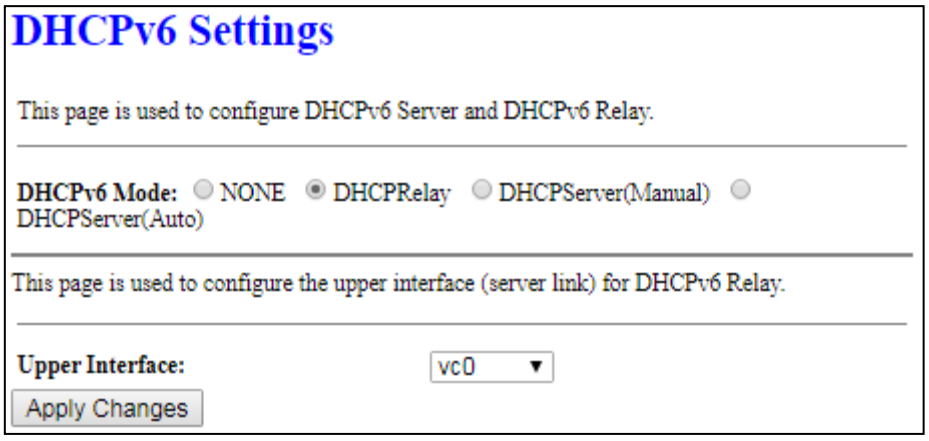
9.7.3.2 DHCPv6 – NONE

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



9.7.3.3 DHCPv6 – DHCP Relay

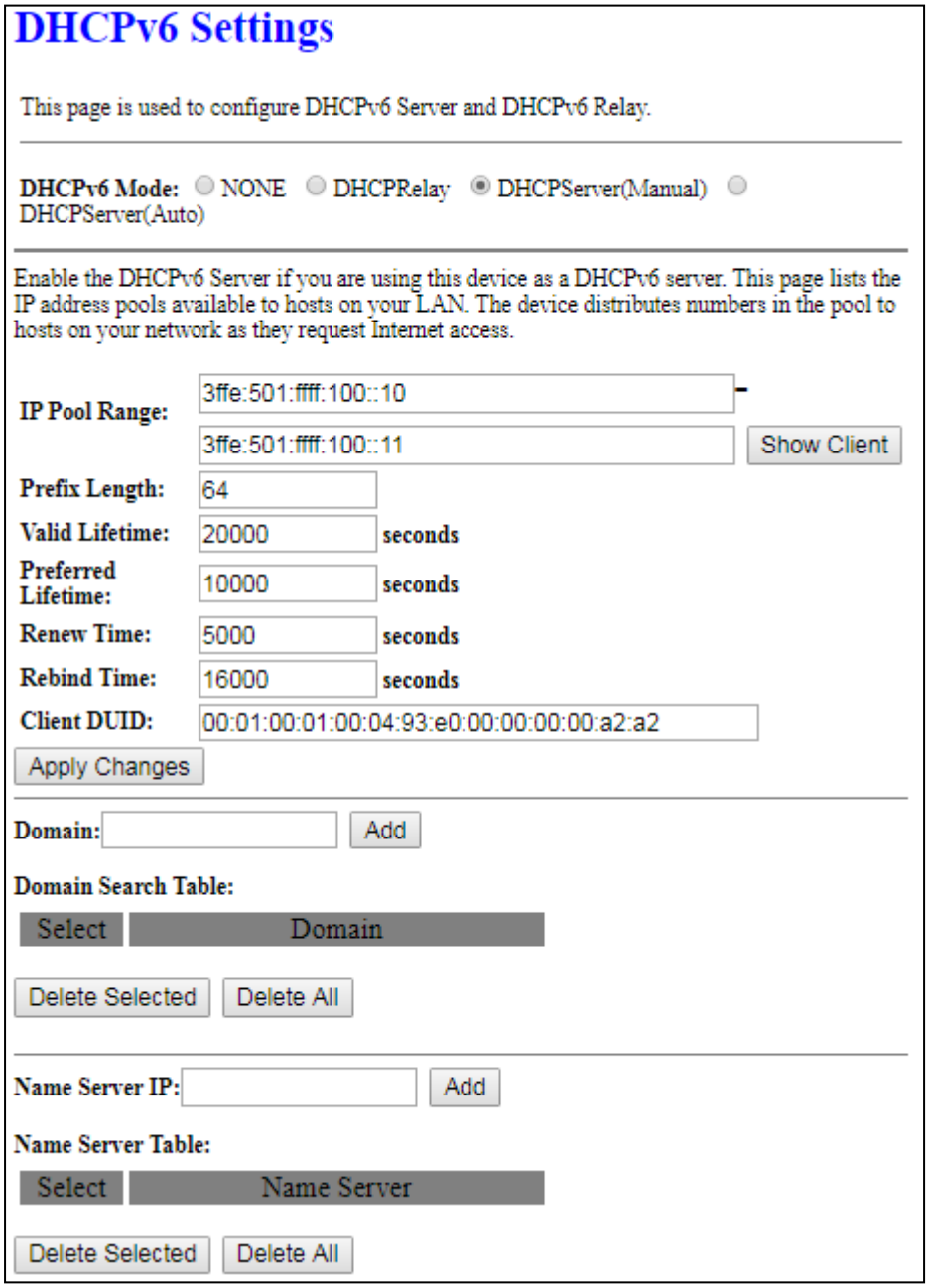
This page is used to configure the upper interface (server link) for DHCPv6 Relay.



Select the Upper Interface from the drop-down menu, and click the **Apply Changes** button for your changes to take effect.

9.7.3.4 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.

