# WR-6891u

## FTTH Gateway

## User Manual

Version A1.0, May 28, 2015

## 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. awet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

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

## ⚠ WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix C – Specifications.

## Copyright

**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

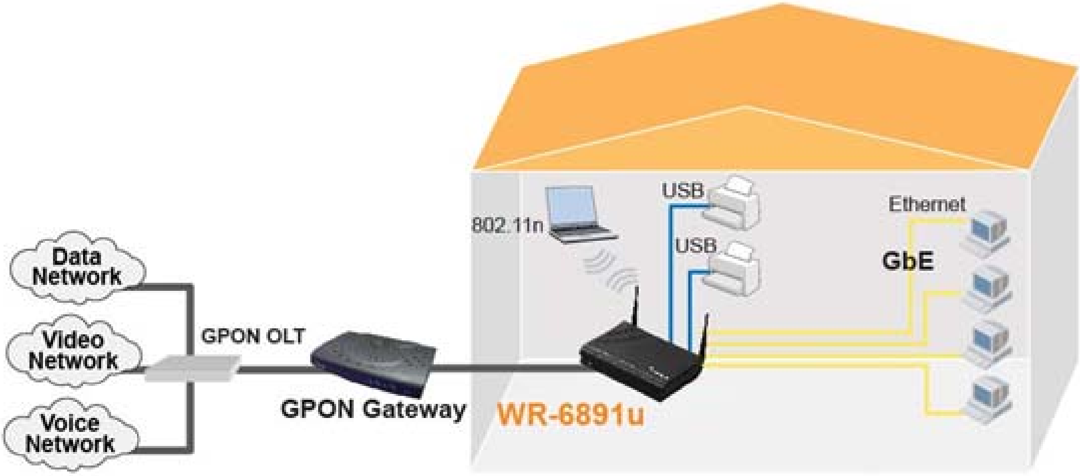
# Chapter 1 Introduction

The WR-6891u is an 802.11n 2.4GHz concurrently compliant VoIP Gateway. It employs a 10/100/1000 Base-T Gigabit Ethernet port for WAN, four 10/100/1000 Base-T Gigabit Ethernet ports for LAN, one USB Host, one WiFi On-Off/WPS button, and an integrated 802.11n 2.4GHz(2T2R) for WLAN Access Point (AP), which is backward compatible with 802.11b/g; therefore WR-6891u allows both wired LAN connectivity and wireless connectivity. It is also capable of facilitating predictable, real-time, toll-quality voice over the Internet.

WR-6891u connects to xDSL or GPON (Gigabit-Capable Passive Optical Network) modem and supports state-of-the-art security features such as WPA data encryption, Firewall & VPN pass through. It is designed for both residential and business applications that require wireless and wired connectivity. WR-6891u is also designed with a TR-068 compliant color panel and LED indicators for easy installation and user-friendliness. WR-6891u supports Triple services (Data+VoIP+IPTV) by wired or wireless protocol.

## 1.1 Application

The following diagram depicts the application of the WR-6891u with GPON.



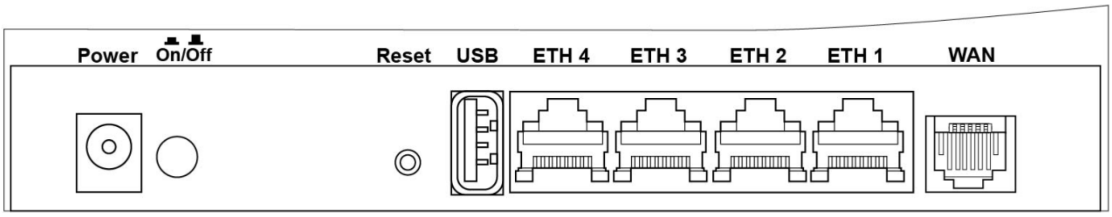
# Chapter 2 Installation

## 2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

**BACK PANEL**

The figure below shows the back panel of the device.



**Power ON**

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

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

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

**Reset Button**

Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section 2.2 LED Indicators).

**NOTE:** If pressed down for more than 20 seconds, the WR-6891u 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.

**USB HOST PORT**

Two USB 2.0 host ports support compatible printers. See Appendix G for setup instructions. Support for other devices may be added in future firmware upgrades.

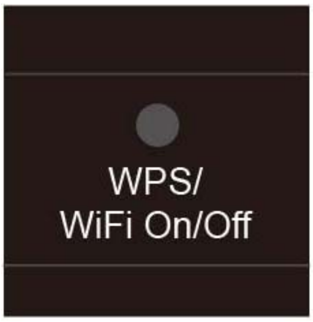
**ETH PORTS**

Use 1000-BASE-T RJ-45 cables to connect up to four network devices to a Gigabit LAN, or 10/100BASE-T RJ-45 cables for slower networks. As these ports are auto-sensing MDI/X, either straight-through or crossover cable can be used.

**ETH WAN PORT**

This port has the same features as the LAN ports described above with additional Ethernet WAN functionality.

## FRONT PANEL

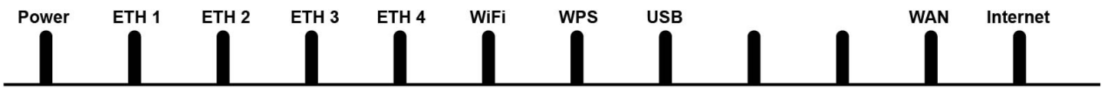


### WPS / WLAN Switch

Press the WPS/WIFI button for 5 seconds to enable the WIFI function (then WIFI led should light up). Press for another 5 seconds to enable WPS which will allow 5 minutes for WIFI connection. To disable WIFI, press the WPS/WIFI button for 10 seconds and then WLAN led should go off.

## 2.2 LED Indicators

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



| LED | Color | Mode | Function |
|---|---|---|---|
| POWER | GREEN | On | The device is powered up. |
| | | Off | The device is powered down. |
| | RED | On | POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. |
| ETH 1X-4X | GREEN | On | An Ethernet Link is established. |
| | | Off | An Ethernet Link is not established. |
| | | Blink | Data transmitting or receiving over LAN. |
| WiFi | GREEN | On | The wireless module is ready. (i.e. installed and enabled). |
| | | Off | The wireless module is not ready. (i.e. either not installed or disabled). |
| | | Blink | Data transmitting or receiving over WLAN. |
| WPS enabled and PC connected to WLAN WPS disabled when WPS configured | WPS enabled and PC connected to WLAN WPS disabled when WPS configured | WPS enabled and PC connected to WLAN | WPS enabled and PC connected to WLAN. |
| | | WPS disabled when WPS configured | WPS disabled when WPS configured. |
| | | The router is searching for WPS clients or WPS un-configured. | The router is searching for WPS clients or WPS un-configured. |
| USB | GREEN | On | No device is connected to the any USB ports or a device is connected to any USB port but not active. |
| | | Off | At least one device is connected to any USB port and active. |
| | | Blink | Data TX/RX through at least one of the USB ports. |

| | | | |
|---|---|---|---|
| WAN | GREEN | On | An Ethernet WAN Link is established. |
| | | Off | An Ethernet WAN Link is not established. |
| | | On | Data transmitting or receiving over Ethernet WAN. |
| INTERNET | GREEN | On | IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present. |
| | | Off | Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off. |
| | | Blink | IP connected and IP Traffic is passing thru the device (either direction) |
| | RED | On | Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.) |

# Chapter 3 Web User Interface

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

## 3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root** , password: **12345**)
- 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 te lnet user interface, or ot her management protocols. The factory default configuration can be restored either by pushing the reset button for more than five 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 WR-6891u 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.

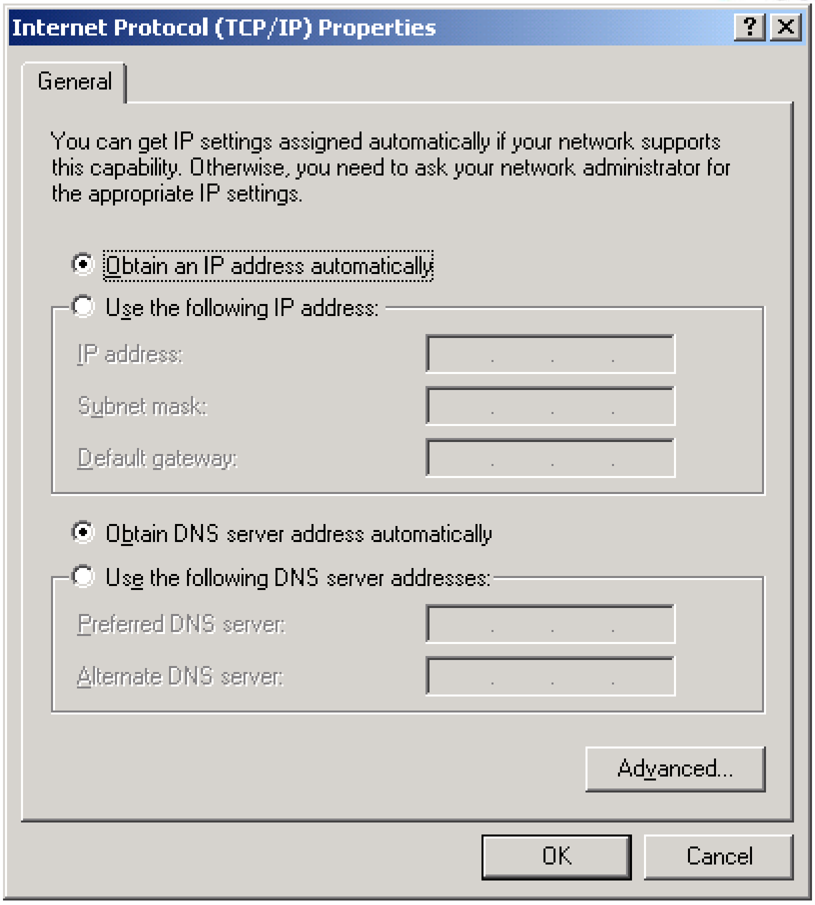
To obtain an IP address from the DCHP server, follow the steps provided below.

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

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

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

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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

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

### STATIC IP MODE

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

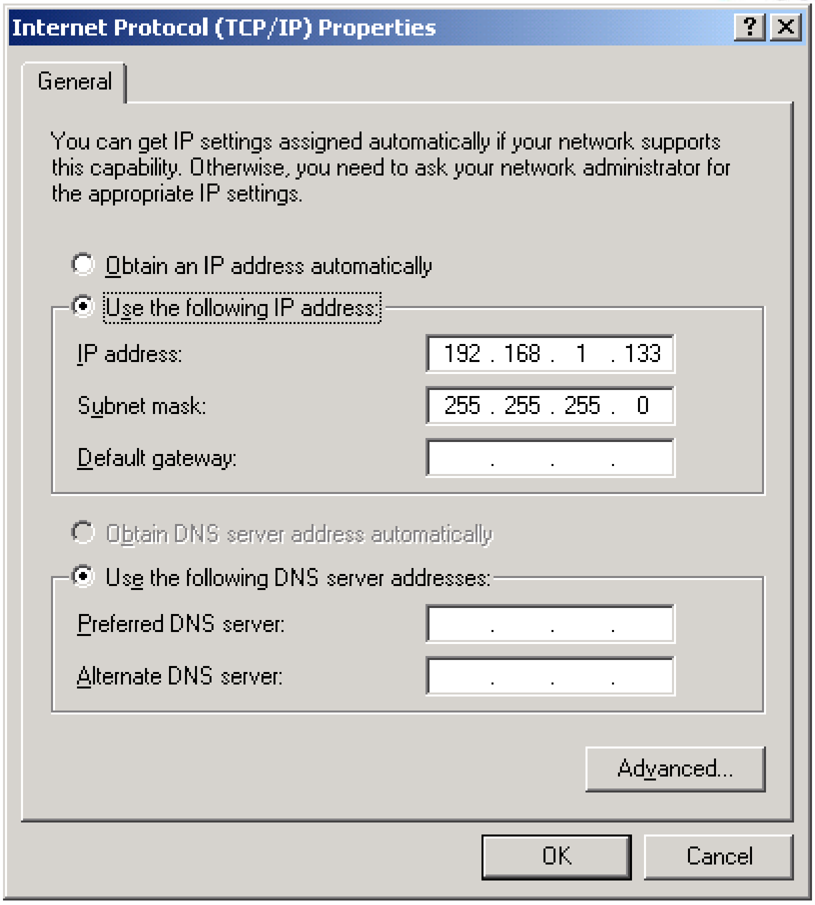
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

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

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

**STEP 3:** Change the IP address to the 192.168.1.x (2<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 133

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

## 3.3 Login Procedure

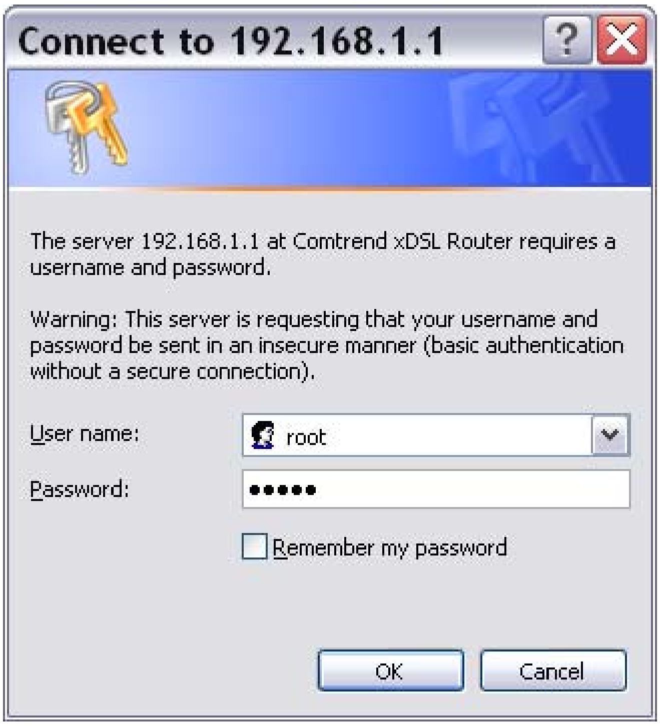
Perform the following steps to login to the web user interface.

| | |
|---|---|
| **NOTE:** | The default settings can be found in Section 3.1. |

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

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

**STEP 2:** A dialog box will appear, such as the one below. Enter the default username and password, as defined in 3.1 Default Settings.



Connect to 192.168.1.1

The server 192.168.1.1 at Comtrend xDSL Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: root

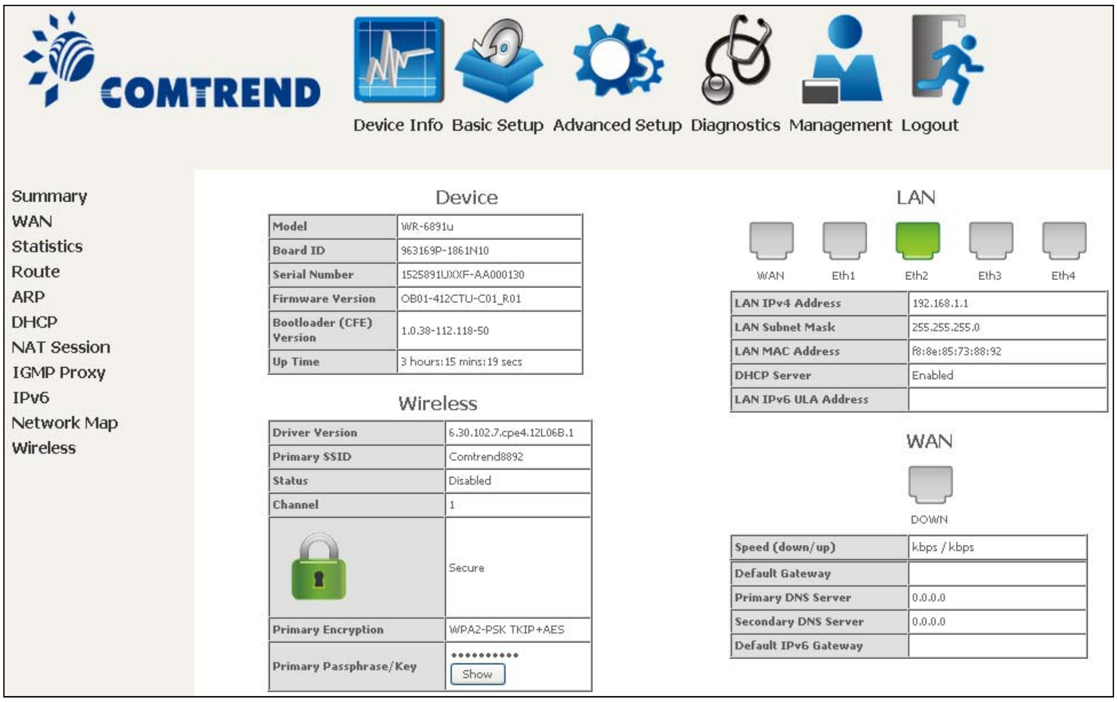
Password: •••••

□ Remember my password

Click **OK** to continue.

| | |
|---|---|
| **NOTE:** | The login password can be changed later (see 8.6.1 Passwords) |

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



Device

| | |
|---|---|
| Model | WR-6891u |
| Board ID | 963169P-1861N10 |
| Serial Number | 1525891UXXF-AA000130 |
| Firmware Version | OB01-412CTU-C01_R01 |
| Bootloader (CFE) Version | 1.0.38-112.118-50 |
| Up Time | 3 hours:15 mins:19 secs |

Wireless

| | |
|---|---|
| Driver Version | 6.30.102.7.cpe4.12L06B.1 |
| Primary SSID | Comtrend8892 |
| Status | Disabled |
| Channel | 1 |
| | Secure |
| Primary Encryption | WPA2-PSK TKIP+AES |
| Primary Passphrase/Key | •••••••••• |

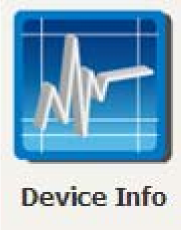
LAN

| | |
|---|---|
| LAN IPv4 Address | 192.168.1.1 |
| LAN Subnet Mask | 255.255.255.0 |
| LAN MAC Address | f8:8e:85:73:88:92 |
| DHCP Server | Enabled |
| LAN IPv6 ULA Address | |

WAN

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

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



# Chapter 4 Device Information

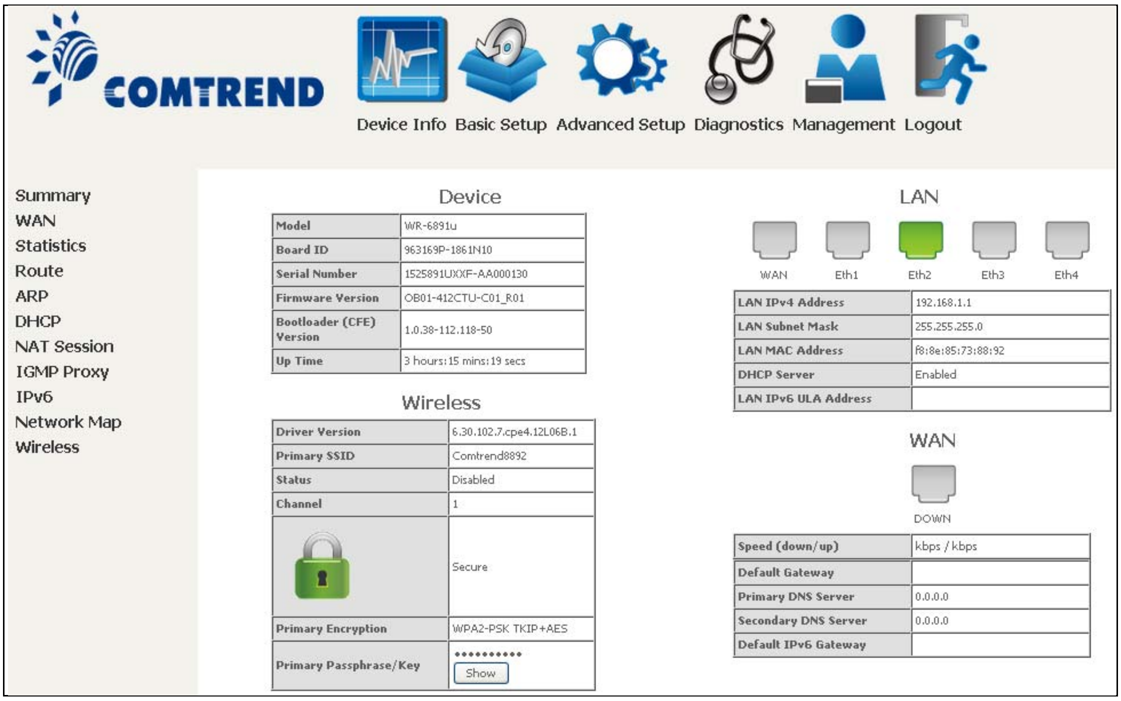
You can reach this page by clicking on the following icon located at the top of the screen.

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

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

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

The Device Info Summary screen displays at startup.



Device

| | |
|---|---|
| Model | WR-6891u |
| Board ID | 963169P-1861N10 |
| Serial Number | 1525891UXXF-AA000130 |
| Firmware Version | OB01-412CTU-C01_R01 |
| Bootloader (CFE) Version | 1.0.38-112.118-50 |
| Up Time | 3 hours:15 mins:19 secs |

Wireless

| | |
|---|---|
| Driver Version | 6.30.102.7.cpe4.12L06B.1 |
| Primary SSID | Comtrend8892 |
| Status | Disabled |
| Channel | 1 |
| | Secure |
| Primary Encryption | WPA2-PSK TKIP+AES |
| Primary Passphrase/Key | •••••••••• |

LAN

| | |
|---|---|
| LAN IPv4 Address | 192.168.1.1 |
| LAN Subnet Mask | 255.255.255.0 |
| LAN MAC Address | f8:8e:85:73:88:92 |
| DHCP Server | Enabled |
| LAN IPv6 ULA Address | |

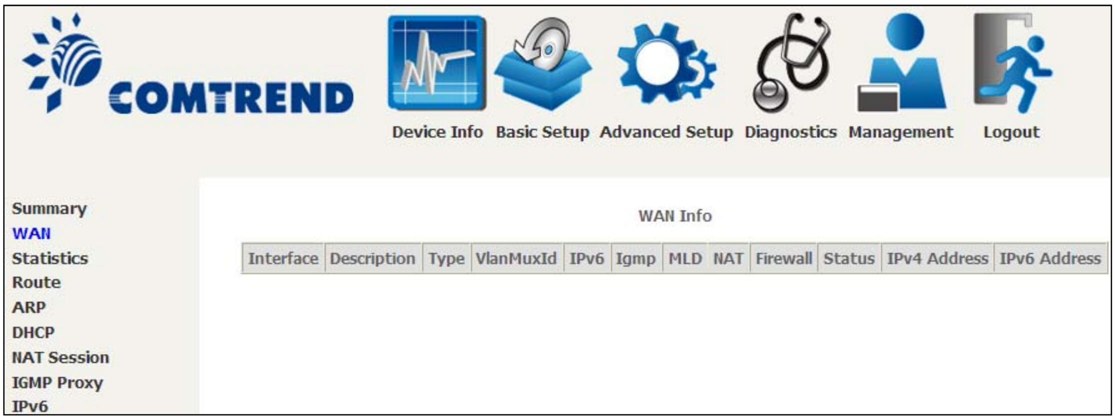
WAN

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

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

## 4.1 WAN

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



WAN Info

| Interface | Description | Type | VlanMuxId | IPv6 | Igmp | MLD | NAT | Firewall | Status | IPv4 Address | IPv6 Address |
|---|---|---|---|---|---|---|---|---|---|---|---|

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

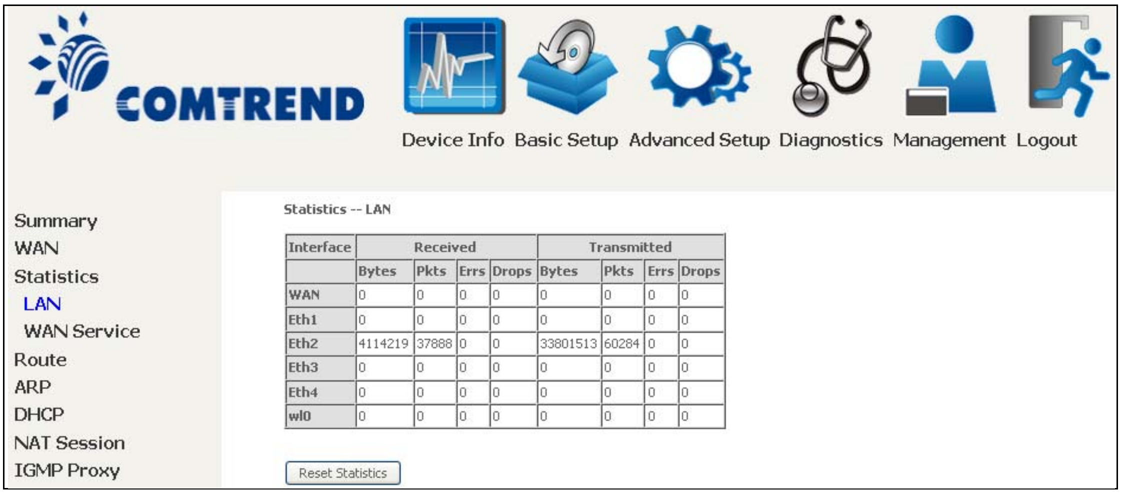
## 4.2 Statistics

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

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

### 4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.



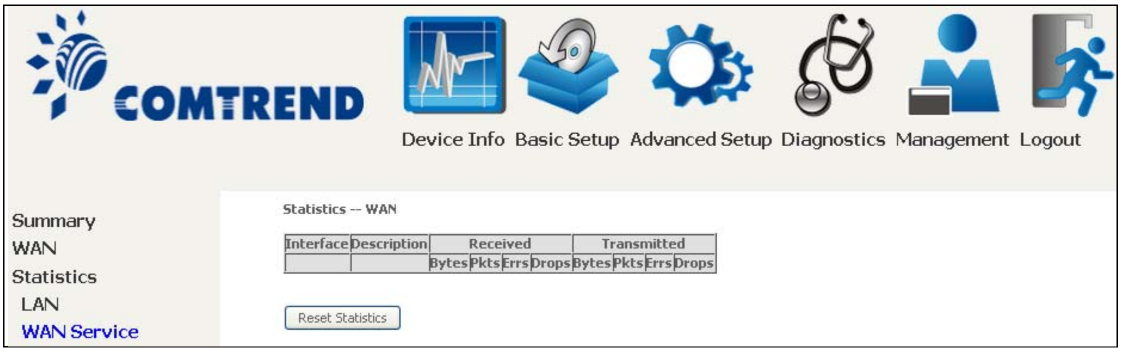
Statistics -- LAN

| Interface | Received | | | | Transmitted | | | |
|---|---|---|---|---|---|---|---|---|
| | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Errs | Drops |
| WAN | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Eth1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Eth2 | 4114219 | 37888 | 0 | 0 | 33801513 | 60284 | 0 | 0 |
| Eth3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Eth4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| wl0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| **Heading** | | **Description** |
|---|---|---|
| Interface | | LAN interface(s) |
| Received/Transmitted: | - Bytes<br>- Pkts<br>- Errs<br>- Drops | Number of Bytes<br>Number of Packets<br>Number of packets with errors<br>Number of dropped packets |

### 4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.



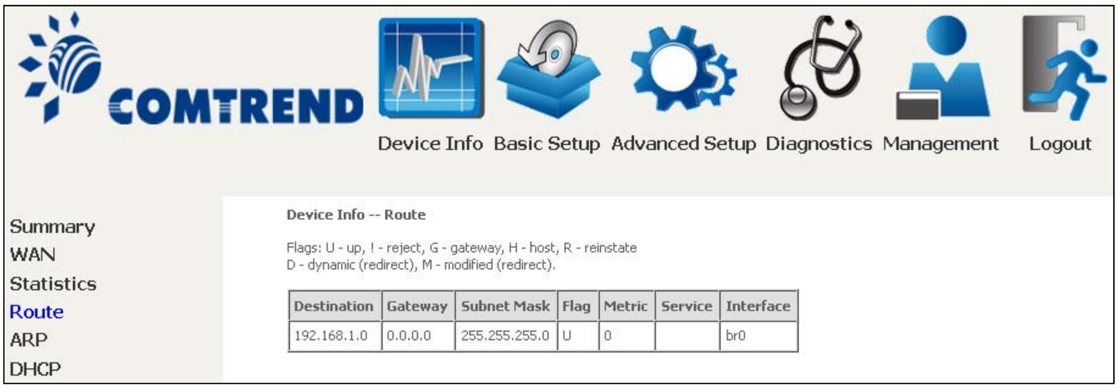
Statistics -- WAN

| Interface | Description | Received | | | | Transmitted | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Errs | Drops |
| | | | | | | | | | |

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

## 4.3 Route

Choose **Route** to display the routes that the WR-6891u has found.



Device Info -- Route

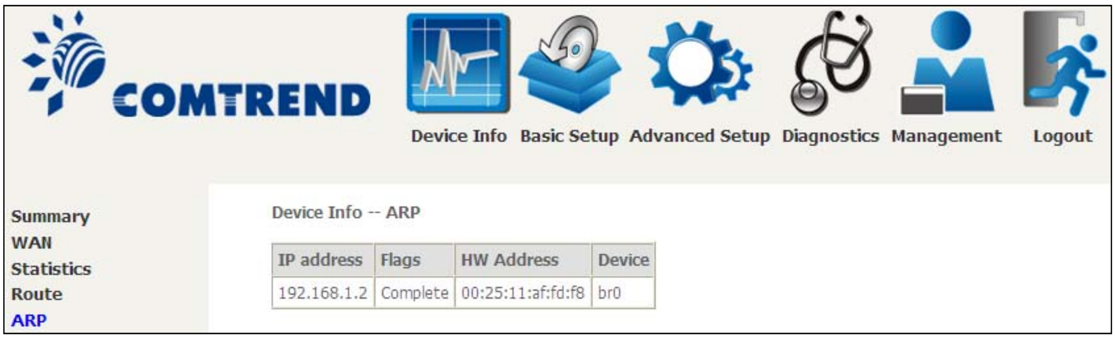
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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

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

## 4.4 ARP

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



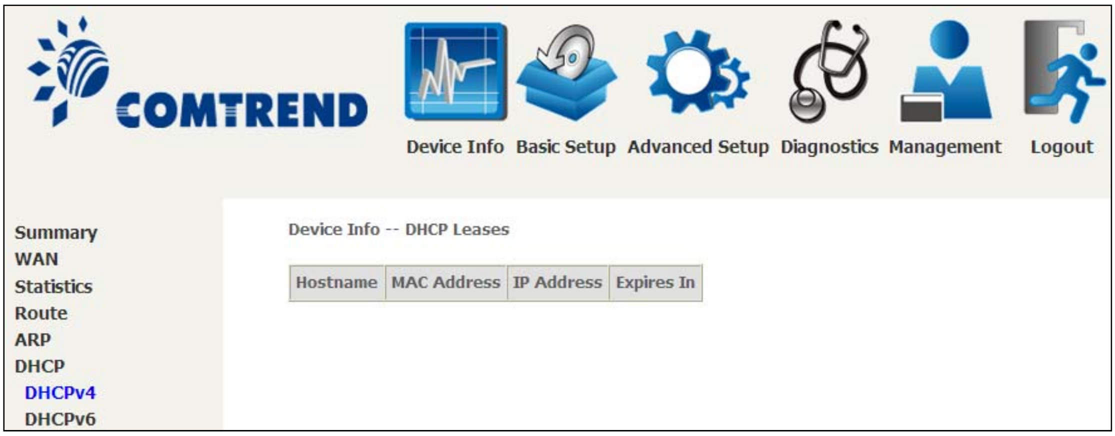
Device Info -- ARP

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

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

## 4.5 DHCP

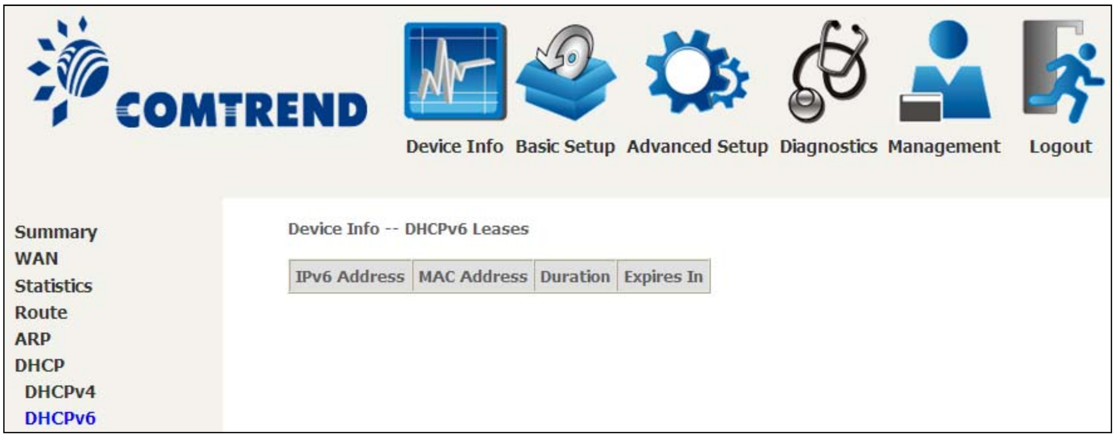
Click **DHCP** to display all DHCP Leases.



Device Info -- DHCP Leases

| Hostname | MAC Address | IP Address | Expires In |
|---|---|---|---|

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

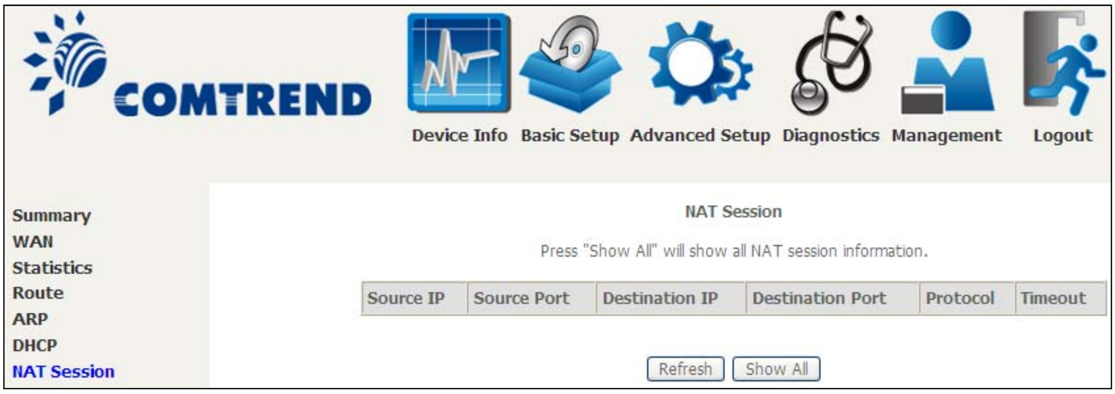


Device Info -- DHCPv6 Leases

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

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

## 4.6 NAT Session

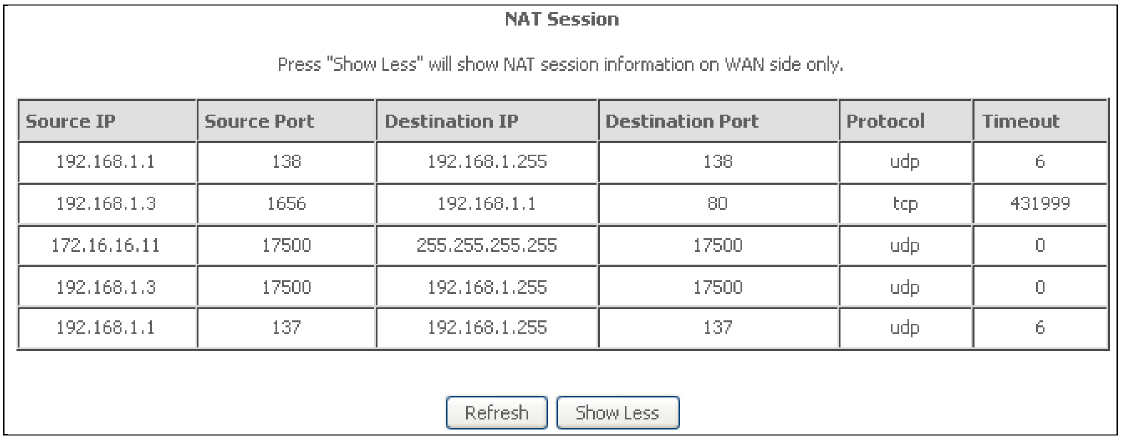


NAT Session

Press "Show All" will show all NAT session information.

| Source IP | Source Port | Destination IP | Destination Port | Protocol | Timeout |
|---|---|---|---|---|---|

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



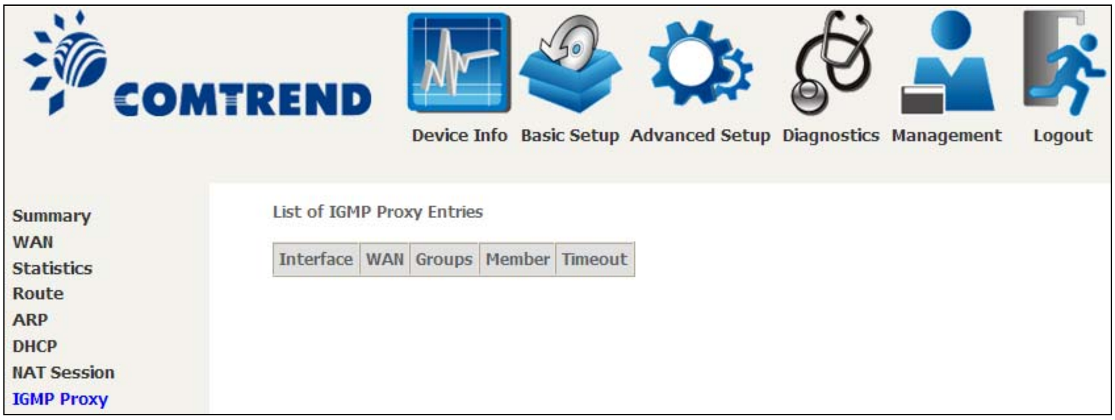
NAT Session

Press "Show Less" will show NAT session information on WAN side only.

| Source IP | Source Port | Destination IP | Destination Port | Protocol | Timeout |
|---|---|---|---|---|---|
| 192.168.1.1 | 138 | 192.168.1.255 | 138 | udp | 6 |
| 192.168.1.3 | 1656 | 192.168.1.1 | 80 | tcp | 431999 |
| 172.16.16.11 | 17500 | 255.255.255.255 | 17500 | udp | 0 |
| 192.168.1.3 | 17500 | 192.168.1.255 | 17500 | udp | 0 |
| 192.168.1.1 | 137 | 192.168.1.255 | 137 | udp | 6 |

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

## 4.7 IGMP Proxy



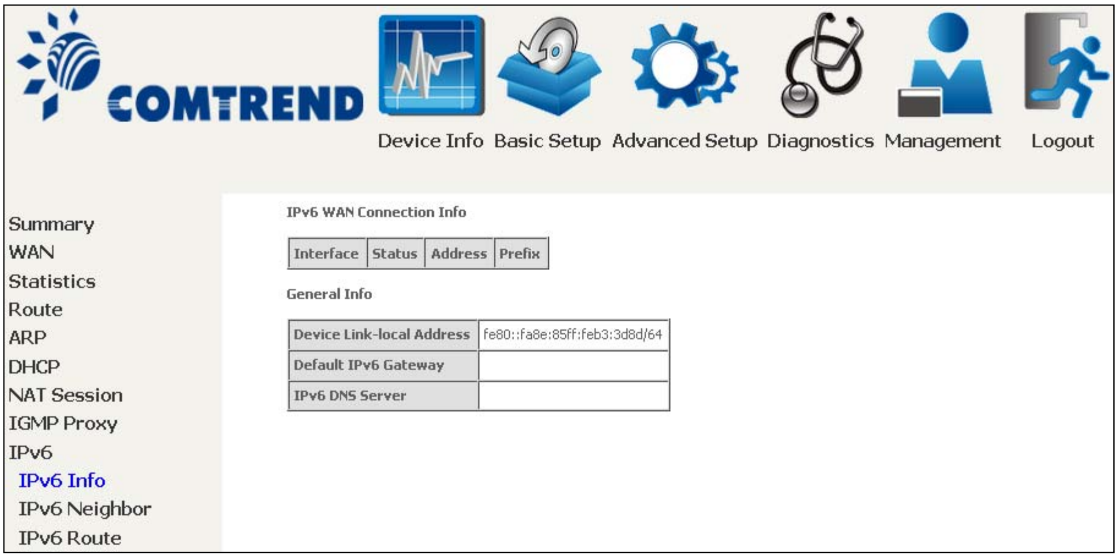
List of IGMP Proxy Entries

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

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

# 4.8 IPv6

## 4.8.1 IPv6 Info



IPv6 WAN Connection Info

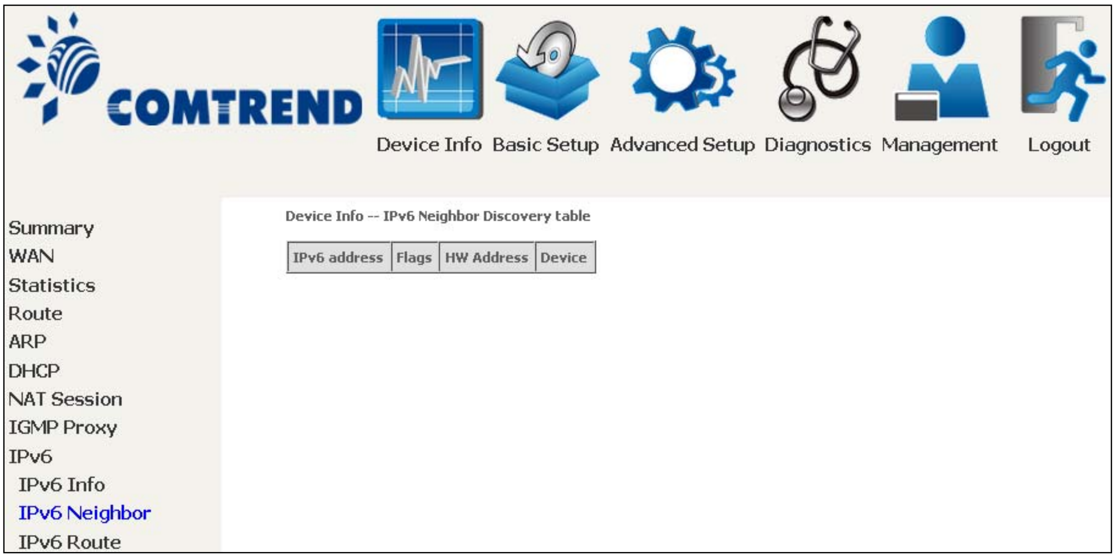
| Interface | Status | Address | Prefix |
|---|---|---|---|