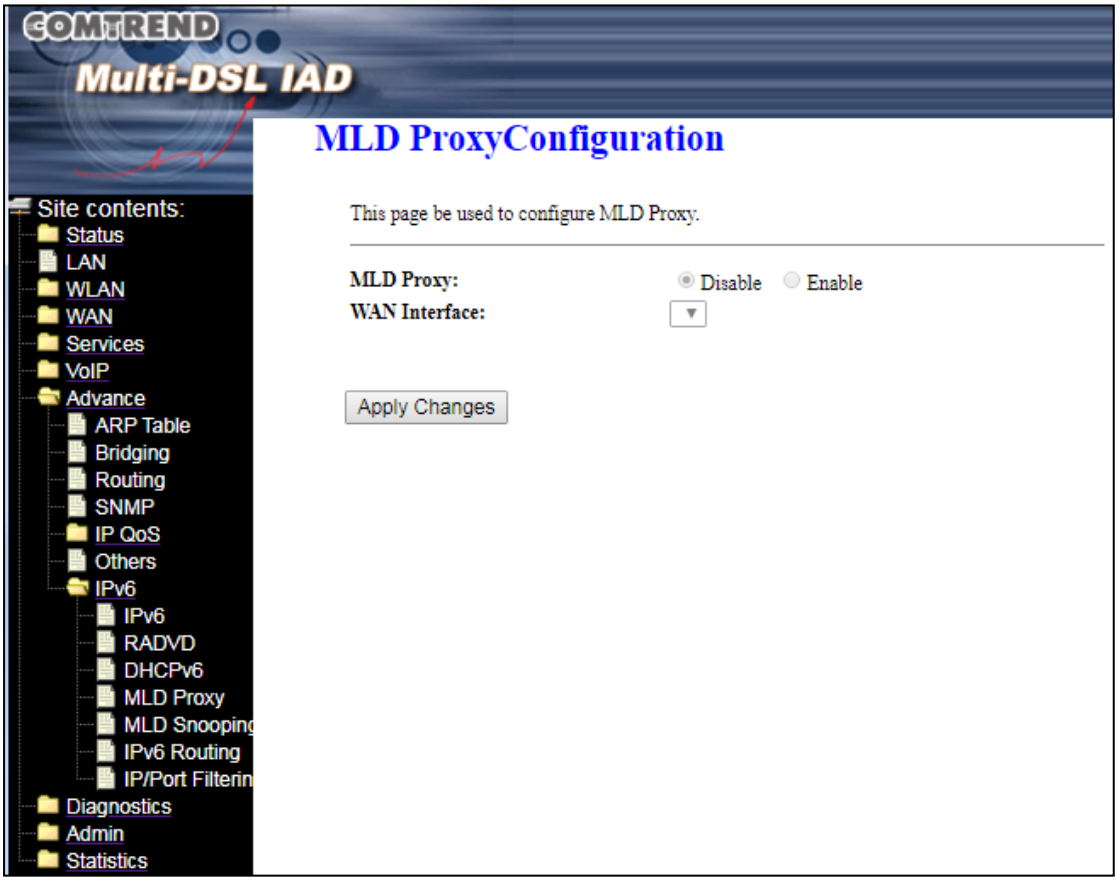


Field/Header	Description
IP Pool Range	Input the IP pool range
Prefix Length	Input the prefix length
Valid Lifetime	Input the valid lifetime in seconds
Preferred Lifetime	Input the preferred lifetime in seconds
Renew Time	Input the renew time in seconds

Field/Header	Description
Rebind Time	Input the rebind time in seconds
Client DUID	This is the is the globally unique identifier of the client
Domain	Input the domain name of the server
Name Server IP	Input the IP address of the server

9.7.4 MLD Proxy

This page can be used to configure MLD Proxy.



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

Field/Header	Description
MLD Proxy	Select Enable/Disable depending on your requirements
WAN Interface	Select the WAN interface from the drop-down menu

9.7.5 MLD Snooping

This page can be used to configure MLD Snooping.

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

9.7.6 IPv6 Routing

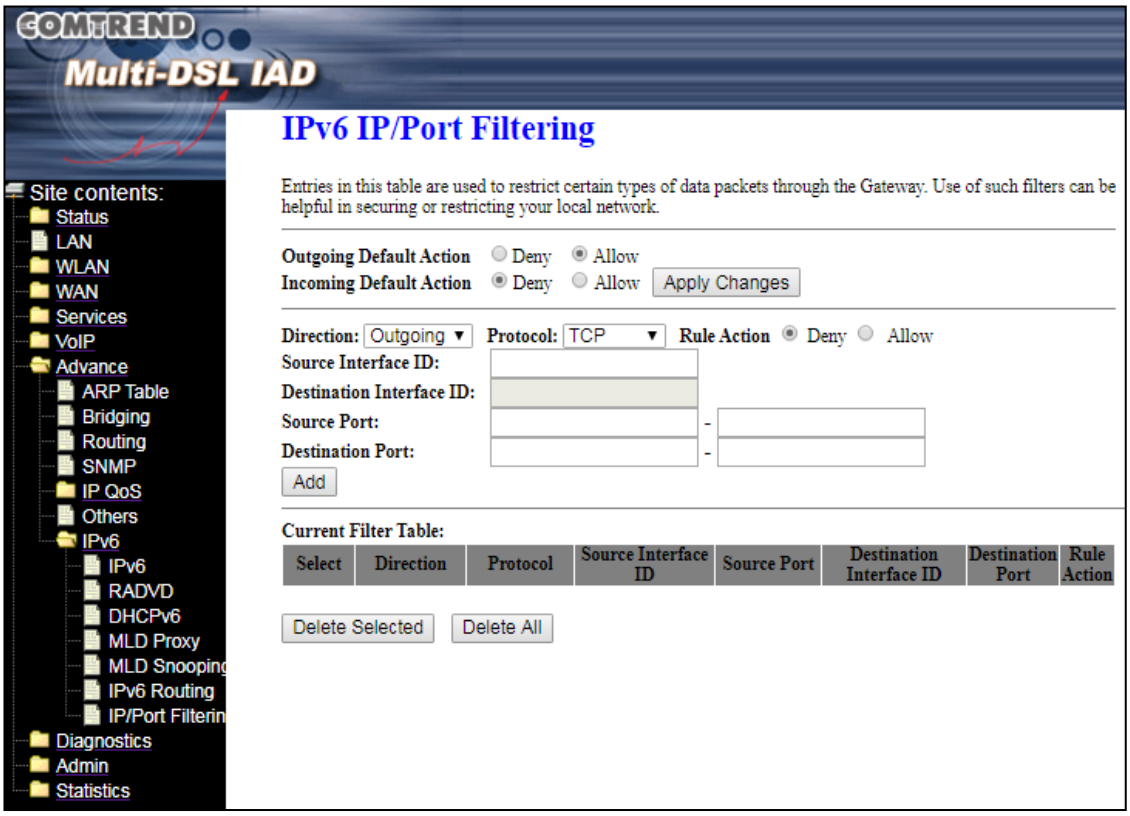
This page is used to configure the IPv6 static routing information. Here you can add/delete static IP routes.