General Info

| | |
|---|---|
| Device Link-local Address | fe80::fa8e:85ff:feb3:3d8d/64 |
| Default IPv6 Gateway | |
| IPv6 DNS Server | |

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

## 4.8.2 IPv6 Neighbor

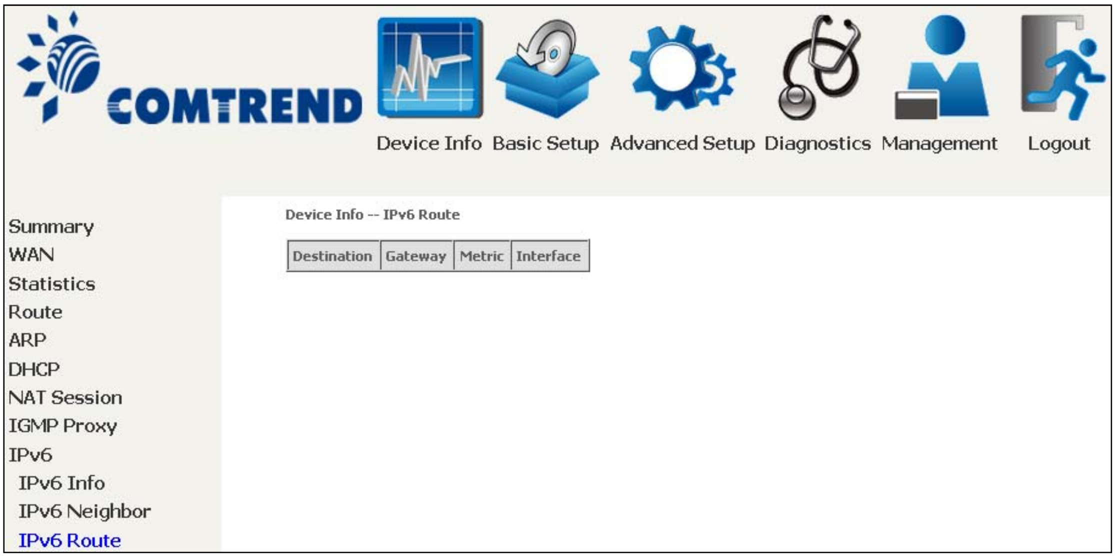


Device Info -- IPv6 Neighbor Discovery table

| IPv6 address | Flags | HW Address | Device |
|---|---|---|---|

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

### 4.8.3 IPv6 Route



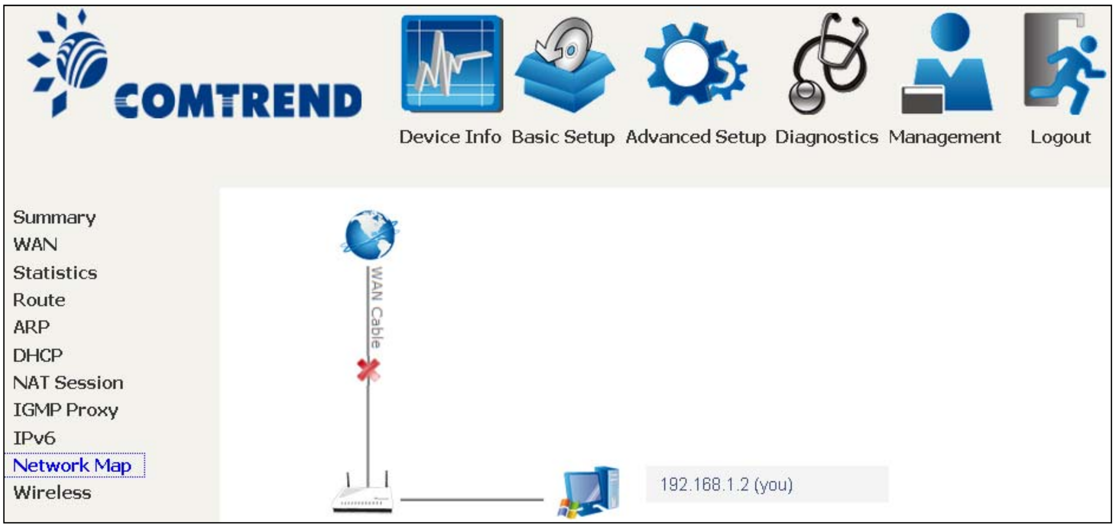
Device Info -- IPv6 Route

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

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

## 4.9 Network Map

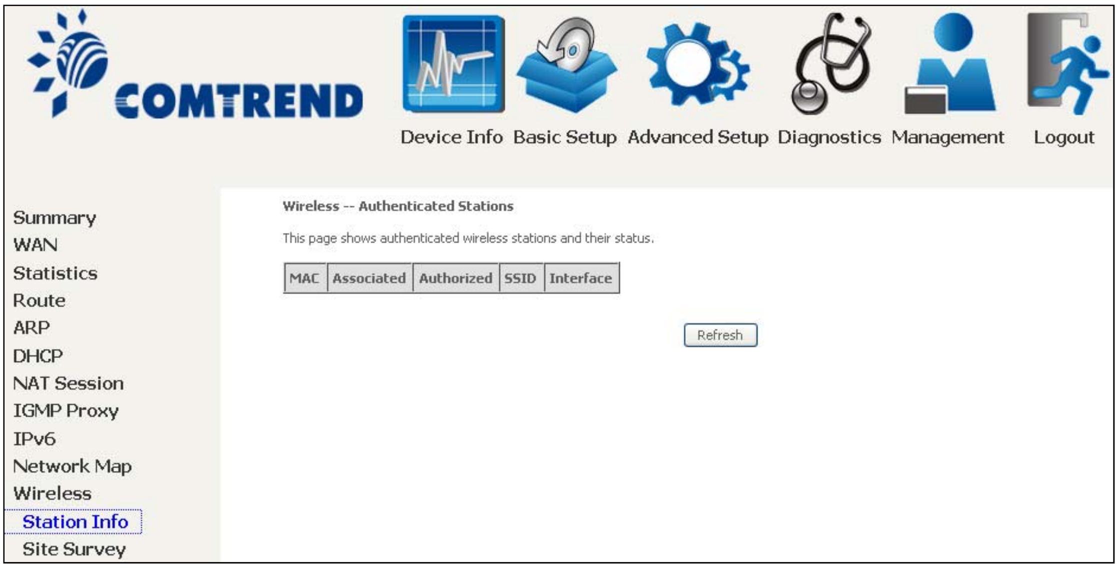
The network map is a graphical representation of router's wan status and LAN devices. The feature is only available using a non-IE browser.



# 4.10 Wireless

## 4.10.1 Station Info

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



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

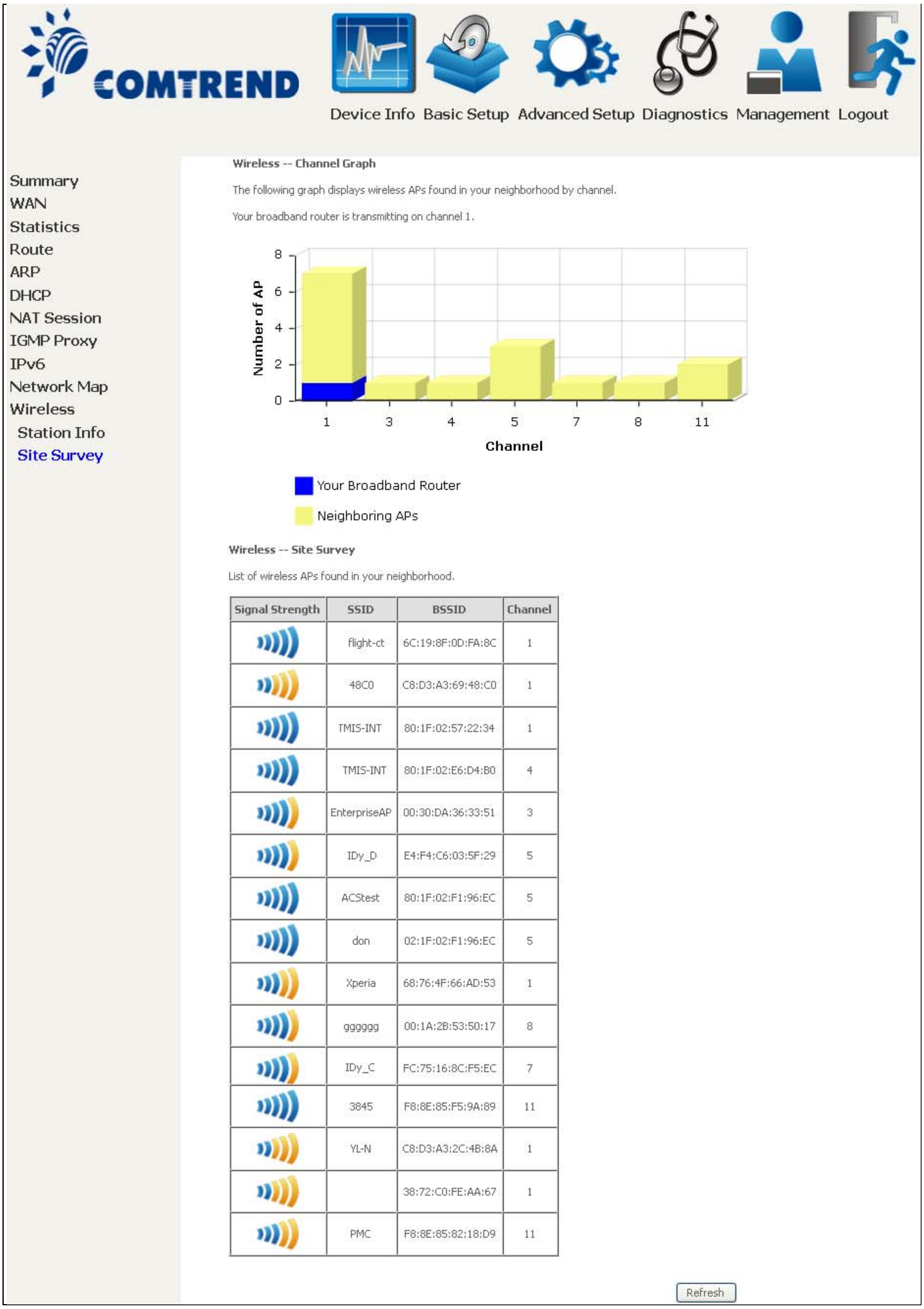
| MAC | Associated | Authorized | SSID | Interface |
|---|---|---|---|---|

Consult the table below for descriptions of each column heading.

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

### 4.10.2 Site Survey

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



**Wireless -- Channel Graph**

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

Your broadband router is transmitting on channel 1.

**Wireless -- Site Survey**

List of wireless APs found in your neighborhood.

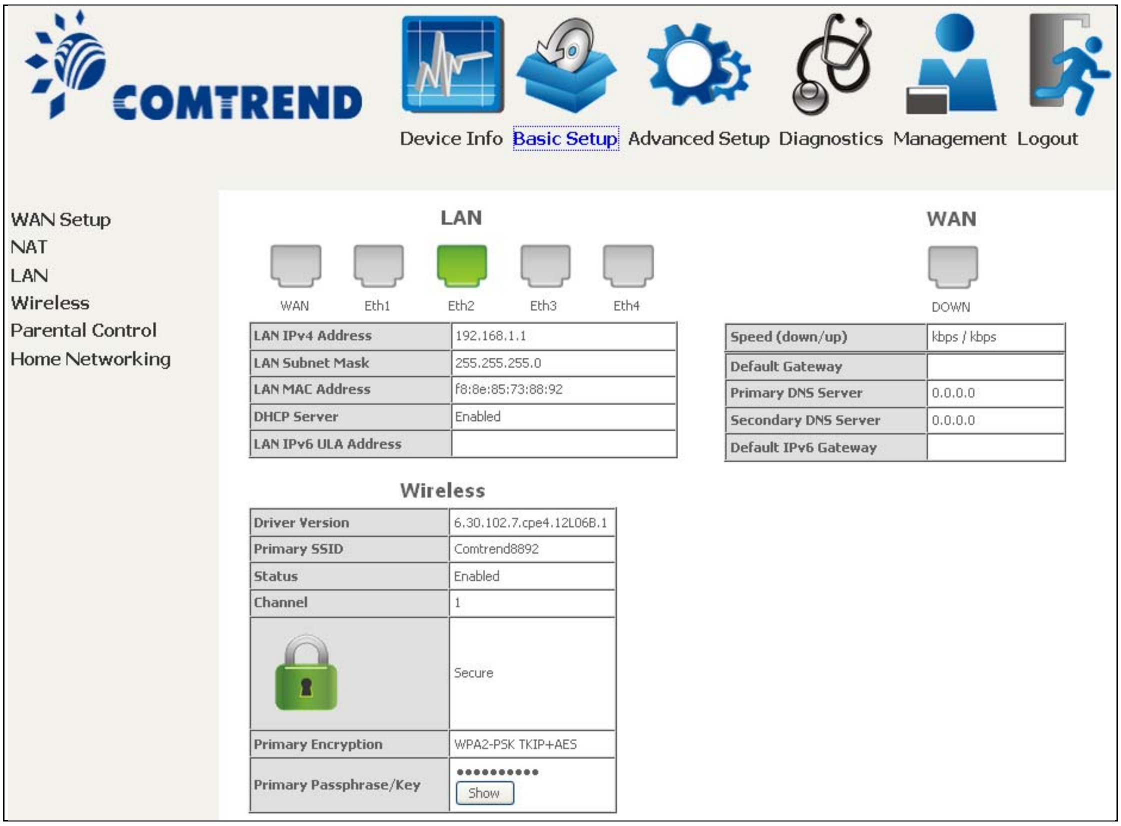
| Signal Strength | SSID | BSSID | Channel |
|---|---|---|---|
| | flight-ct | 6C:19:8F:0D:FA:8C | 1 |
| | 48C0 | C8:D3:A3:69:48:C0 | 1 |
| | TMIS-INT | 80:1F:02:57:22:34 | 1 |
| | TMIS-INT | 80:1F:02:E6:D4:B0 | 4 |
| | EnterpriseAP | 00:30:DA:36:33:51 | 3 |
| | IDy_D | E4:F4:C6:03:5F:29 | 5 |
| | ACStest | 80:1F:02:F1:96:EC | 5 |
| | don | 02:1F:02:F1:96:EC | 5 |
| | Xperia | 68:76:4F:66:AD:53 | 1 |
| | gggggg | 00:1A:2B:53:50:17 | 8 |
| | IDy_C | FC:75:16:8C:F5:EC | 7 |
| | 3845 | F8:8E:85:F5:9A:89 | 11 |
| | YL-N | C8:D3:A3:2C:4B:8A | 1 |
| | | 38:72:C0:FE:AA:67 | 1 |
| | PMC | F8:8E:85:82:18:D9 | 11 |

# Chapter 5 Basic Setup

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

Basic Setup

This will bring you to the following screen.



LAN

| | |
|---|---|
| LAN IPv4 Address | 192.168.1.1 |
| LAN Subnet Mask | 255.255.255.0 |
| LAN MAC Address | f8:8e:85:73:88:92 |
| DHCP Server | Enabled |
| LAN IPv6 ULA Address | |

WAN

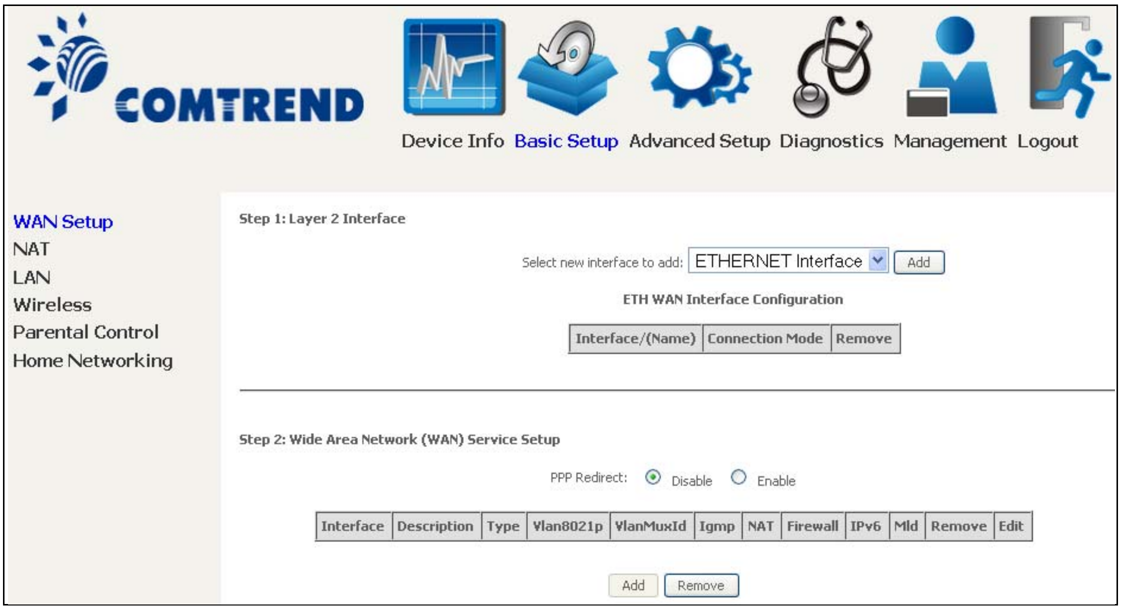
| | |
|---|---|
| Speed (down/up) | kbps / kbps |
| Default Gateway | |
| Primary DNS Server | 0.0.0.0 |
| Secondary DNS Server | 0.0.0.0 |
| Default IPv6 Gateway | |

Wireless

| | |
|---|---|
| Driver Version | 6.30.102.7.cpe4.12L06B.1 |
| Primary SSID | Comtrend8892 |
| Status | Enabled |
| Channel | 1 |
| | Secure |
| Primary Encryption | WPA2-PSK TKIP+AES |
| Primary Passphrase/Key | ●●●●●●●●●●<br>Show |

## 5.1 Wan Setup

Add or remove ETH WAN interface connections here.



Step 1: Layer 2 Interface

Select new interface to add: ETHERNET Interface [Add]

ETH WAN Interface Configuration

| Interface/(Name) | Connection Mode | Remove |
|---|---|---|

Step 2: Wide Area Network (WAN) Service Setup

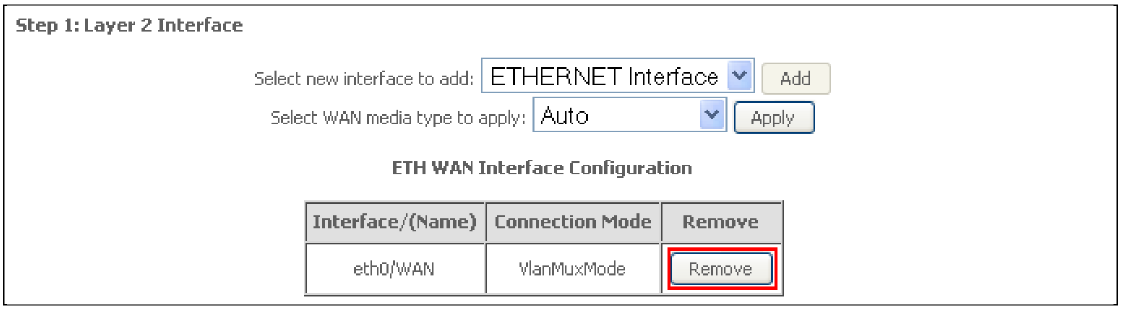
PPP Redirect: ● Disable ○ Enable

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

[Add] [Remove]

Click **Add** to create a new Layer 2 Interface (see Appendix E - Connection Setup).

To remove a connection, click the **Remove** button.