Field/Header	Description
Enable	Tick the checkbox to enable
Destination	Input the destination IP address
Next Hop	Input the next hop
Metric	Input the metric
Interface	Select the interface from the drop-down menu

9.7.7 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.

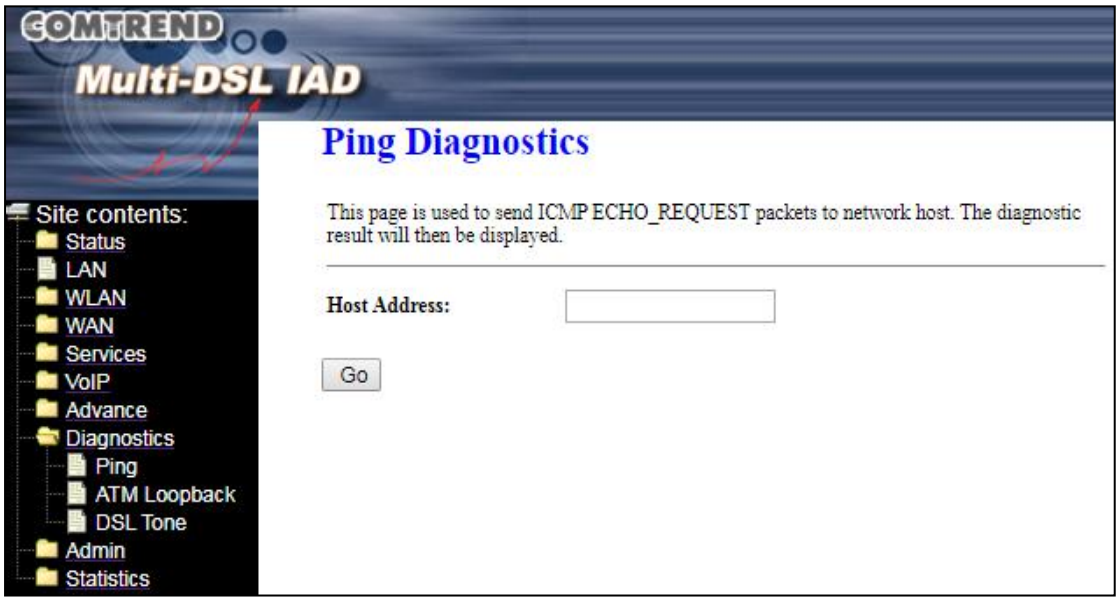


Field/Header	Description
Outgoing Default Action	Select the Deny/Allow radio button depending on your requirements
Incoming Default Action	Select the Deny/Allow radio button depending on your requirements
Direction	Select the direction from the drop-down menu
Protocol	Select the protocol from the drop-down menu
Rule Action	Select the Deny/Allow radio button depending on your requirements
Source Interface ID	Input the Source Interface ID
Destination Interface ID	Input the destination Interface ID
Source Port	Input the Source port number
Destination Port	Input the destination port number

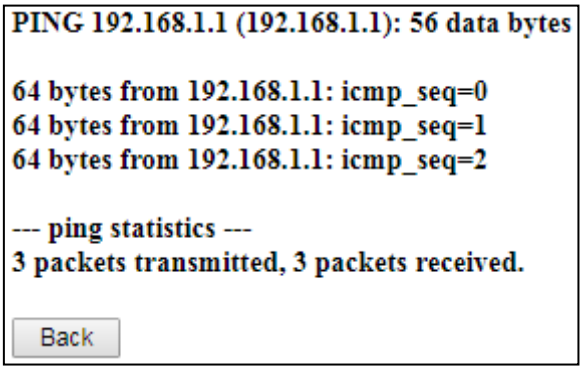
9.8 Diagnostics

9.8.1 Ping

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

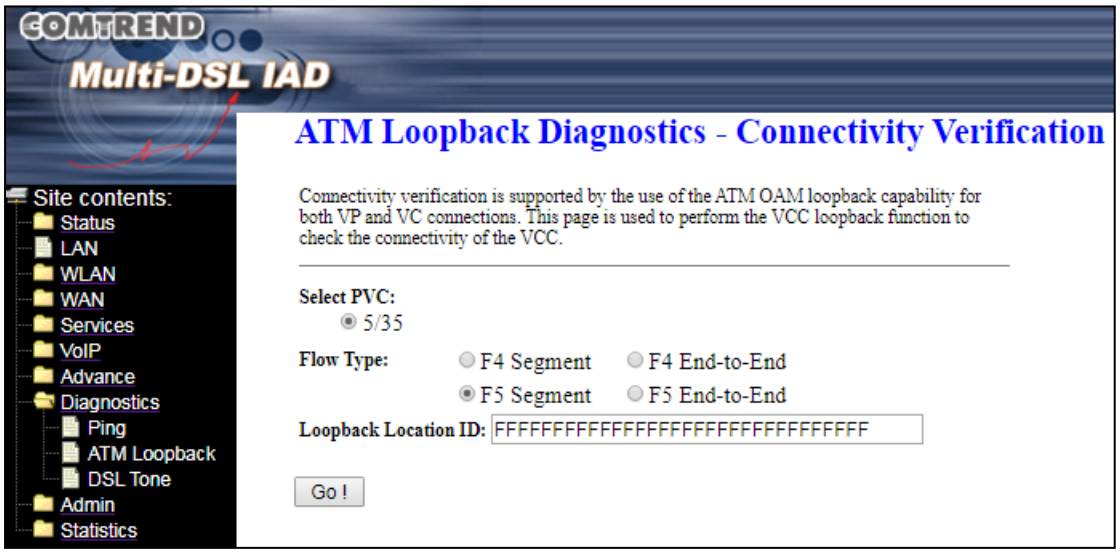


Please see the test result below for reference.

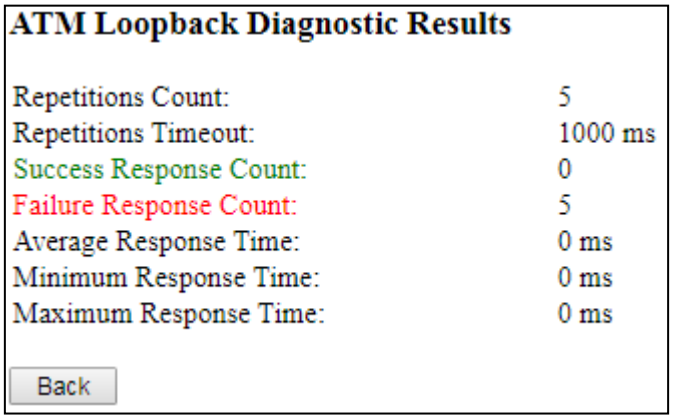


9.8.2 ATM Loopback

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.

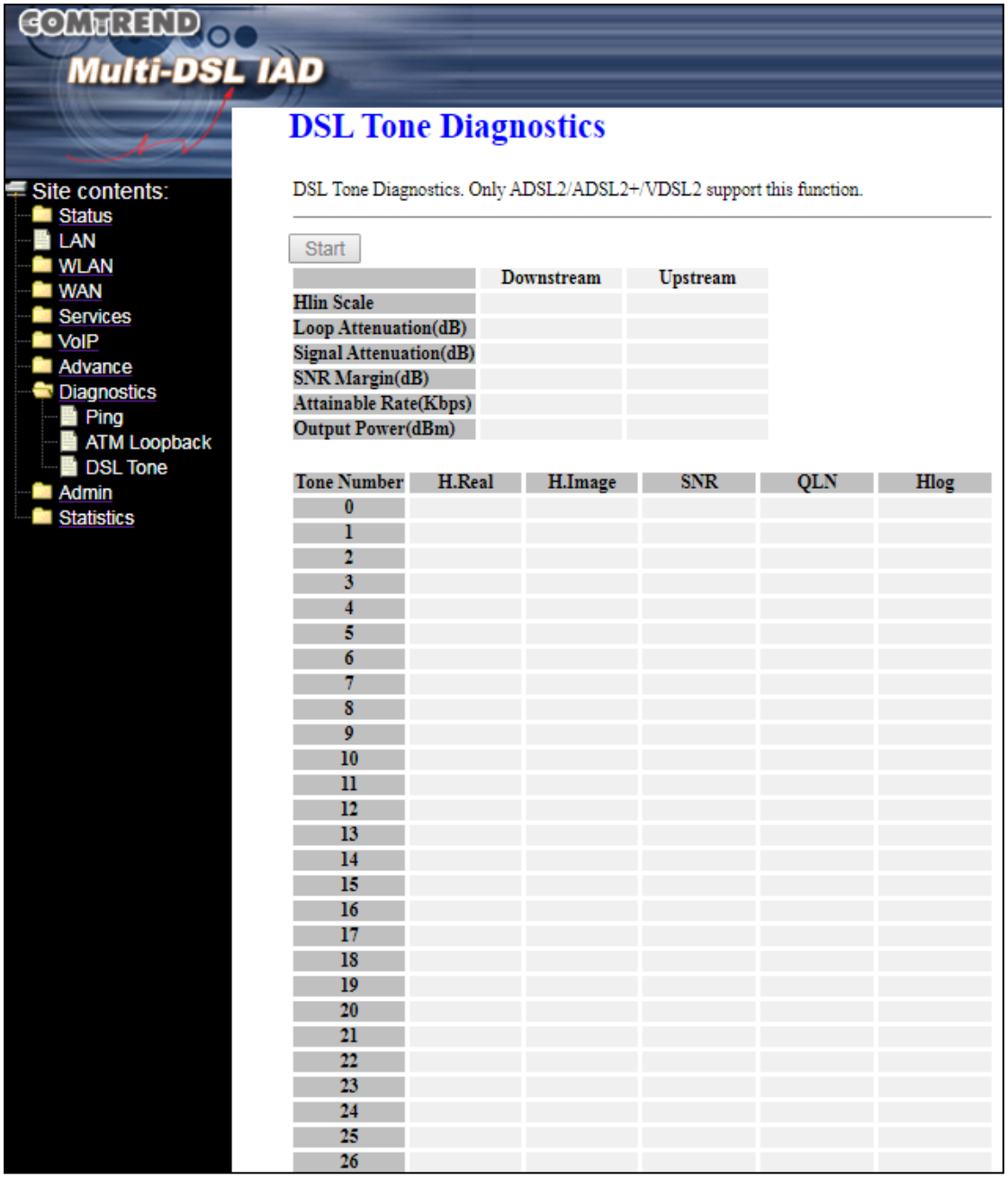


Click the **Go!** button to see the result.