Step 1: Layer 2 Interface

Select new interface to add: ETHERNET Interface [Add]

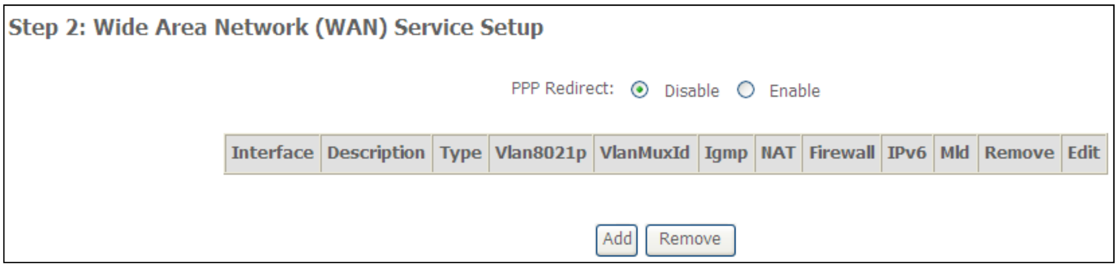
Select WAN media type to apply: Auto [Apply]

ETH WAN Interface Configuration

| Interface/(Name) | Connection Mode | Remove |
|---|---|---|
| eth0/WAN | VlanMuxMode | [Remove] |

### 5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.



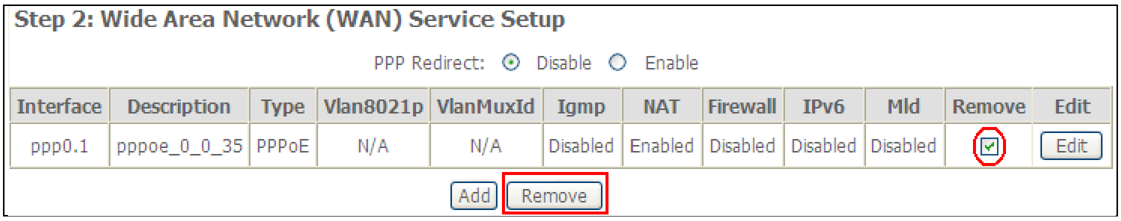
Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect: ● Disable ○ Enable

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

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

To remove a connection, select its remove checkbox and click **Remove**.



Step 2: Wide Area Network (WAN) Service Setup

PPP Redirect: ● Disable ○ Enable

| Interface | Description | Type | Vlan8021p | VlanMuxId | Igmp | NAT | Firewall | IPv6 | Mld | Remove | Edit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ppp0.1 | pppoe_0_0_35 | PPPoE | N/A | N/A | Disabled | Enabled | Disabled | Disabled | Disabled | ☑ | Edit |

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

To remove a connection, select its remove checkbox and click **Remove**.

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

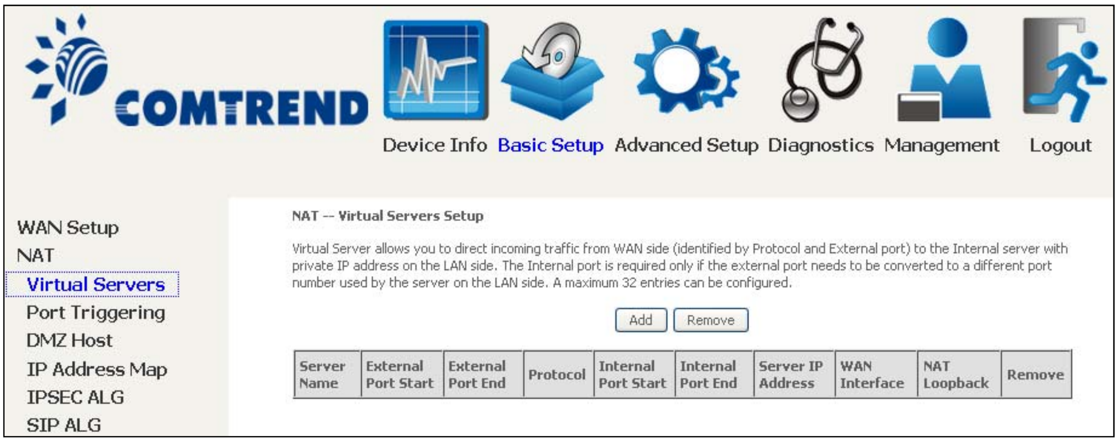
| | |
|---|---|
| **NOTE:** | Up to 16 PVC profiles can be configured and saved in flash memory. Also, ETH and PTM/ATM service connections cannot coexist. |

## 5.2 NAT

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

### 5.2.1 Virtual Servers

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

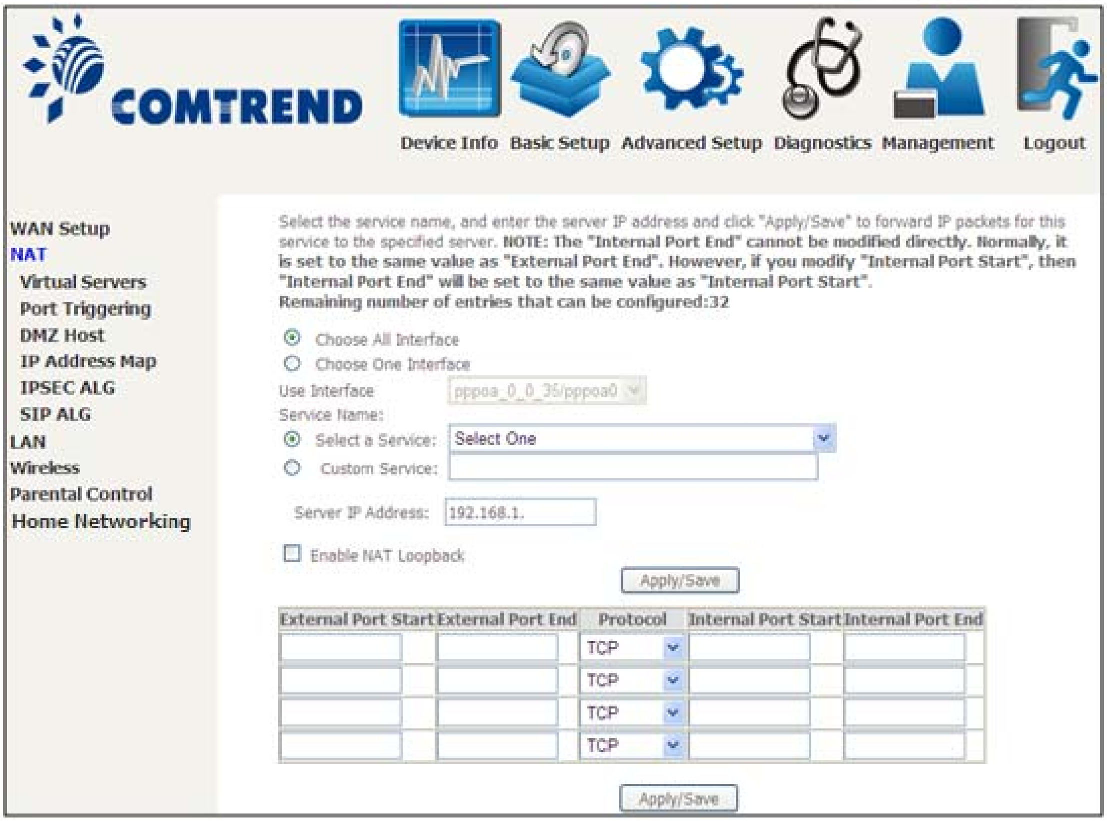


NAT -- Virtual Servers Setup

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

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

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



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

**Remaining number of entries that can be configured:32**

● Choose All Interface
○ Choose One Interface

Use Interface: pppoa_0_0_35/pppoa0

Service Name:
● Select a Service: Select One
○ Custom Service:

Server IP Address: 192.168.1.

□ Enable NAT Loopback

Apply/Save

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

Apply/Save

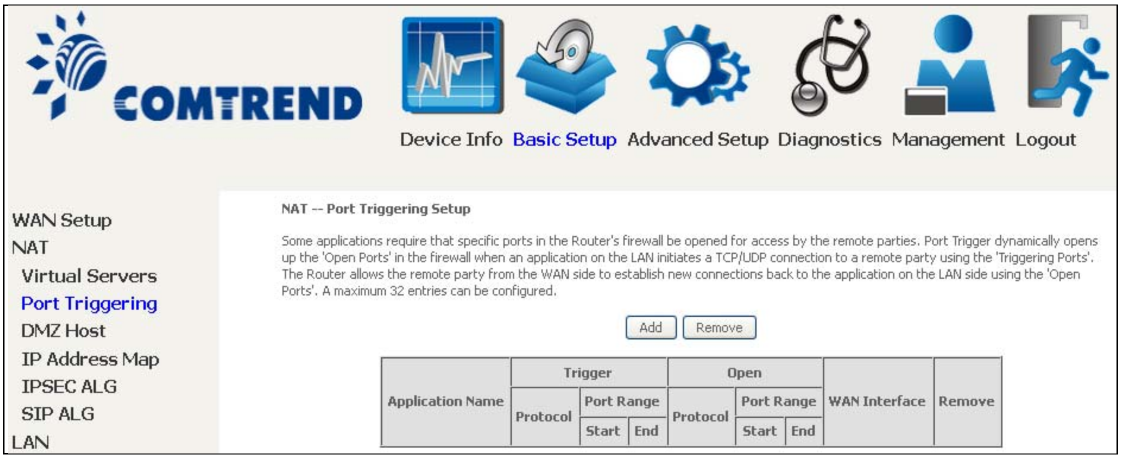
Consult the table below for field and header descriptions.

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

| Field / Header | Description |
|---|---|
| Internal Port End | Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured. |

## 5.2.2 Port Triggering

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

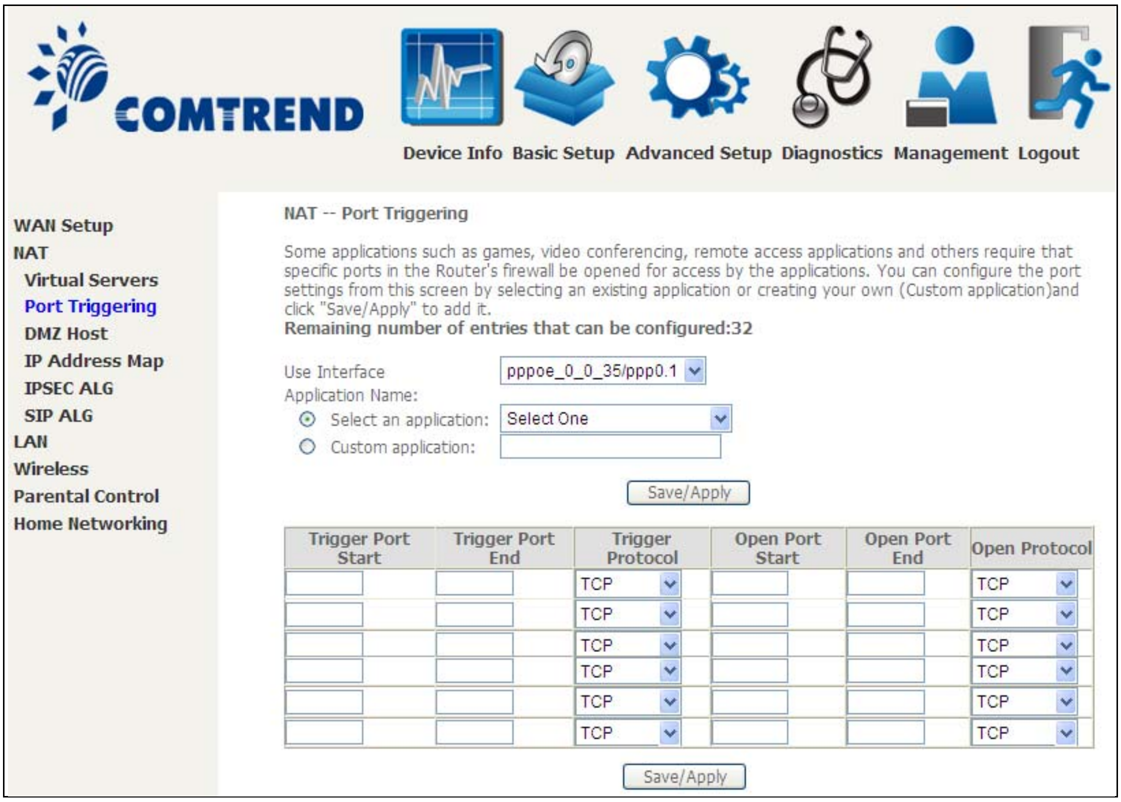


NAT -- Port Triggering Setup

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

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

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



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.

**Remaining number of entries that can be configured:32**

Use Interface: pppoe_0_0_35/ppp0.1

Application Name:

● Select an application: Select One

○ Custom application:

Save/Apply

| Trigger Port Start | Trigger Port End | Trigger Protocol | Open Port Start | Open Port End | Open Protocol |
|---|---|---|---|---|---|
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |
| | | TCP | | | TCP |

Save/Apply

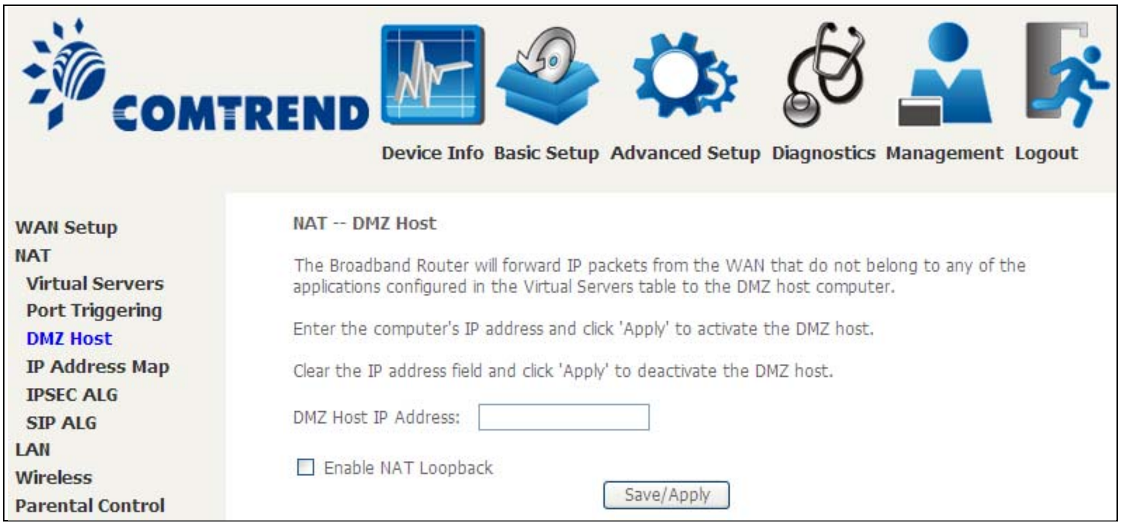
Click Save/Apply to save and apply the settings.

Consult the table below for field and header descriptions.

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

### 5.2.3 DMZ Host

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



NAT -- DMZ Host

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

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

□ Enable NAT Loopback

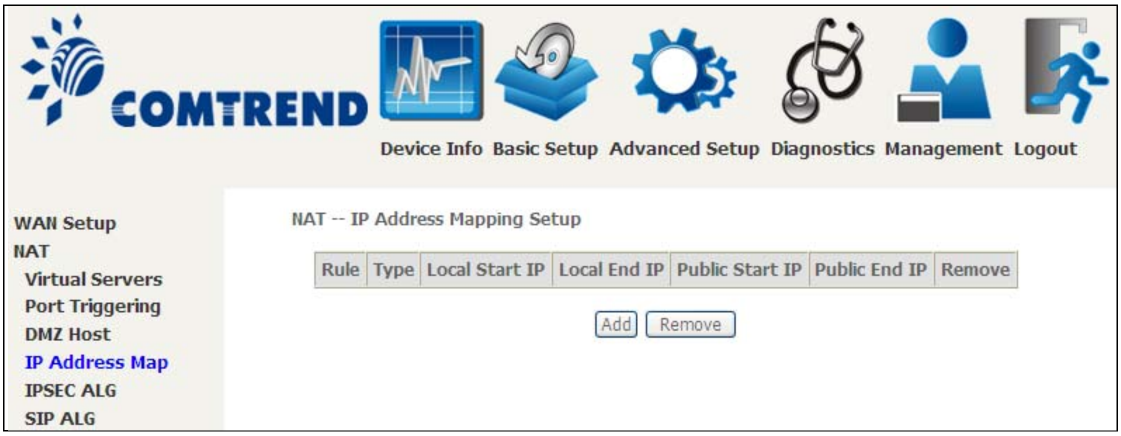
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

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

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

### 5.2.4 IP Address Map

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

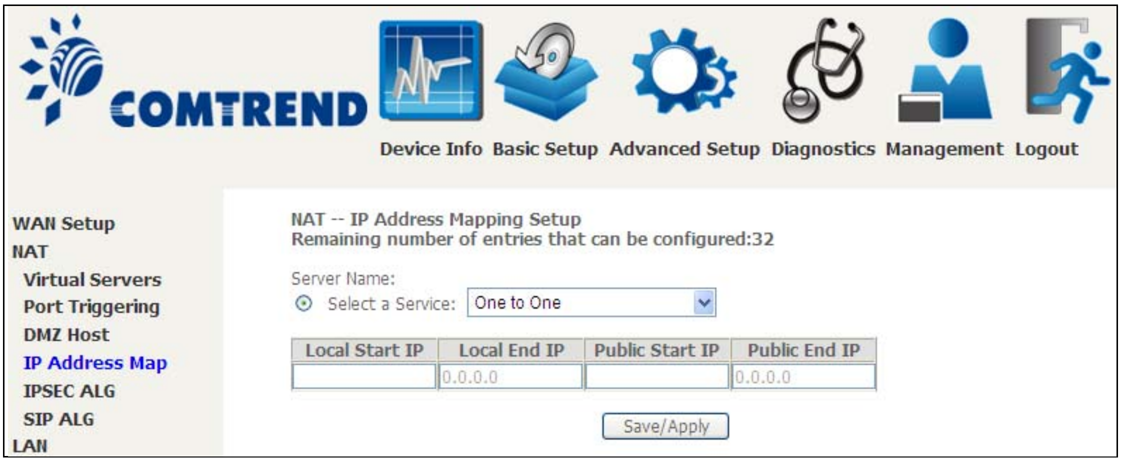


NAT -- IP Address Mapping Setup

| Rule | Type | Local Start IP | Local End IP | Public Start IP | Public End IP | Remove |
|---|---|---|---|---|---|---|

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

Click the Add button to display the following.



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

Server Name:
● Select a Service: One to One

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

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

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

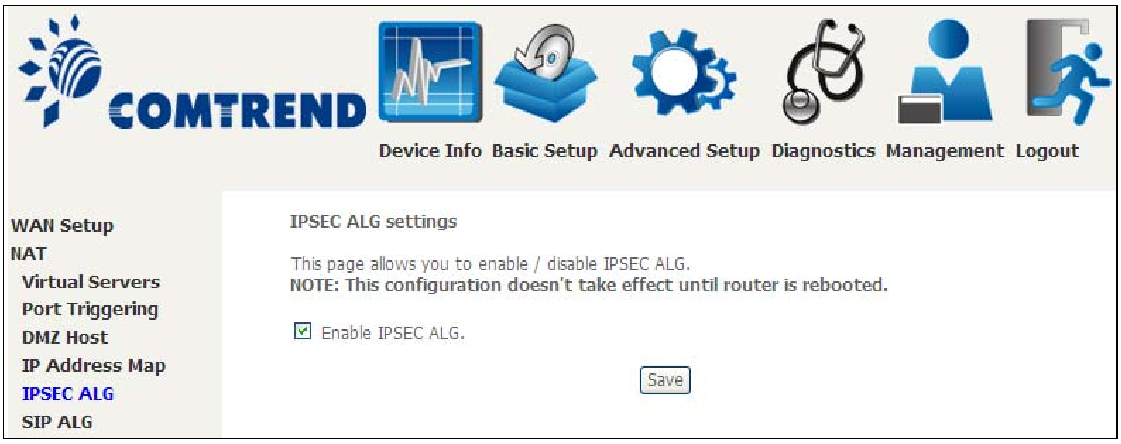
**Many to one:** mapping a range of local IP to a specific public IP

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

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

### 5.2.5 IPSEC ALG

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



IPSEC ALG settings

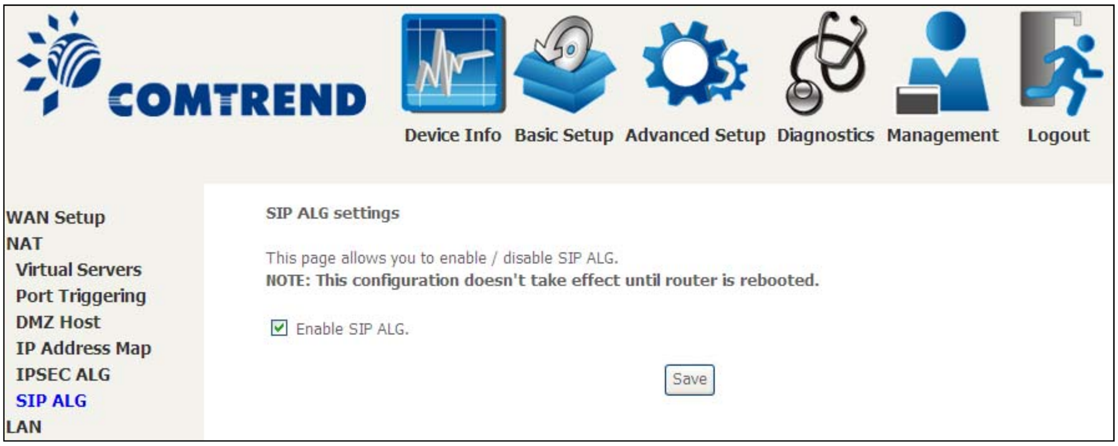
This page allows you to enable / disable IPSEC ALG.
NOTE: This configuration doesn't take effect until router is rebooted.

☑ Enable IPSEC ALG.

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

### 5.2.6 SIP ALG

This page allows you to enable / disable SIP ALG.



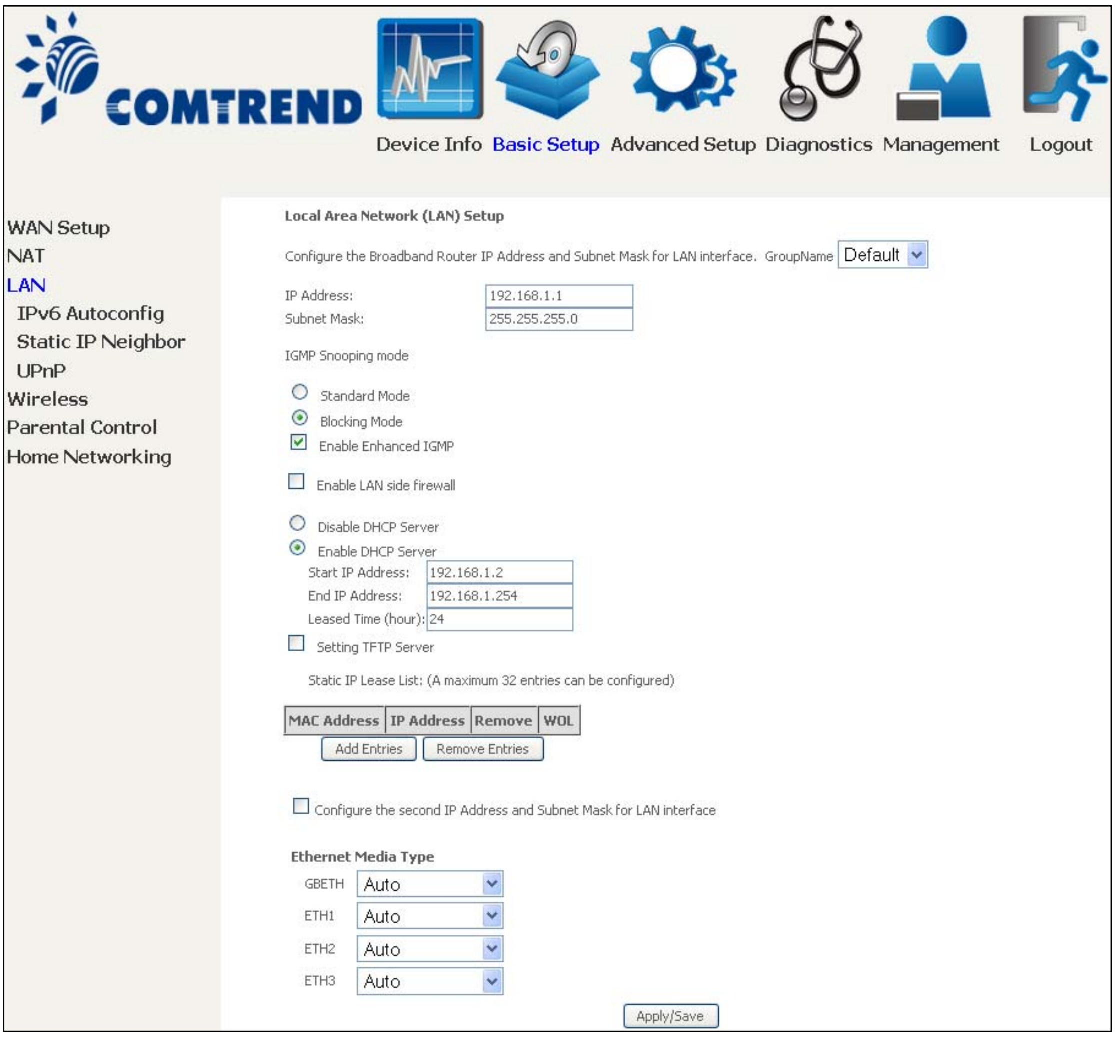
SIP ALG settings

This page allows you to enable / disable SIP ALG.
NOTE: This configuration doesn't take effect until router is rebooted.

☑ Enable SIP ALG.

## 5.3 LAN

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



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

IGMP Snooping mode

○ Standard Mode
● Blocking Mode
☑ Enable Enhanced IGMP

□ Enable LAN side firewall

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24
□ Setting TFTP Server

Static IP Lease List: (A maximum 32 entries can be configured)

| MAC Address | IP Address | Remove | WOL |
|---|---|---|---|

Add Entries    Remove Entries

□ Configure the second IP Address and Subnet Mask for LAN interface

Ethernet Media Type

| | |
|---|---|
| GBETH | Auto |
| ETH1 | Auto |
| ETH2 | Auto |
| ETH3 | Auto |

Apply/Save

Consult the field descriptions below for more details.

**GroupName:** Select an Interface Group.

### 1st LAN INTERFACE

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

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

**IGMP Snooping:**

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

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

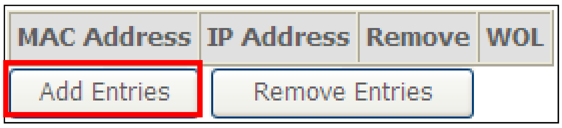
**Enable Enhanced IGMP:** Enable by ticking the checkbox ☑. IGMP packets between LAN ports will be blocked.

**Enable LAN side firewall:** Enable by ticking the checkbox ☑.

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

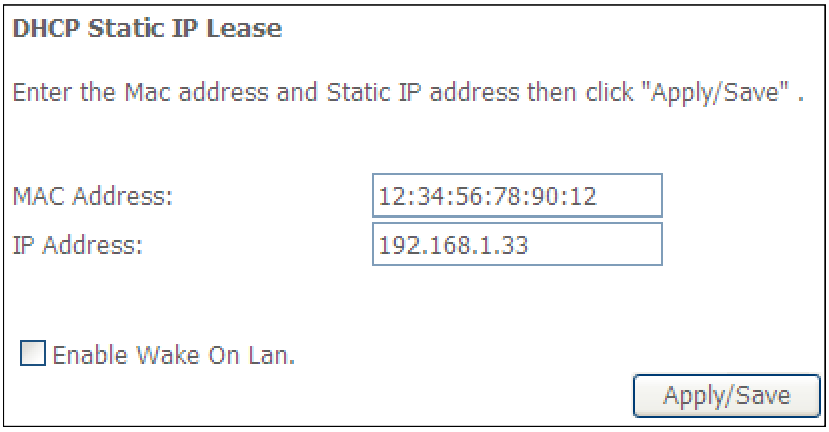
**Setting TFTP Server:** Enable by ticking the checkbox ☑. Then, input the TFTP server address or an IP address.

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



| MAC Address | IP Address | Remove | WOL |
|---|---|---|---|

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



DHCP Static IP Lease

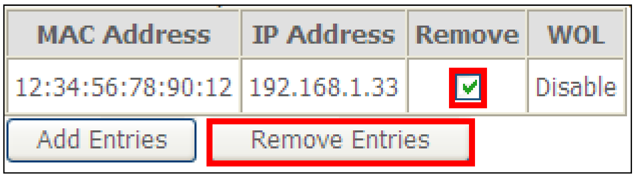
Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address: 12:34:56:78:90:12

IP Address: 192.168.1.33

□ Enable Wake On Lan.

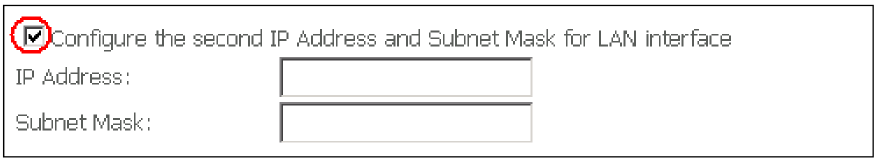
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



| MAC Address | IP Address | Remove | WOL |
|---|---|---|---|
| 12:34:56:78:90:12 | 192.168.1.33 | ☑ | Disable |

## 2ND LAN INTERFACE

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



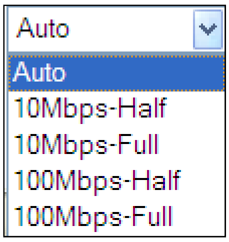
☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

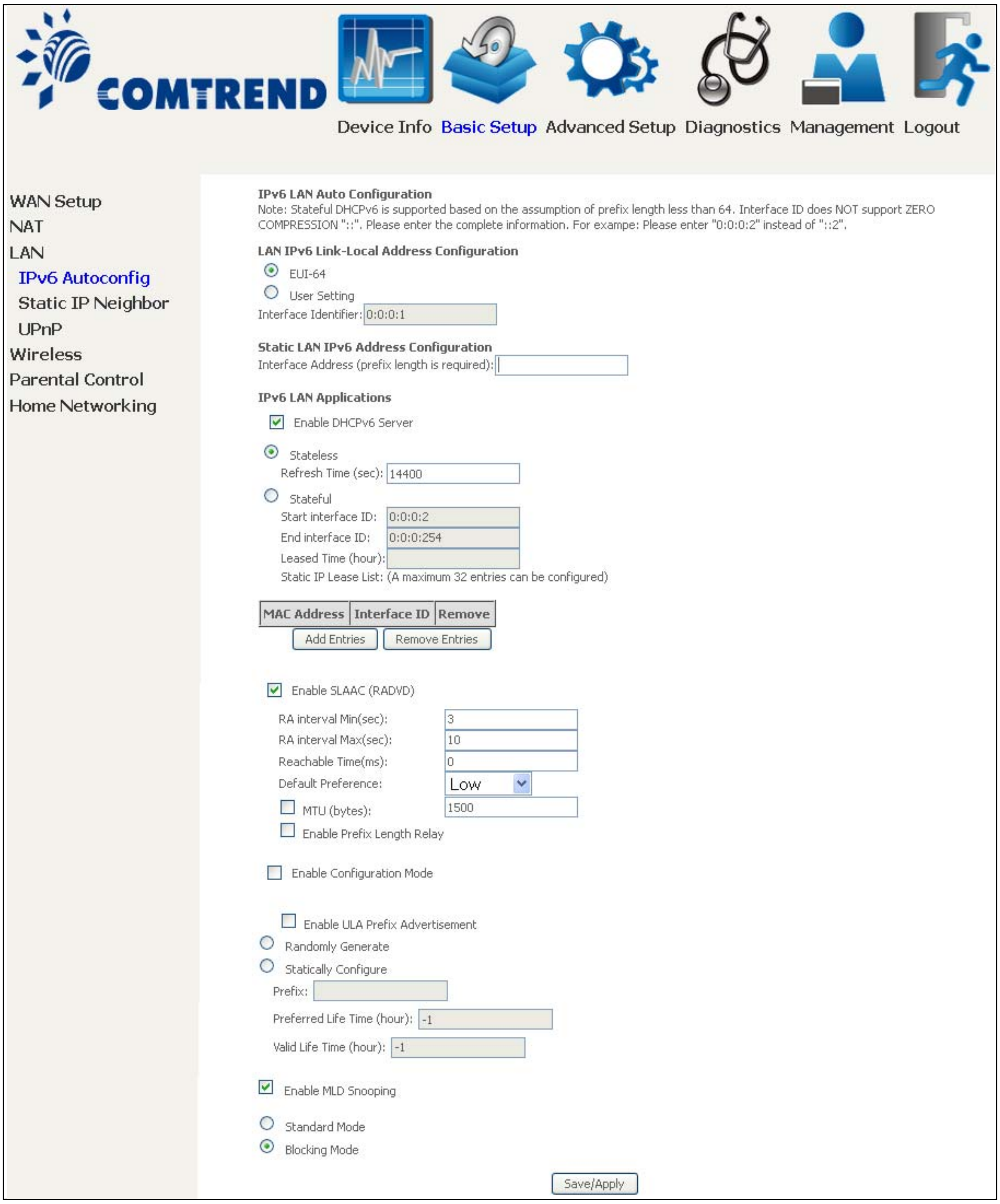
IP Address: Enter the secondary IP address for the LAN port.
Subnet Mask: Enter the secondary subnet mask for the LAN port.
Ethernet Media Type:

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



### 5.3.1 LAN IPv6 Autoconfig

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



**IPv6 LAN Auto Configuration**

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

**LAN IPv6 Link-Local Address Configuration**

● EUI-64
○ User Setting
Interface Identifier: 0:0:0:1

**Static LAN IPv6 Address Configuration**

Interface Address (prefix length is required):

**IPv6 LAN Applications**

☑ Enable DHCPv6 Server

● Stateless
Refresh Time (sec): 14400

○ Stateful
Start interface ID: 0:0:0:2
End interface ID: 0:0:0:254
Leased Time (hour):
Static IP Lease List: (A maximum 32 entries can be configured)

| MAC Address | Interface ID | Remove |
|---|---|---|

☑ Enable SLAAC (RADVD)

RA interval Min(sec): 3
RA interval Max(sec): 10
Reachable Time(ms): 0
Default Preference: Low
□ MTU (bytes): 1500
□ Enable Prefix Length Relay

□ Enable Configuration Mode

□ Enable ULA Prefix Advertisement
○ Randomly Generate
○ Statically Configure
Prefix:
Preferred Life Time (hour): -1
Valid Life Time (hour): -1

☑ Enable MLD Snooping

○ Standard Mode
● Blocking Mode

Consult the field descriptions below for more details.

#### LAN IPv6 Link-Local Address Configuration

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

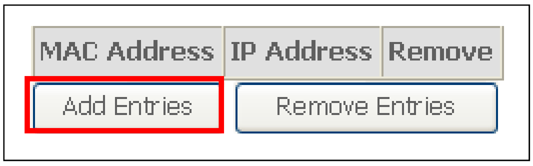
**Static LAN IPv6 Address Configuration**

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

**IPv6 LAN Applications**

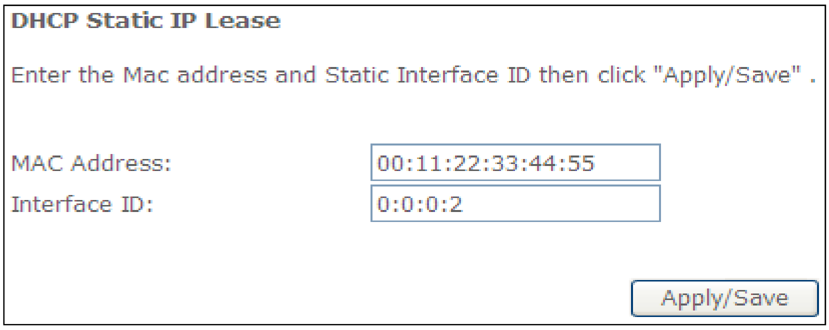
| Heading | Description |
|---|---|
| **Stateless** | Use stateless configuration |
| Refresh Time (sec): | The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6 |
| **Stateful** | Use stateful configuration |
| Start interface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

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



| MAC Address | IP Address | Remove |
|---|---|---|

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



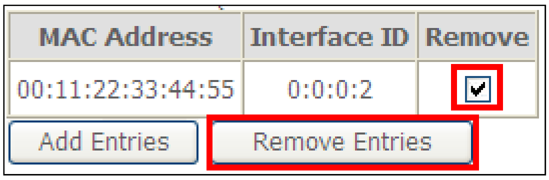
DHCP Static IP Lease

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

MAC Address: 00:11:22:33:44:55

Interface ID: 0:0:0:2

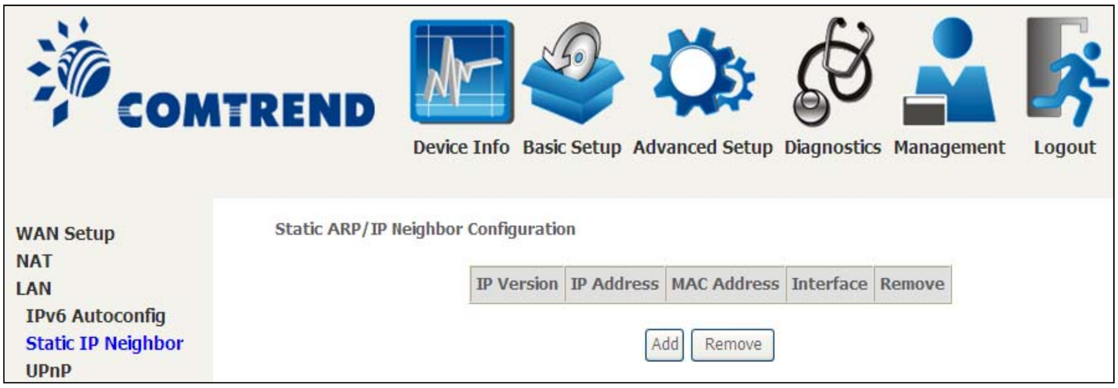
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



| MAC Address | Interface ID | Remove |
|---|---|---|
| 00:11:22:33:44:55 | 0:0:0:2 | ☑ |

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

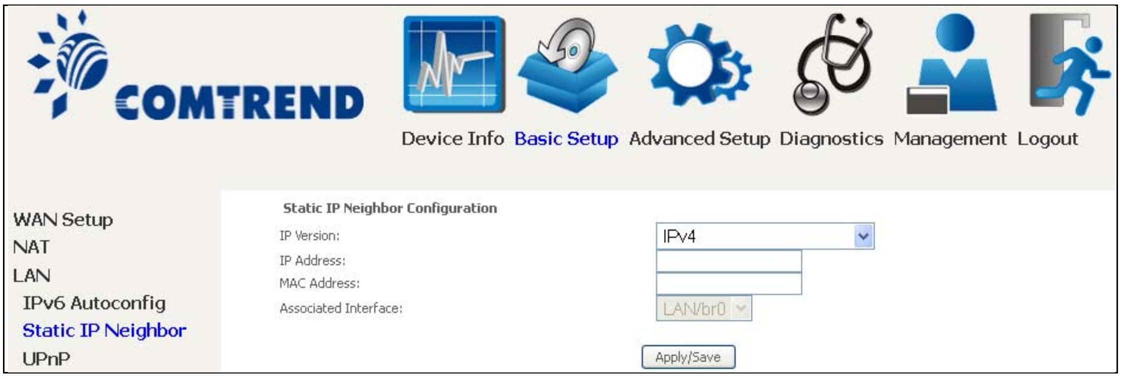
## 5.3.2 Static IP Neighbor



Static ARP/IP Neighbor Configuration

| IP Version | IP Address | MAC Address | Interface | Remove |
|---|---|---|---|---|

Click the Add button to display the following.