9.8.3 DSL Tone

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



9.9 IPv6

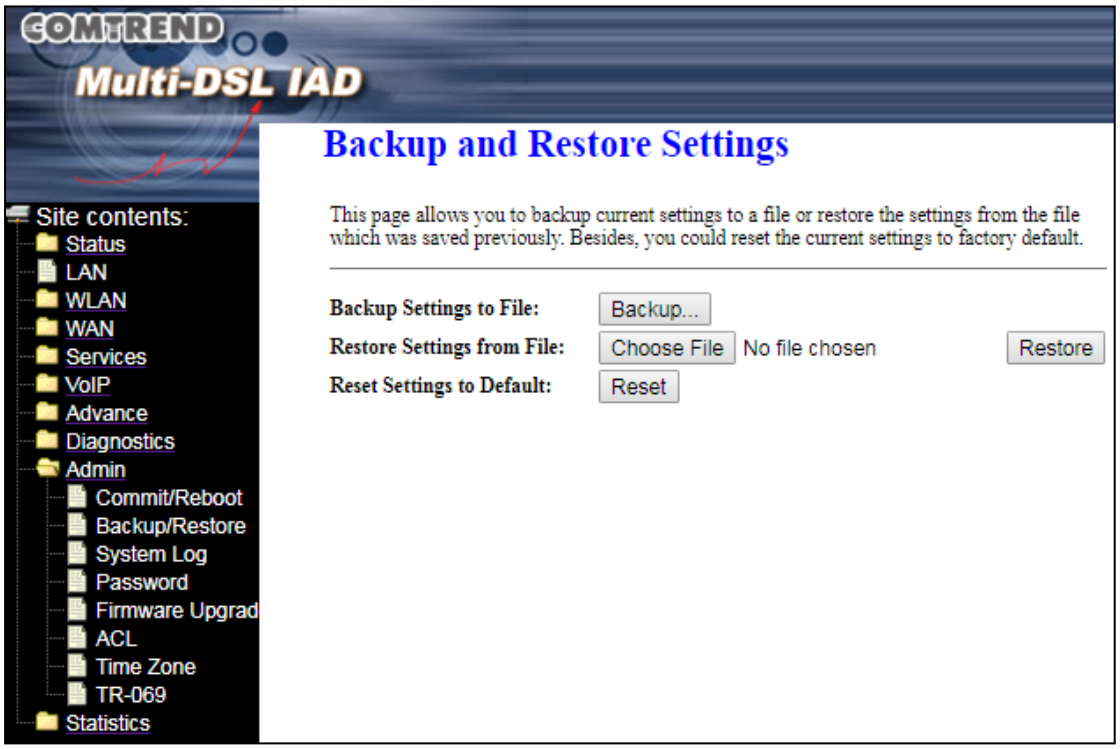
9.9.1 Commit/Reboot

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.

9.9.2 Backup/Restore

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



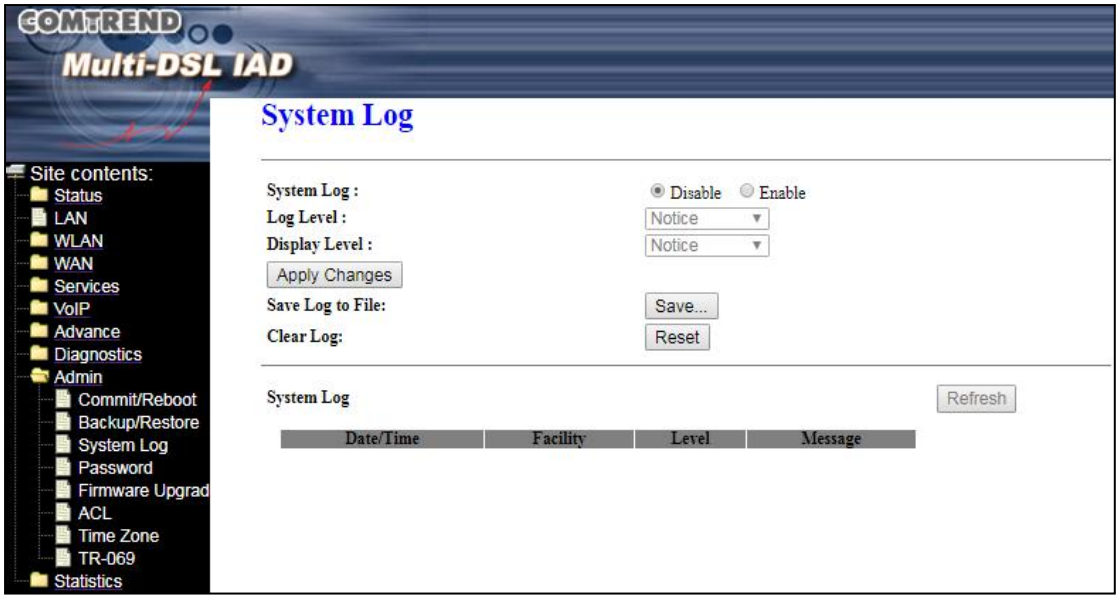
Click the **Backup** button to backup your settings to a file.

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.

9.9.3 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.

Field/Header	Description
System Log	Select the Enable/Disable radio button depending on your requirements
Log Level	Select the log level from the drop-down menu
Display Level	Select the display level from the drop-down menu

9.9.4 Password

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

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

Field/Header	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

9.9.5 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.

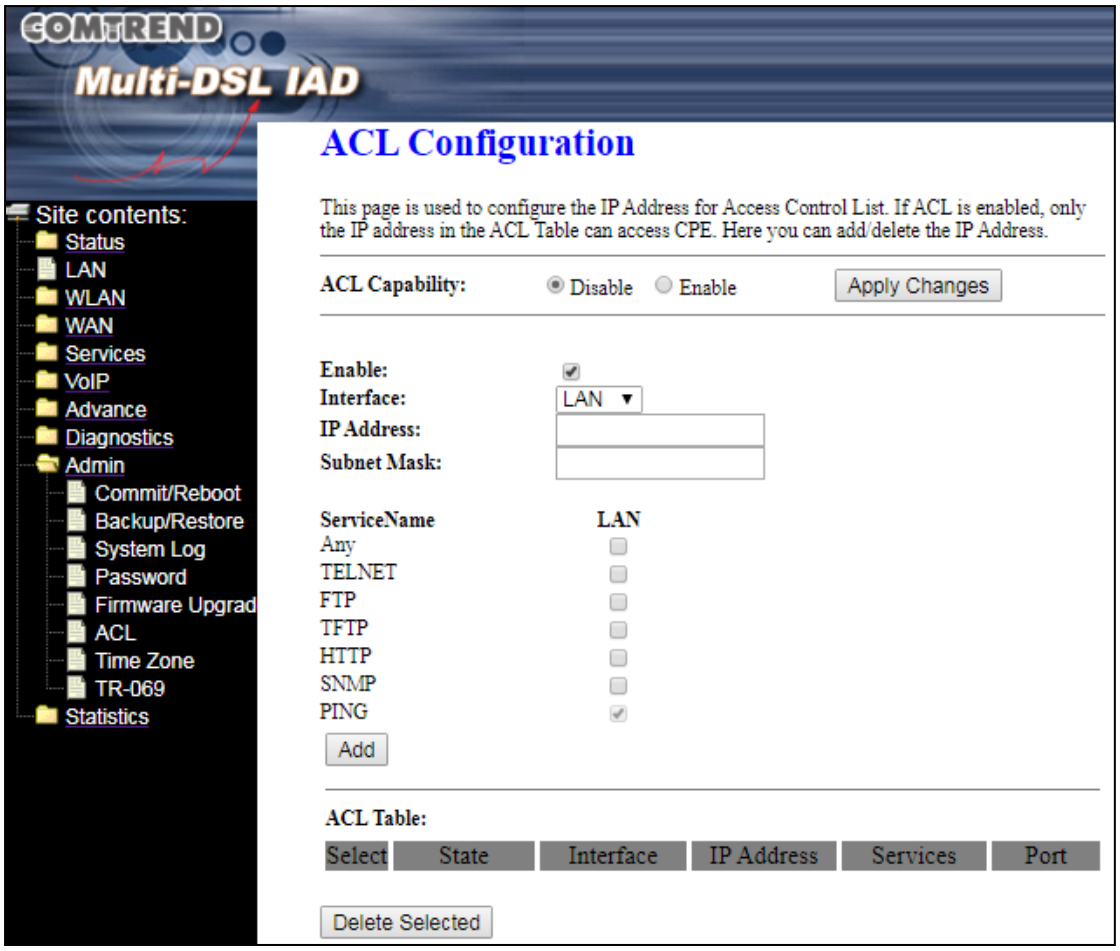
STEP 2: Click the **Browse** button to locate the image file.