Static IP Neighbor Configuration

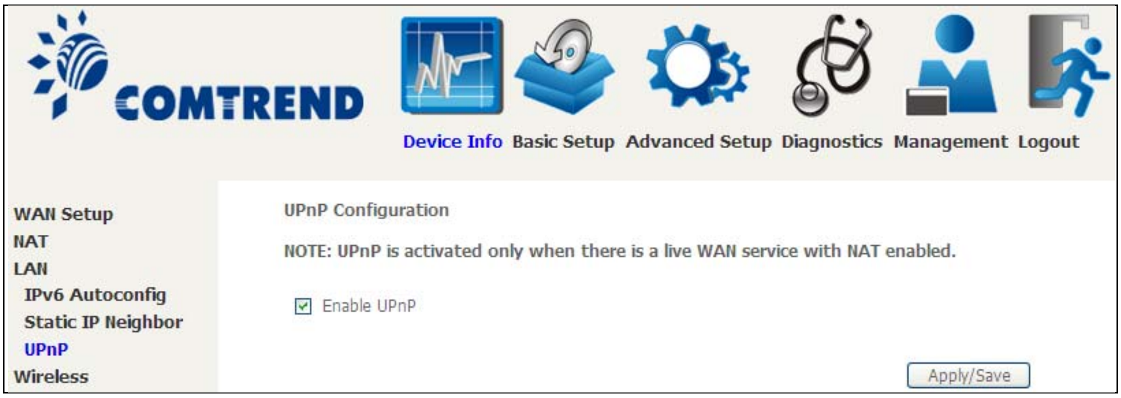
IP Version: IPv4
IP Address:
MAC Address:
Associated Interface: LAN/br0

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

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

### 5.3.3 UPnP

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



UPnP Configuration

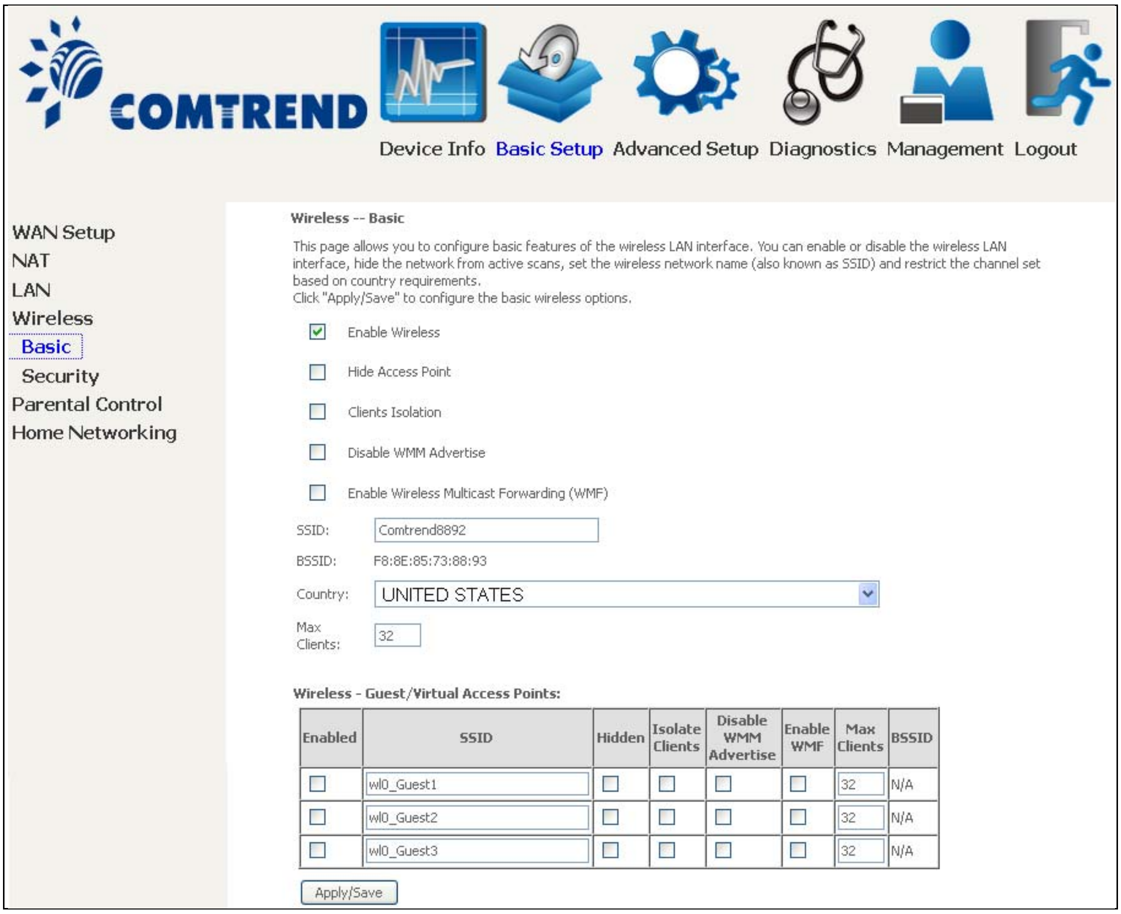
NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☑ Enable UPnP

# 5.4 Wireless

## 5.4.1 Basic

The Basic option allows youto configure basic features of the wirelessLAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



**Wireless -- Basic**

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply/Save" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID: Comtrend8892

BSSID: F8:8E:85:73:88:93

Country: UNITED STATES

Max Clients: 32

**Wireless - Guest/Virtual Access Points:**

| Enabled | SSID | Hidden | Isolate Clients | Disable WMM Advertise | Enable WMF | Max Clients | BSSID |
|---|---|---|---|---|---|---|---|
| □ | wl0_Guest1 | □ | □ | □ | □ | 32 | N/A |
| □ | wl0_Guest2 | □ | □ | □ | □ | 32 | N/A |
| □ | wl0_Guest3 | □ | □ | □ | □ | 32 | N/A |

Apply/Save

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

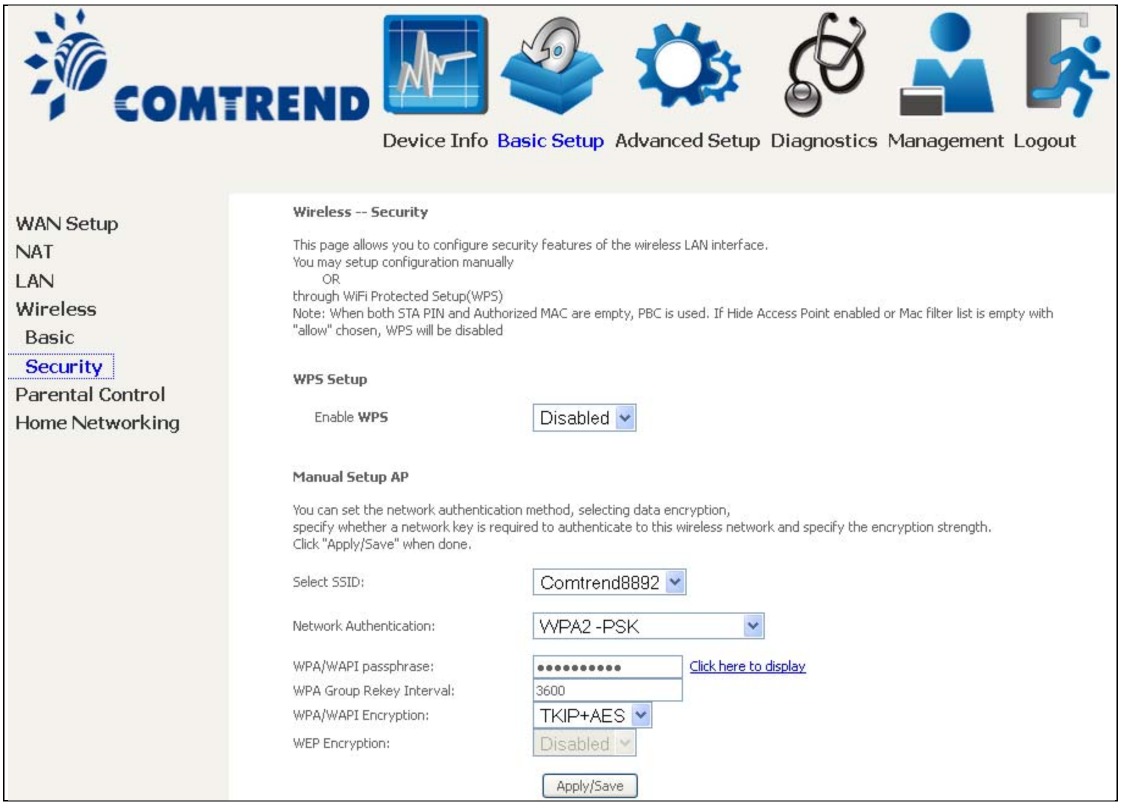
Consult the table below for descriptions of these options.

| Option | Description |
|---|---|
| Enable Wireless | A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear. |

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

### 5.4.2 Security

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



Wireless -- Security

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

WPS Setup

Enable WPS: Disabled

Manual Setup AP

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

Select SSID: Comtrend8892

Network Authentication: WPA2 -PSK

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

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

Please see 6.10.3 WPS for WPS setup instructions.

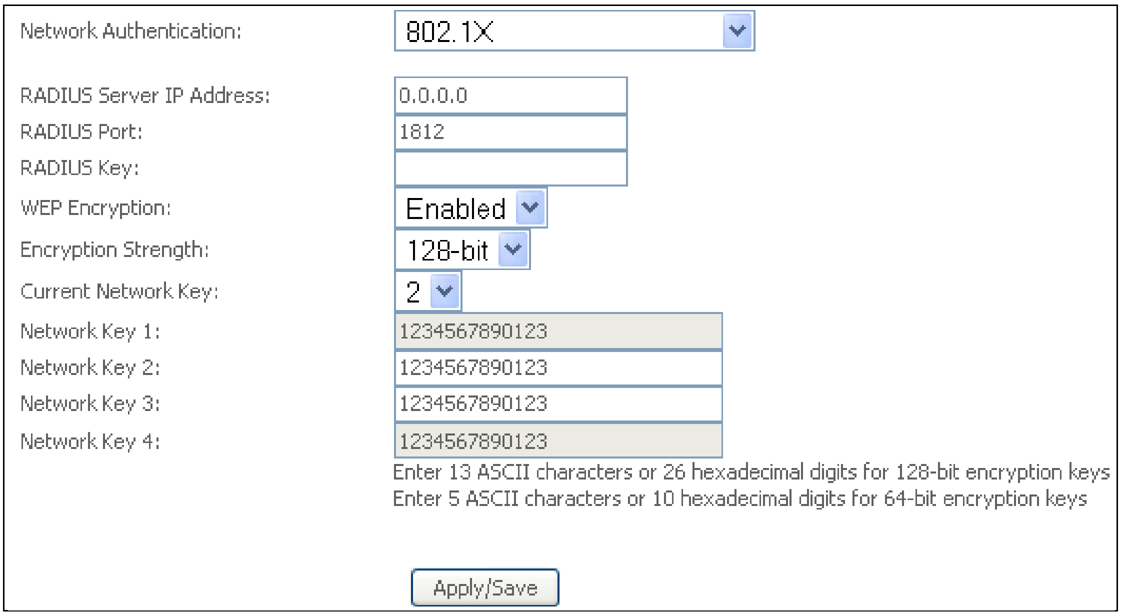
Click **Apply/Save** to implement new configuration settings.

### WIRELESS SECURITY

Setup requires that the user configure these settings using the Web User Interface (see the table below).

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

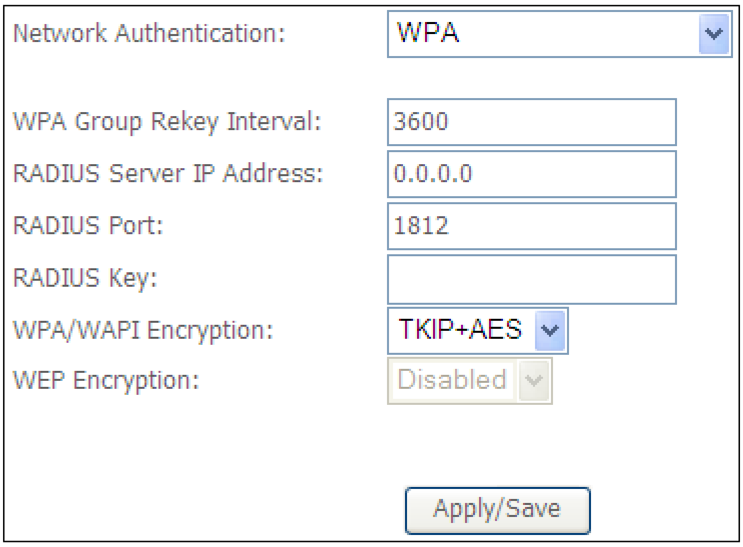
| **Network Authentication** |
|---|
| This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.<br><br>Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below. |



|  |  |
|---|---|
| Network Authentication: | 802.1X |
| RADIUS Server IP Address: | 0.0.0.0 |
| RADIUS Port: | 1812 |
| RADIUS Key: |  |
| WEP Encryption: | Enabled |
| Encryption Strength: | 128-bit |
| Current Network Key: | 2 |
| Network Key 1: | 1234567890123 |
| Network Key 2: | 1234567890123 |
| Network Key 3: | 1234567890123 |
| Network Key 4: | 1234567890123 |

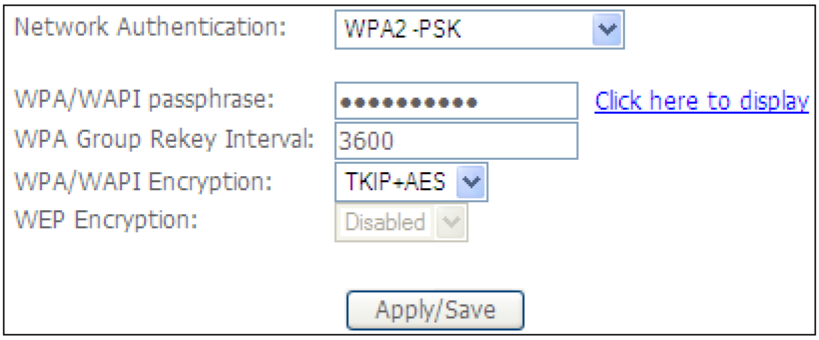
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

The settings for WPA authentication are shown below.



|  |  |
|---|---|
| Network Authentication: | WPA |
| WPA Group Rekey Interval: | 3600 |
| RADIUS Server IP Address: | 0.0.0.0 |
| RADIUS Port: | 1812 |
| RADIUS Key: |  |
| WPA/WAPI Encryption: | TKIP+AES |
| WEP Encryption: | Disabled |

The settings for WPA2-PSK authentication are shown next.



|  |  |  |
|---|---|---|
| Network Authentication: | WPA2 -PSK |  |
| WPA/WAPI passphrase: | ●●●●●●●●●●● | Click here to display |
| WPA Group Rekey Interval: | 3600 |  |
| WPA/WAPI Encryption: | TKIP+AES |  |
| WEP Encryption: | Disabled |  |

| **WEP Encryption** |
|---|
| This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.<br><br>Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.<br>When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.<br><br>Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel. |
| **Encryption Strength** |
| This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of securty and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data. |

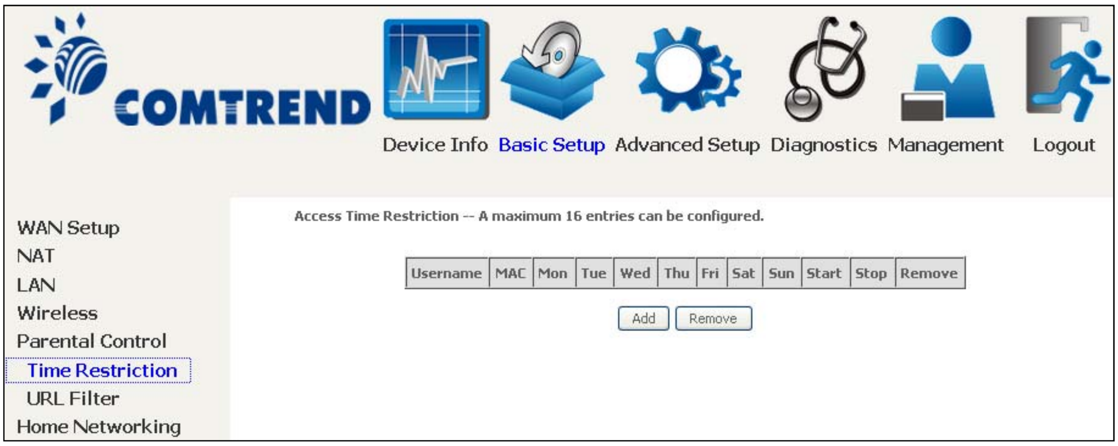
Please see 6.10 for MAC Filter, Wireless Bridge and Advanced Wireless features.

## 5.5 Parental Control

This selection provides WAN access control functionality.

### 5.5.1 Time Restriction

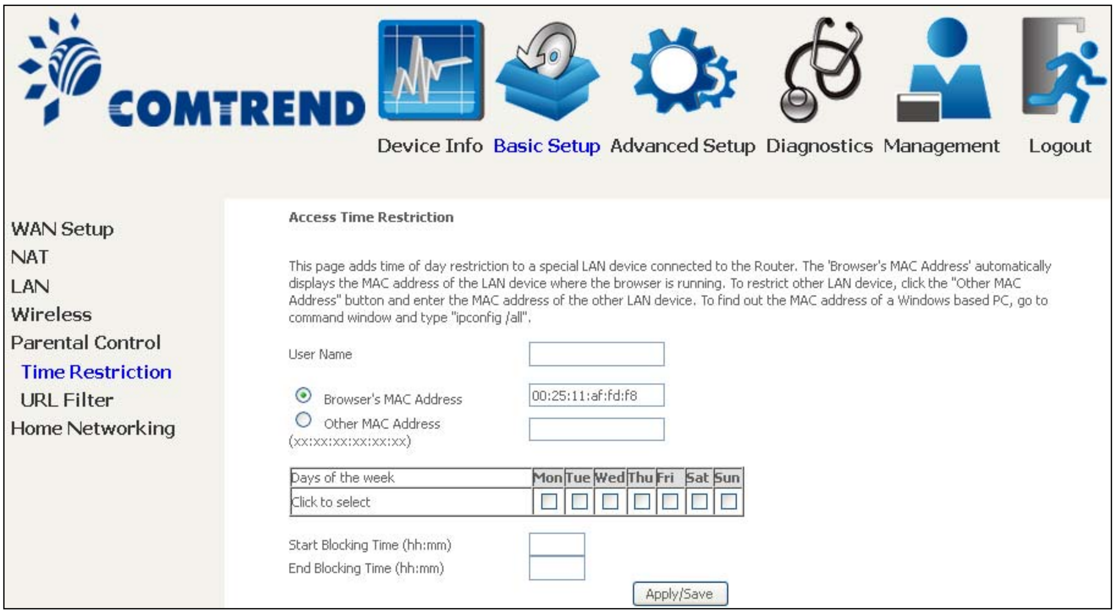
This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.5 Internet Time, so that the scheduled times match your local time.



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

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

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



Access Time Restriction

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

User Name

● Browser's MAC Address 00:25:11:af:fd:f8

○ Other MAC Address
(xx:xx:xx:xx:xx:xx)

| Days of the week | Mon | Tue | Wed | Thu | Fri | Sat | Sun |
|---|---|---|---|---|---|---|---|
| Click to select | □ | □ | □ | □ | □ | □ | □ |

Start Blocking Time (hh:mm)

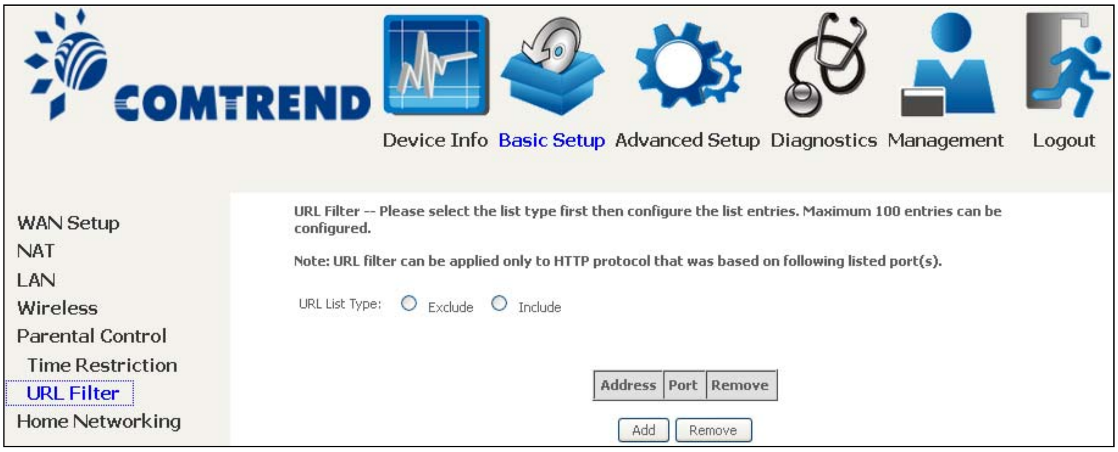
End Blocking Time (hh:mm)

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

**User Name:** A user-defined label for this restriction.
**Browser's MAC Address:** MAC address of the PC running the browser.
**Other MAC Address:** MAC address of another LAN device.
**Days of the Week:** The days the restrictions apply.
**Start Blocking Time:** The time the restrictions start.
**End Blocking Time:** The time the restrictions end.

## 5.5.2 URL Filter

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



URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

Note: URL filter can be applied only to HTTP protocol that was based on following listed port(s).

URL List Type: ○ Exclude ○ Include

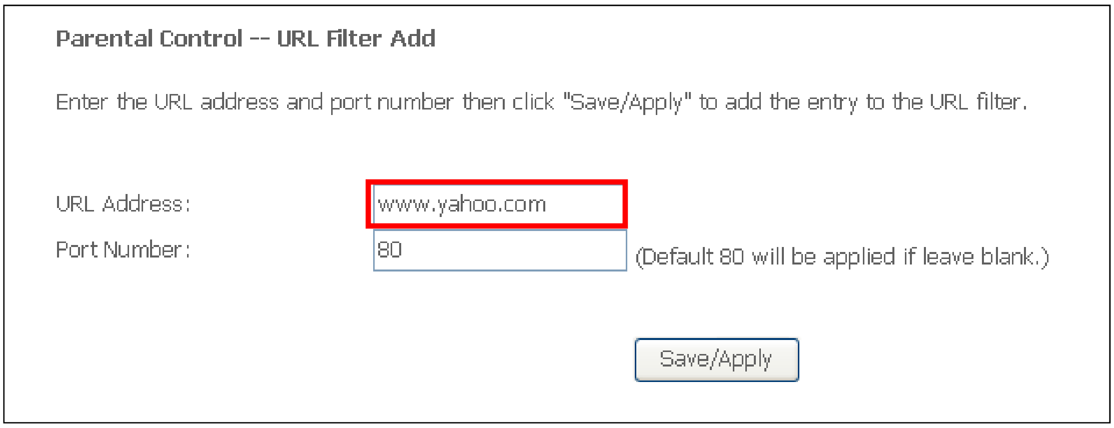
| Address | Port | Remove |
|---|---|---|

Select URL List Type: Exclude or Include.

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

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

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



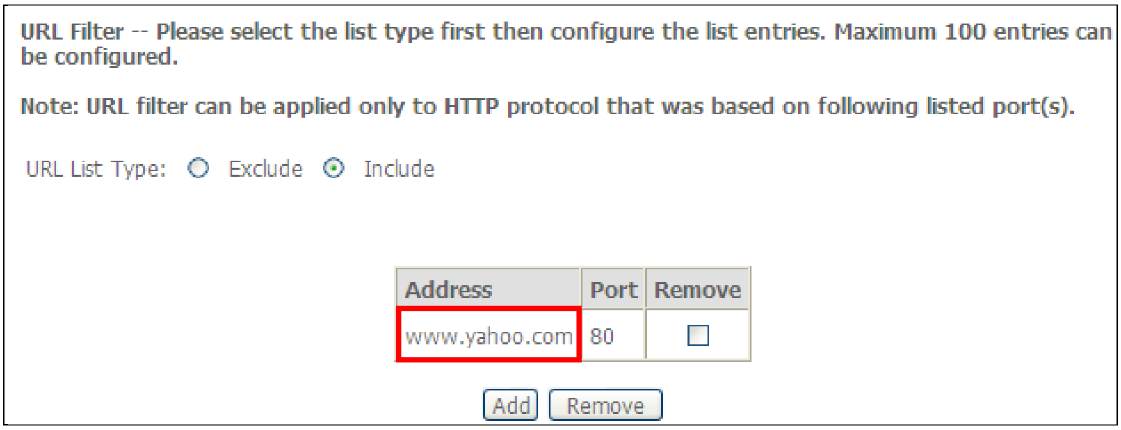
Parental Control -- URL Filter Add

Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.

URL Address: www.yahoo.com

Port Number: 80 (Default 80 will be applied if leave blank.)

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



URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

Note: URL filter can be applied only to HTTP protocol that was based on following listed port(s).

URL List Type: ○ Exclude ● Include

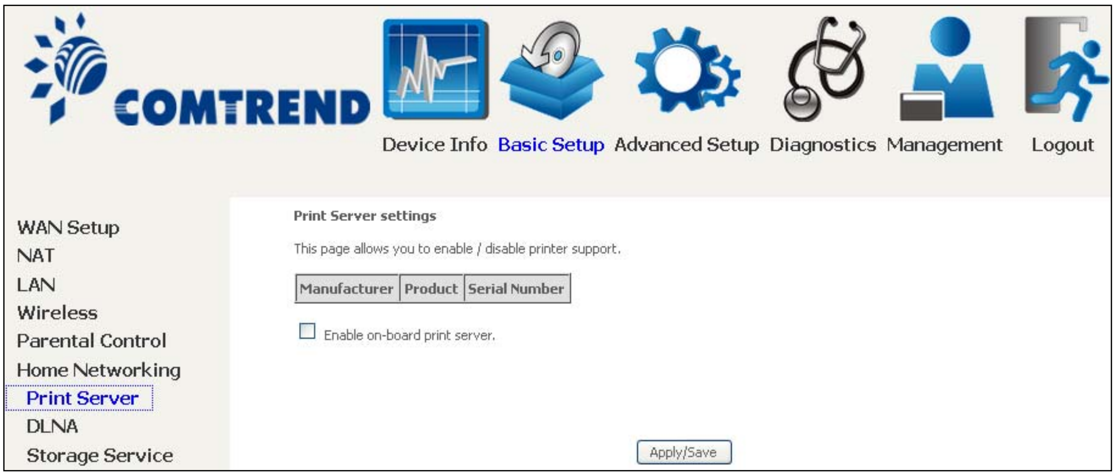
| Address | Port | Remove |
|---|---|---|
| www.yahoo.com | 80 | □ |

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

# 5.6 Home networking

## 5.6.1 Print Server

This page allows you to enable or disable printer support.



Print Server settings

This page allows you to enable / disable printer support.

| Manufacturer | Product | Serial Number |
|---|---|---|

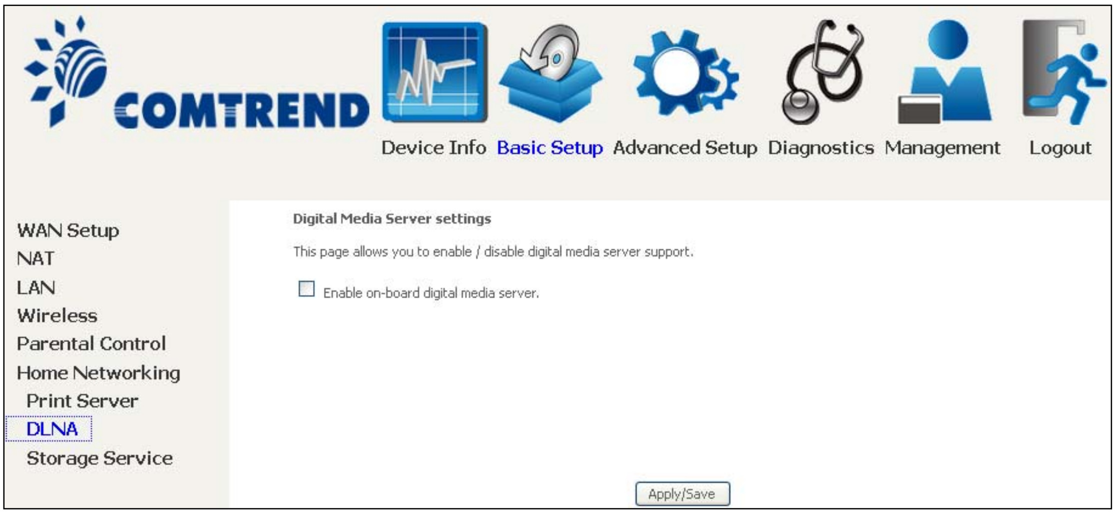
□ Enable on-board print server.

Please reference **Appendix G** to see the procedure for enabling the Printer Server.

## 5.6.2 DLNA

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

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



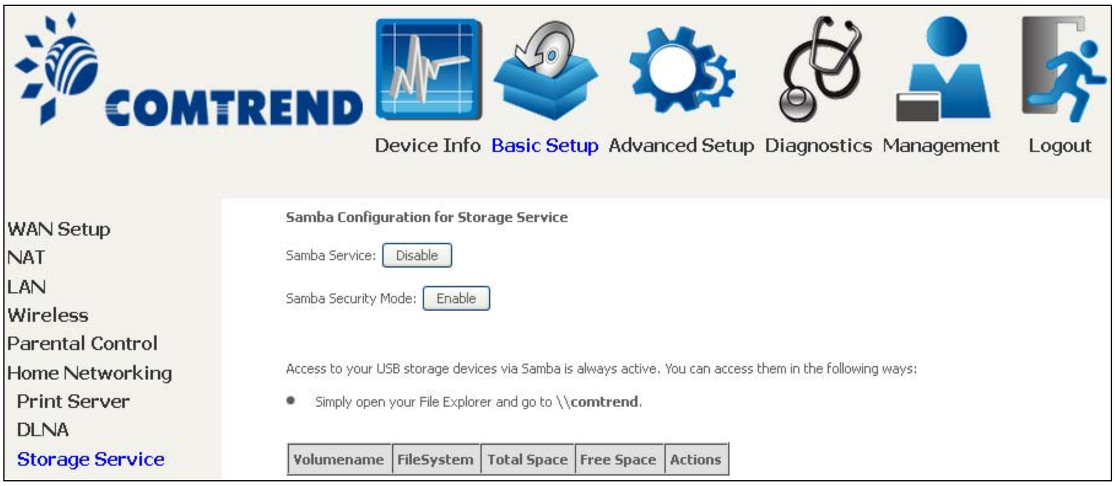
Digital Media Server settings

This page allows you to enable / disable digital media server support.

□ Enable on-board digital media server.

### 5.6.3 Storage Service

Enabling Samba service allows the user to share files on the storage device. Different levels of user access can be configured after samba security mode is enabled. This page also displays storage devices attached to USB host.



Samba Configuration for Storage Service

Samba Service: Disable

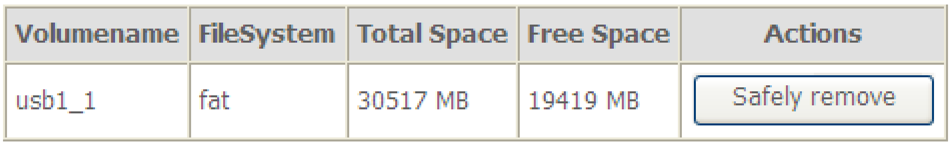
Samba Security Mode: Enable

Access to your USB storage devices via Samba is always active. You can access them in the following ways:

- Simply open your File Explorer and go to \\comtrend.

| Volumename | FileSystem | Total Space | Free Space | Actions |
|---|---|---|---|---|

Display after storage device attached (for your reference).



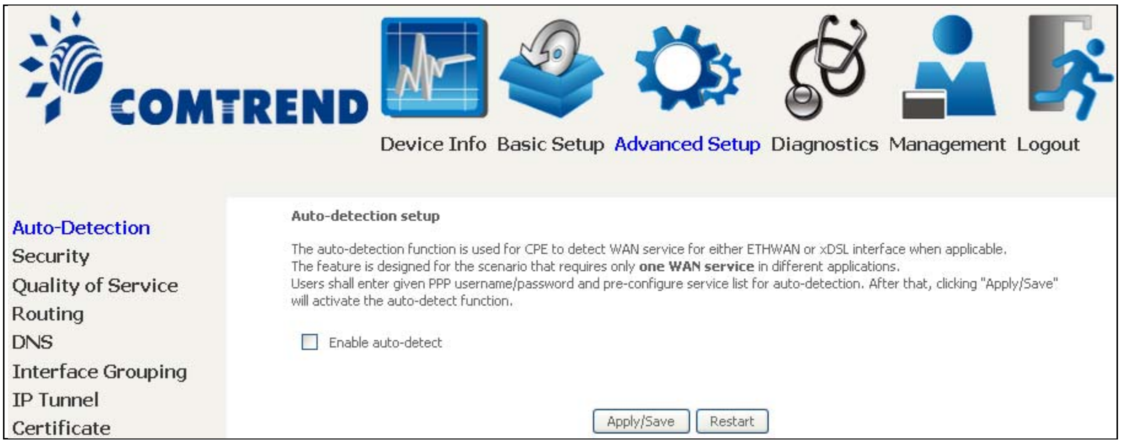
| Volumename | FileSystem | Total Space | Free Space | Actions |
|---|---|---|---|---|
| usb1_1 | fat | 30517 MB | 19419 MB | Safely remove |

# Chapter 6 Advanced Setup

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

## 6.1 Auto-detection setup

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

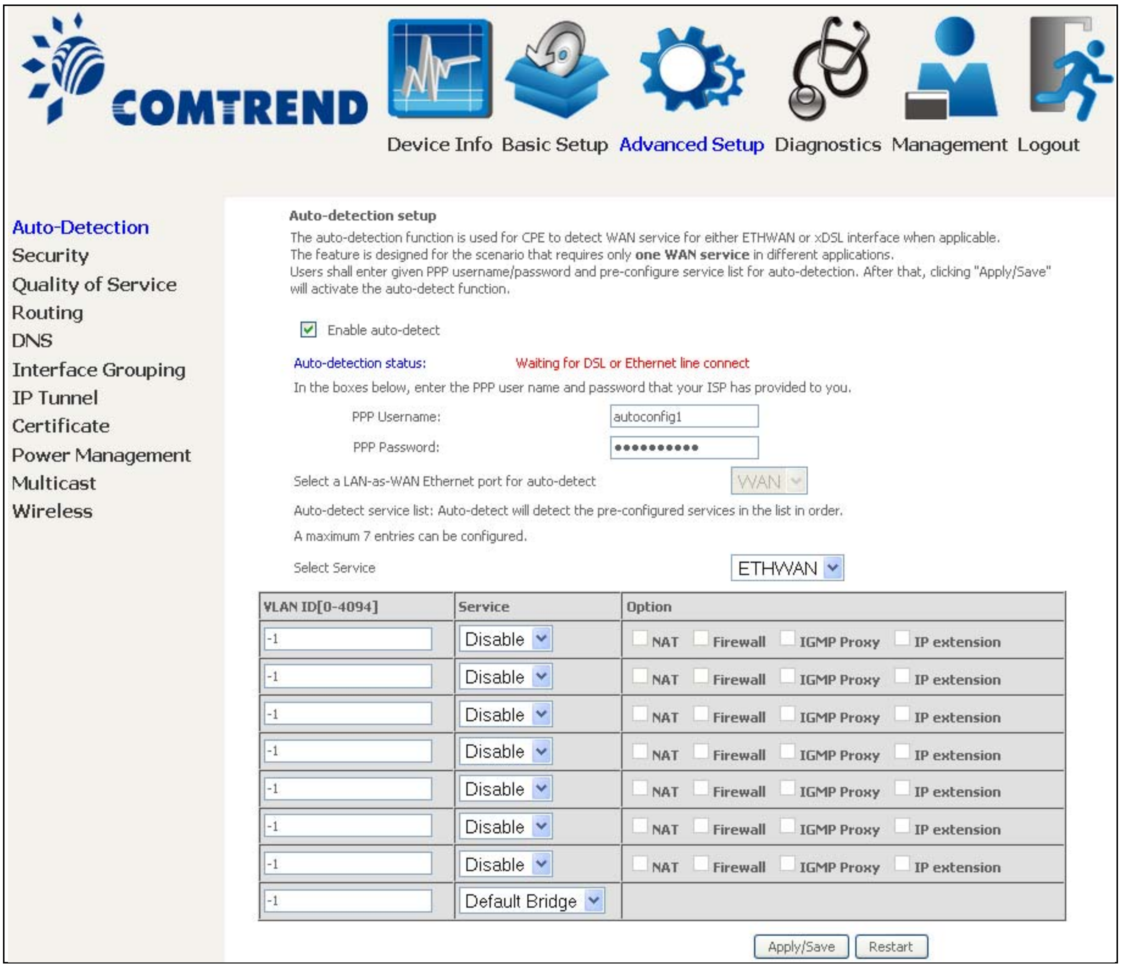


**Auto-detection setup**

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

□ Enable auto-detect

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



**Auto-detection setup**

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

☑ Enable auto-detect

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

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

| | |
|---|---|
| PPP Username: | autoconfig1 |
| PPP Password: | ●●●●●●●●●● |

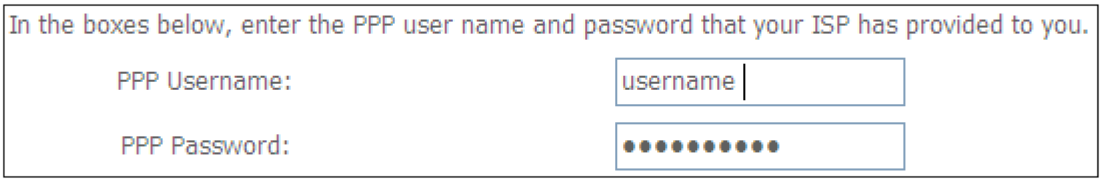
Select a LAN-as-WAN Ethernet port for auto-detect: WAN

Auto-detect service list: Auto-detect will detect the pre-configured services in the list in order.

A maximum 7 entries can be configured.

Select Service: ETHWAN

| VLAN ID[0-4094] | Service | Option |
|---|---|---|
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Default Bridge | |

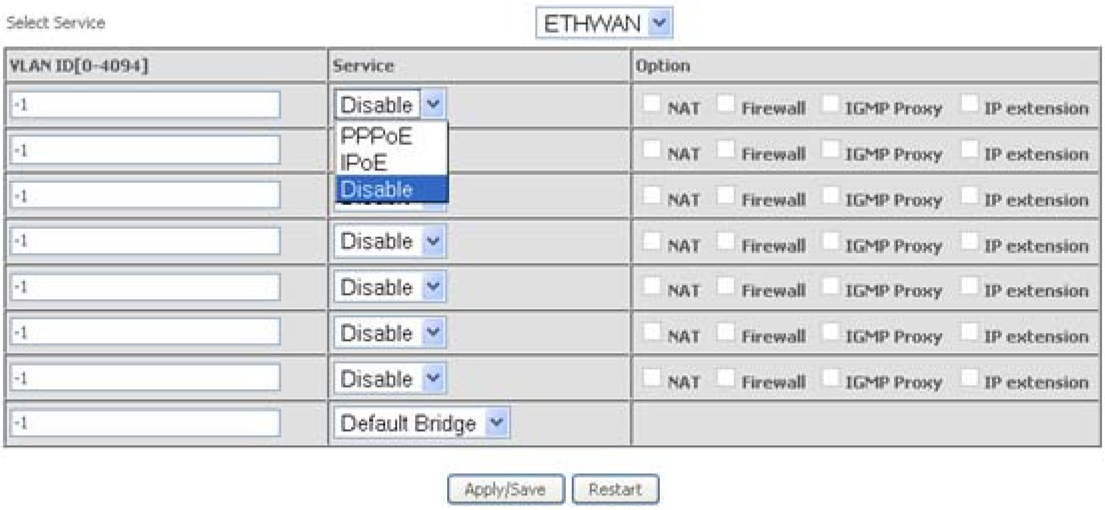


In the boxes below, enter the PPP user name and password that your ISP has provided to you.

| | |
|---|---|
| PPP Username: | username |
| PPP Password: | ●●●●●●●●●● |

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

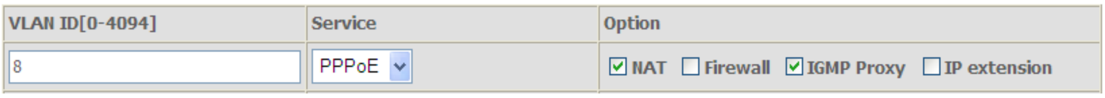
**Select a LAN-as-WAN Ethernet port for auto-detect:**
Select the Ethernet Port that will be used as ETHWAN during auto-detection.



Select Service ETHWAN

| VLAN ID[0-4094] | Service | Option |
|---|---|---|
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Disable | ☐ NAT ☐ Firewall ☐ IGMP Proxy ☐ IP extension |
| -1 | Default Bridge | |

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

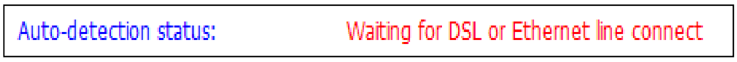


| VLAN ID[0-4094] | Service | Option |
|---|---|---|
| 8 | PPPoE | ☑ NAT ☐ Firewall ☑ IGMP Proxy ☐ IP extension |

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

### Auto Detection status and Restart

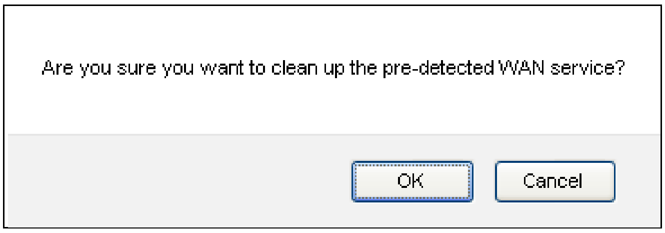
The Auto-detection status is used to display the real time status of the Auto-detection feature.



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

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

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



Are you sure you want to clean up the pre-detected WAN service?