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

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

9.9.6 ACL

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

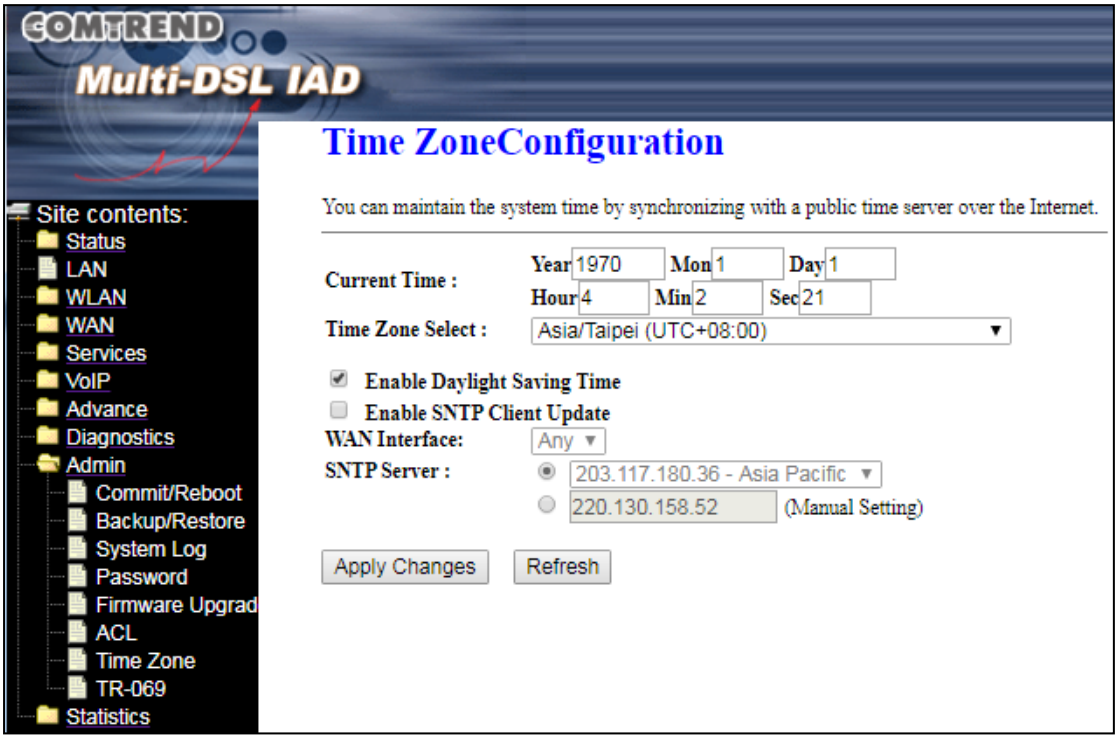


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
ACL Capability	Tick the checkbox to enable or disable ACL
Enable	Tick the checkbox to enable ACL entry
Interface	Select the required interface from the drop-down menu
Service Name / LAN	Tick the checkbox to select service type

9.9.7 Time Zone

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

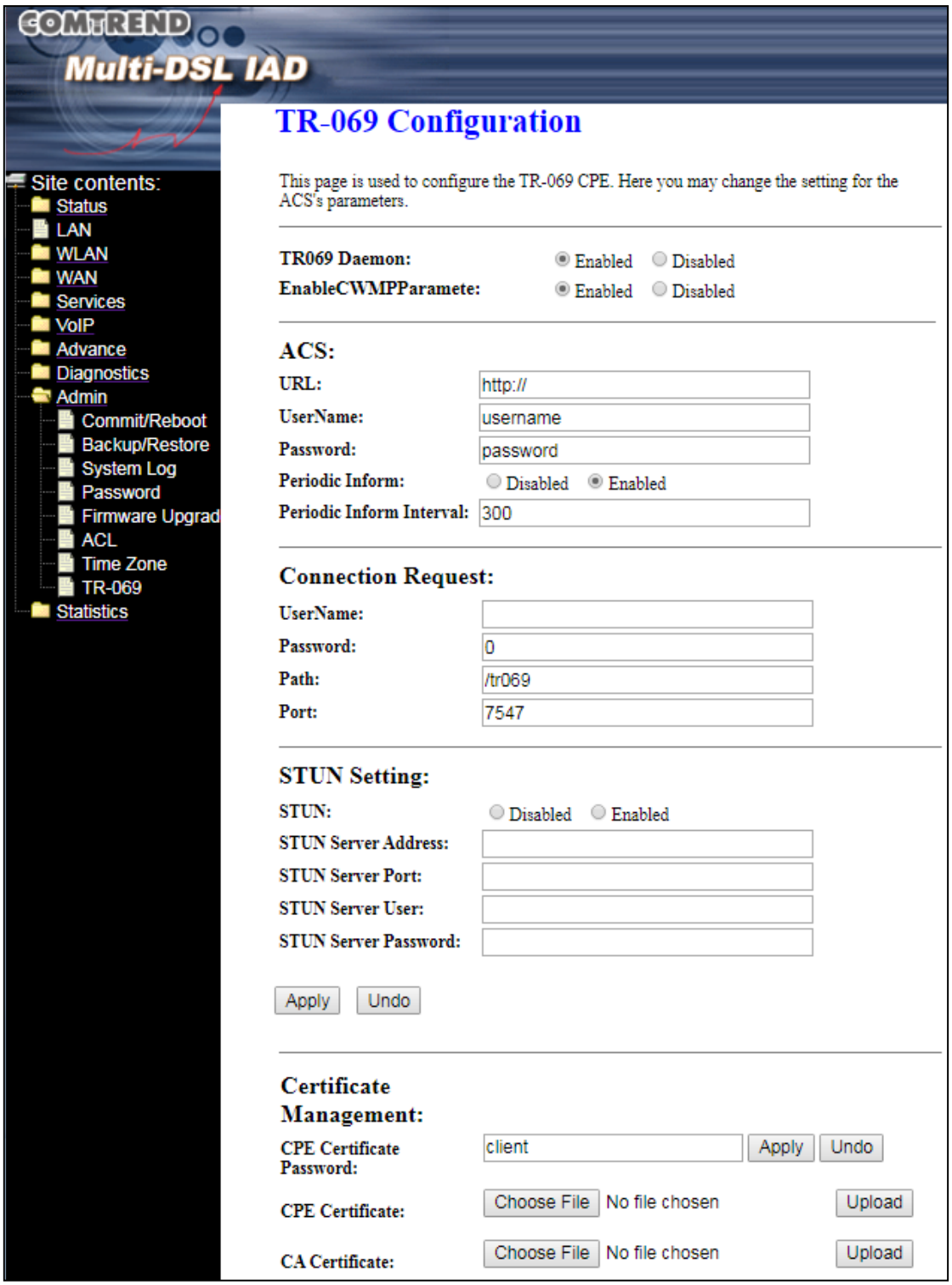


Click the **Apply Changes** button for your changes to take effect.

Field/Header	Description
Current Time	Input the current date and time
Time Zone Select	Select the time zone for your region
Enable Daylight Saving Time	Tick the checkbox to enable daylight saving time
Enable SNTP Client Update	Tick the checkbox to enable SNTP (Simple Network Time Protocol)
WAN Interface	Select the WAN interface from the drop-down menu
SNTP Server	Select SNTP server or manually input the SNTP server IP address

9.9.8 TR-069

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

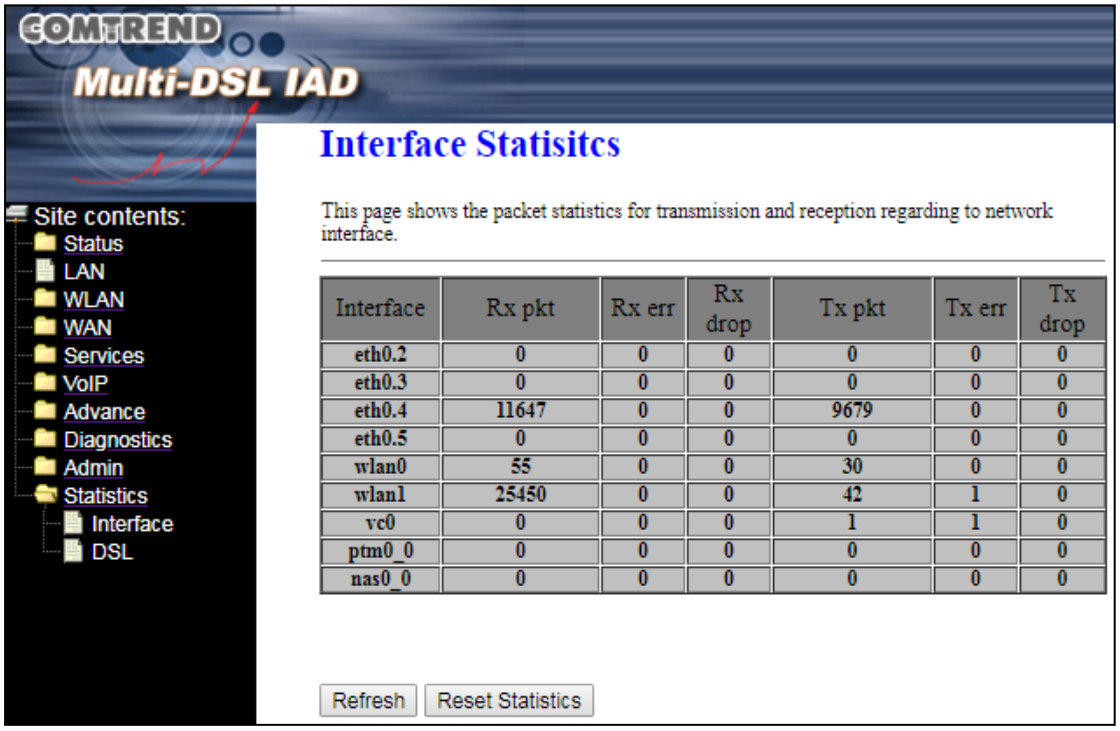


Field/Header	Description
TR069 Daemon	Select the Enable/Disable radio button depending on your requirements
Enable CWMP Parameter	Select the Enable/Disable radio button depending on your requirements
ACS	
URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
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	Select the Enable/Disable radio button depending on your requirements
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
Connection Request	
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
STUN Setting	
STUN	Select the Enable/Disable radio button depending on your requirements
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
Certificate Management	
CPE Certificate Password	Input the Certificate Password
CPE Certificate	Click the **Choose File** button to select the required file. Then, click the **Upload** button.
CA Certificate	Click the **Choose File** button to select the required file. Then, click the **Upload** button.

9.10 Statistics

9.10.1 Interface

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



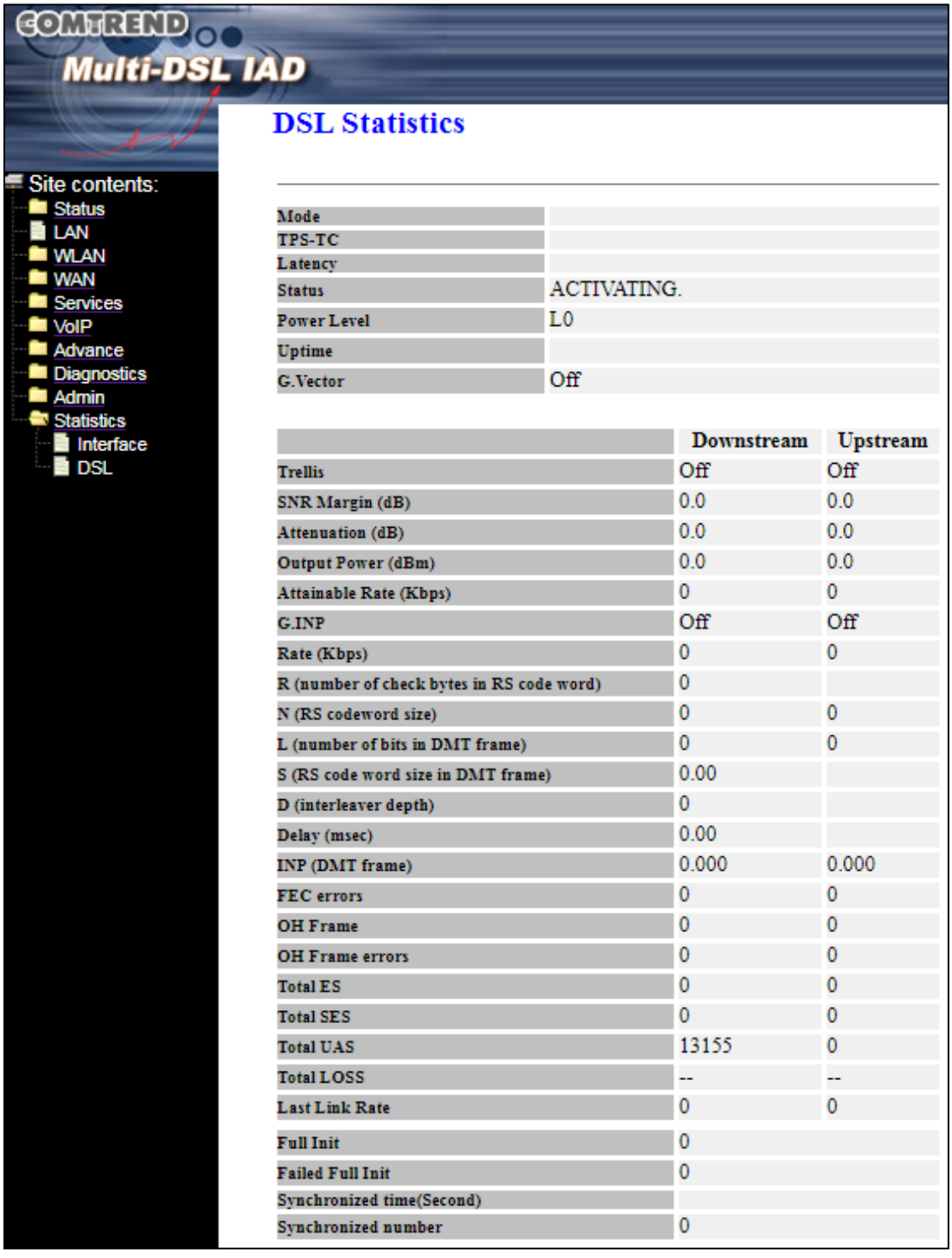
Click the **Refresh** button to reload the page.

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

Field/Header	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

9.10.2 DSL

This page shows the DSL statistics.



Field/Header	Description
Mode	Displays the xDSL type
TPS-TC	Displays PTM or ATM

Field/Header	Description
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
Downstream/Upstream	
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

· Chipset: RTL8685FB (CPU) + RTL8275-VS (AFE) + RTL8192FR-CG (2.4GHz) + RTL8812FR-CG (5GHz)

· Interfaces: 1 x DSL Port, 1 x 10/100/1000Mbps WAN Port, 4 x 10/100/1000Mbps LAN Ports, 1 x USB2.0

· Power Supply: DC 12V 1.5A

· Memory: 16MB FLASH / 128MB DRAM (embedded)

· Antenna: 4x internal antennas

· Dimensions (WxDxH): 186x151x30mm

General

· DSL Standards: VDSL2, ADSL2/2+, ADSL

· Wireless Standards: IEEE802.11a/n/ac,5GHz, IEEE802.11b/g/n,2.4GHz

· Signal Rate: 5GHz: Up to 876Mbps,
2.4GHz: Up to 300Mbps

· Operation Frequency: 2.4GHz & 5GHz

· Reception Sensitivity:
5GHz:
11a 6Mbps: -96dBm, 11a 54Mbps: -79dBm
11ac HT20: -71dBm, 11ac HT40: -66dBm, 11ac HT80: -63dBm,
11n HT20: -72dBm, 11n HT40: -71dBm

2.4GHz:
11g 54M: -77dBm
11n HT20: -74dBm, 11n HT40: -72dBm

· Wireless Security: WEP, WPA / WPA2, WPA-PSK/WPA2-PSK encryption

Software Features

· WAN Type: ATM/PTM/ETH/Dongle

· DHCP: Server, Client, DHCP Client List, Address Reservation

· Quality of Service: WMM, Bandwidth Control

· Port Forwarding: Virtual Server, Port Triggering, UPnP, DMZ

· VPN Pass-Through: PPTP, L2TP, IPSec

· Access Control: Parental Control, Local Management Control, Host List, Access Schedule, Rule management

· Firewall Security:
DoS, SPI Firewall, IP Address Filter / MAC Address Filter / Domain Filter, IP and MAC Address Binding

· USB Sharing: Support Samba (Storage) / FTP Server, Media Server / Printer Server / DLNA

· Management: Access Control, Local Management, Remote Management

· Internet Protocol: IPv4, IPv6

Environment

· Operating Temperature: 0°C~40°C (32°F~104°F)

· Storage Temperature: -40°C~70°C (-40°F~158°F)

· Relative Humidity: 10%~90%, non-condensing

· Storage Humidity: 5%~90%, non-condensing

Kit Weight
(1* VR-3047eu, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter)

NOTE:	Specifications are subject to change without notice.

Appendix C - SSH Client

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

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

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

To access the router using the Linux ssh client

For LAN access, type: ssh -l 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