### Auto Detection notice

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

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

## 6.2 Security

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

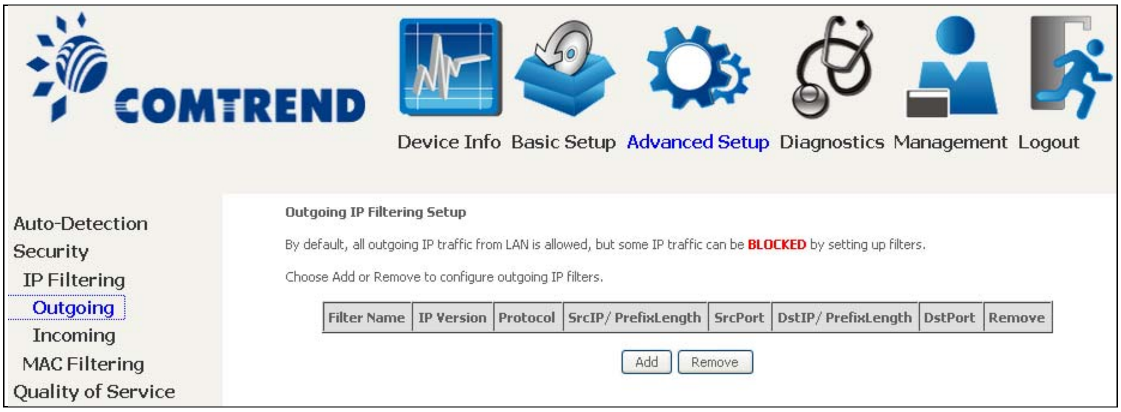
### 6.2.1 IP Filtering

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

**NOTE:** This function is not available when in bridge mode. Instead, MAC Filtering performs a similar function.

**OUTGOING IP FILTER**

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



**Outgoing IP Filtering Setup**

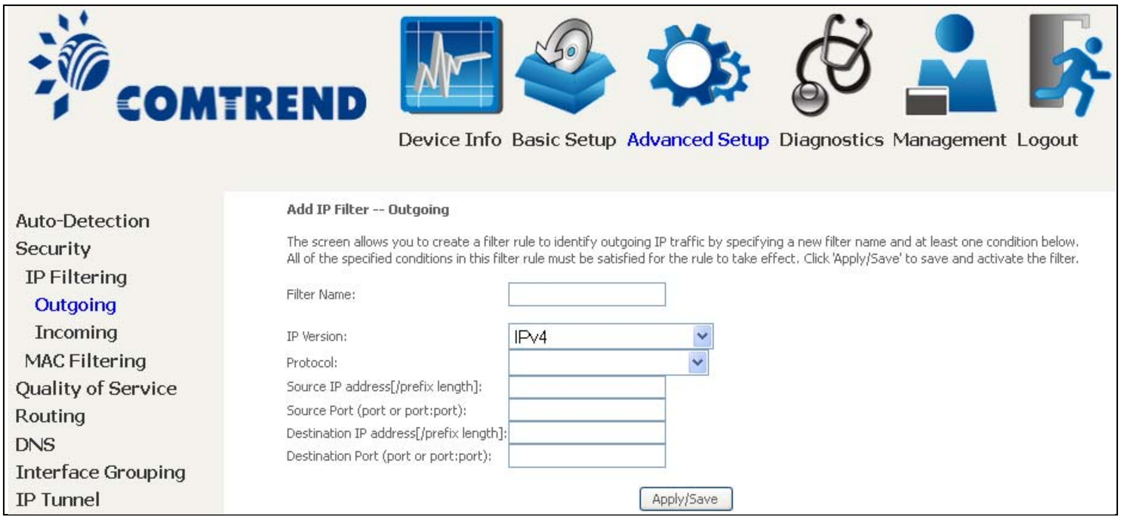
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

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

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

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



**Add IP Filter -- Outgoing**

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

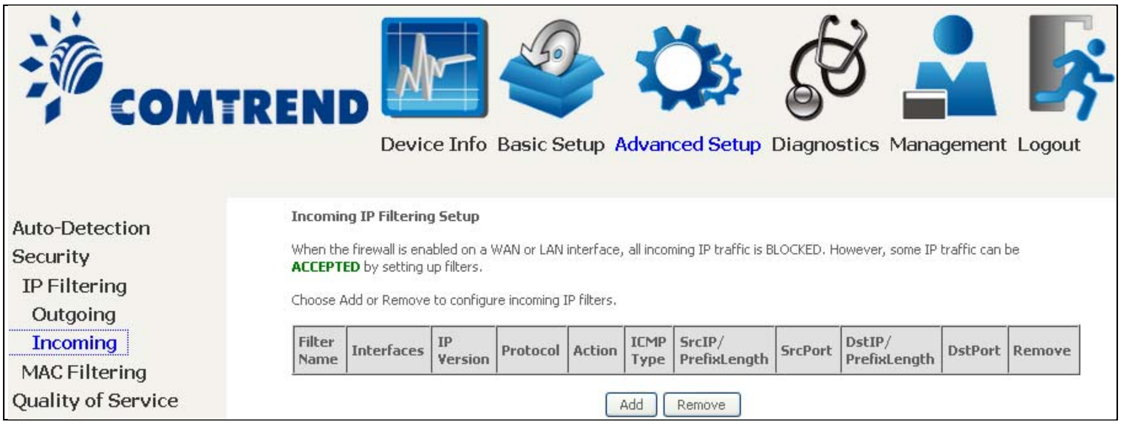
| | |
|---|---|
| Filter Name: | |
| IP Version: | IPv4 |
| Protocol: | |
| Source IP address[/prefix length]: | |
| Source Port (port or port:port): | |
| Destination IP address[/prefix length]: | |
| Destination Port (port or port:port): | |

Consult the table below for field descriptions.

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

## INCOMING IP FILTER

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



**Incoming IP Filtering Setup**

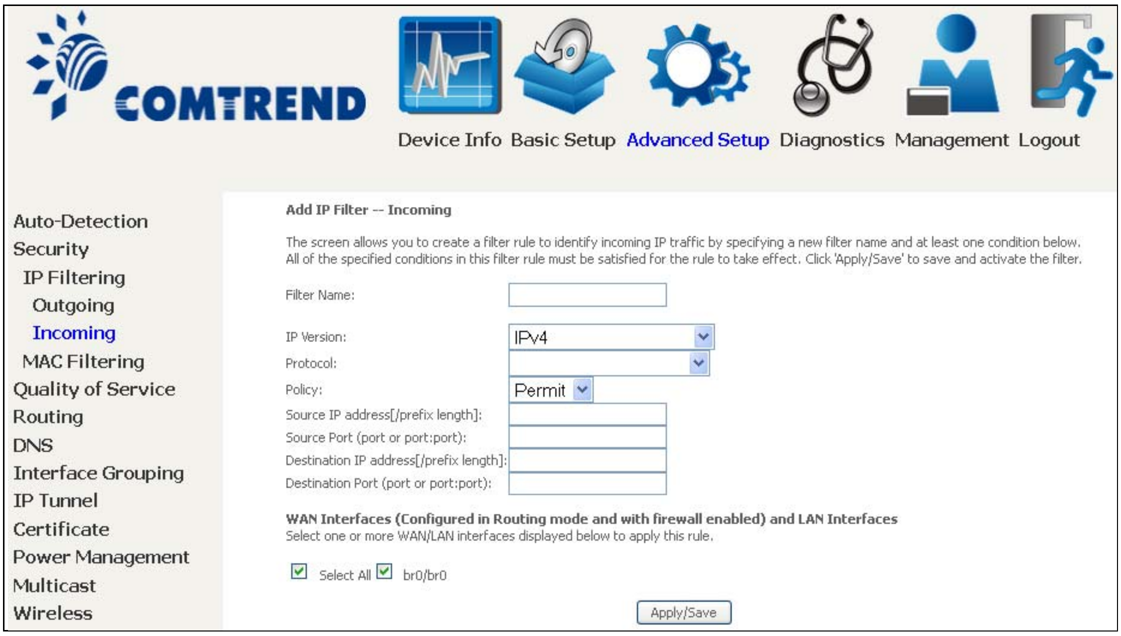
When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

| Filter Name | Interfaces | IP Version | Protocol | Action | ICMP Type | SrcIP/ PrefixLength | SrcPort | DstIP/ PrefixLength | DstPort | Remove |
|---|---|---|---|---|---|---|---|---|---|---|

To add a filter (to allow incoming IP traffic), click the **Add** button.

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



**Add IP Filter -- Incoming**

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

| | |
|---|---|
| Filter Name: | |
| IP Version: | IPv4 |
| Protocol: | |
| Policy: | Permit |
| Source IP address[/prefix length]: | |
| Source Port (port or port:port): | |
| Destination IP address[/prefix length]: | |
| Destination Port (port or port:port): | |

**WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces**
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All ☑ br0/br0

Consult the table below for field descriptions.

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

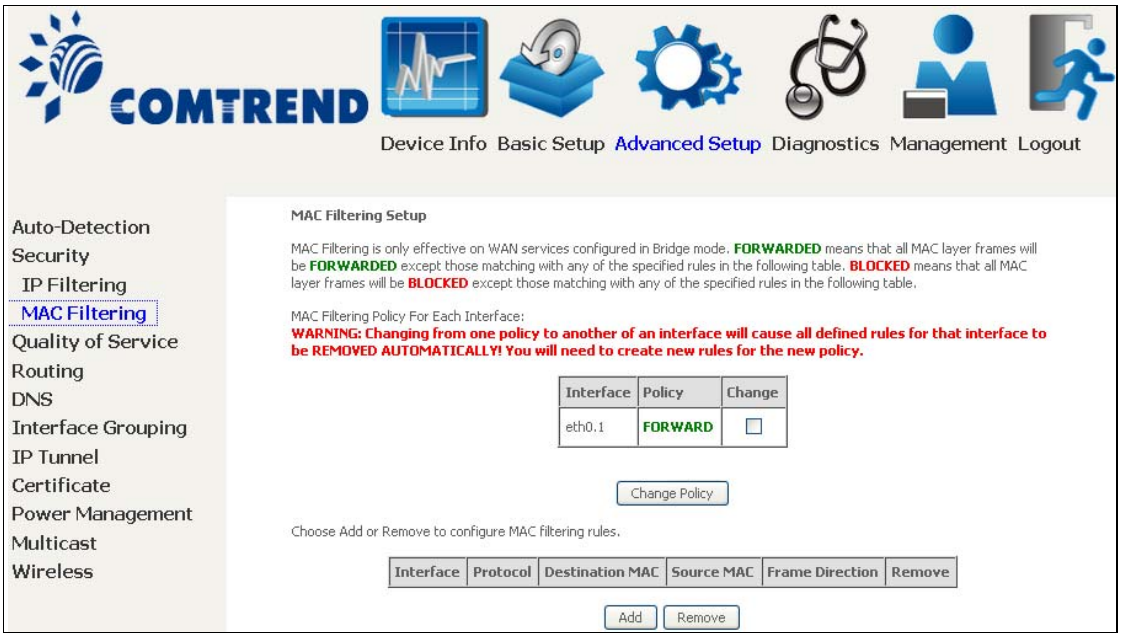
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

### 6.2.2 MAC Filtering

| | |
|---|---|
| **NOTE:** | This option is only available in bridge mode. Other modes use IP Filtering to perform a similar function. |

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the WR-6891u can be set according to the following procedure.

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



MAC Filtering Setup

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

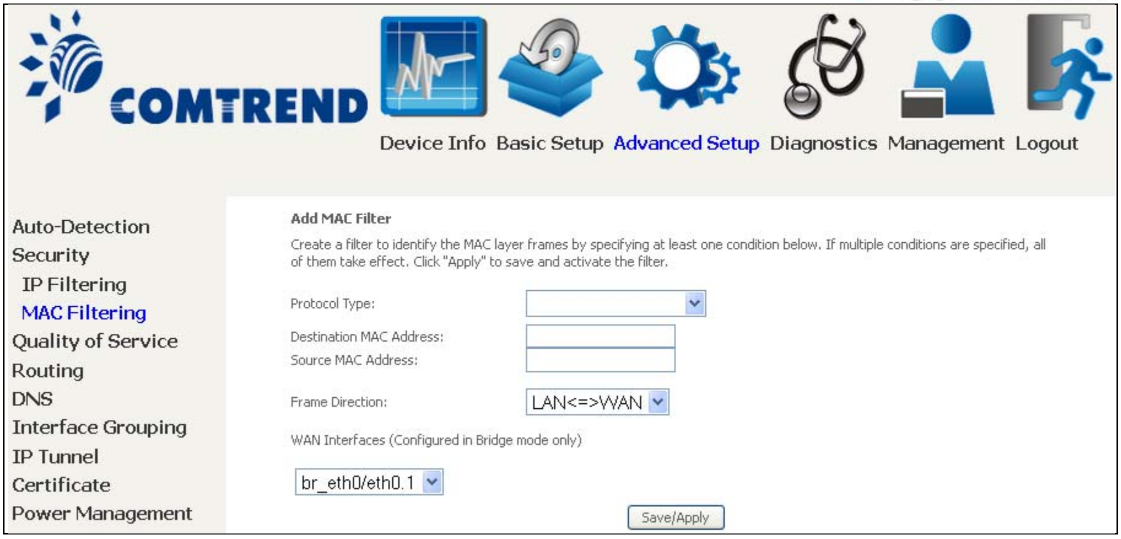
MAC Filtering Policy For Each Interface:
**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

| Interface | Policy | Change |
|---|---|---|
| eth0.1 | FORWARD | □ |

Choose Add or Remove to configure MAC filtering rules.

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

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



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_eth0/eth0.1

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

Consult the table below for detailed field descriptions.

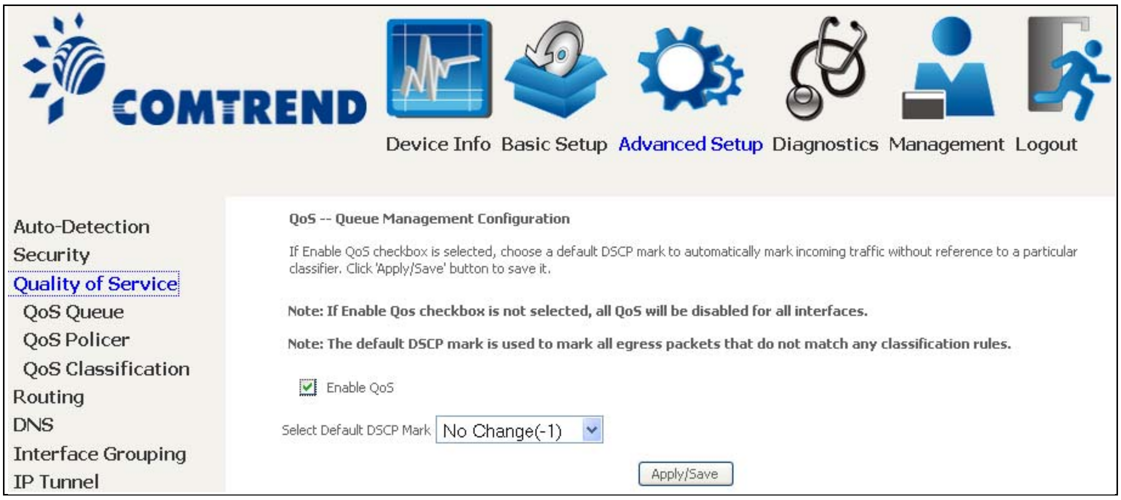
| Field | Description |
|---|---|
| Protocol Type | PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP |
| Destination MAC Address | Defines the destination MAC address |
| Source MAC Address | Defines the source MAC address |
| Frame Direction | Select the incoming/outgoing packet interface |
| WAN Interfaces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

## 6.3 Quality of Service (QoS)

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

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

Click Apply/Save to activate QoS.



QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

**Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.**

**Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.**

☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

### QoS and DSCP Mark are defined as follows:

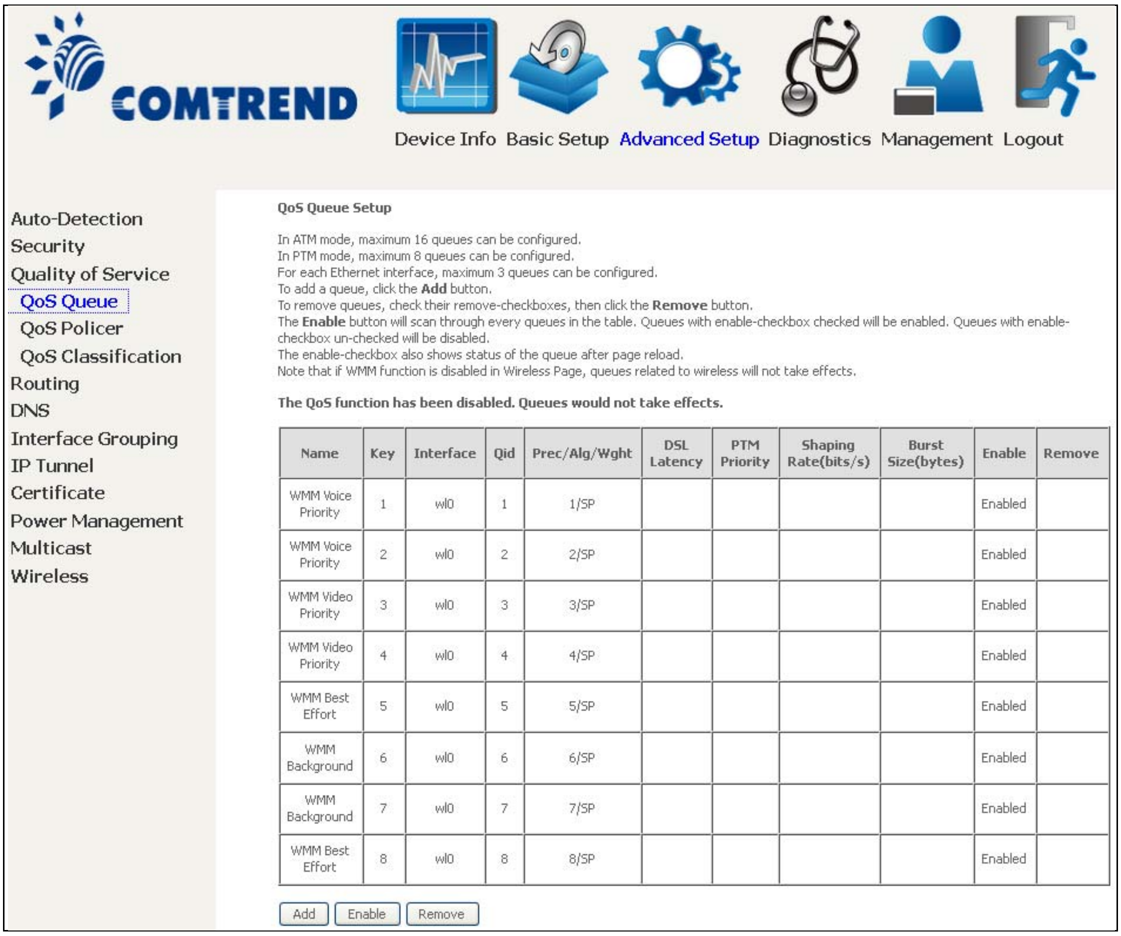
Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

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

## 6.3.1 QoS Queue Setup

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

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 3 queues can be configured.



QoS Queue Setup

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

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

| Name | Key | Interface | Qid | Prec/Alg/Wght | DSL Latency | PTM Priority | Shaping Rate(bits/s) | Burst Size(bytes) | Enable | Remove |
|---|---|---|---|---|---|---|---|---|---|---|
| WMM Voice Priority | 1 | wl0 | 1 | 1/SP | | | | | Enabled | |
| WMM Voice Priority | 2 | wl0 | 2 | 2/SP | | | | | Enabled | |
| WMM Video Priority | 3 | wl0 | 3 | 3/SP | | | | | Enabled | |
| WMM Video Priority | 4 | wl0 | 4 | 4/SP | | | | | Enabled | |
| WMM Best Effort | 5 | wl0 | 5 | 5/SP | | | | | Enabled | |
| WMM Background | 6 | wl0 | 6 | 6/SP | | | | | Enabled | |
| WMM Background | 7 | wl0 | 7 | 7/SP | | | | | Enabled | |
| WMM Best Effort | 8 | wl0 | 8 | 8/SP | | | | | Enabled | |

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

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

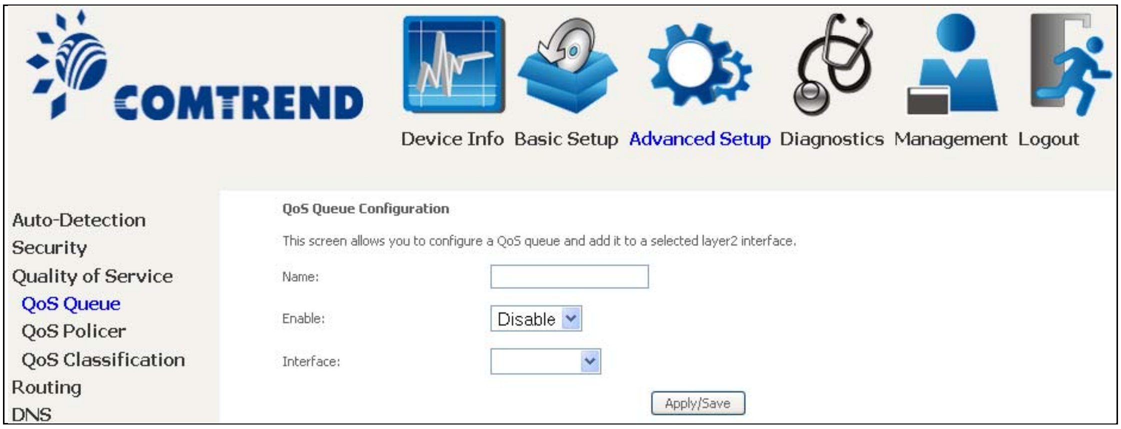
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

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

Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effect. This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button.

Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.

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



QoS Queue Configuration

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

Name:

Enable: Disable

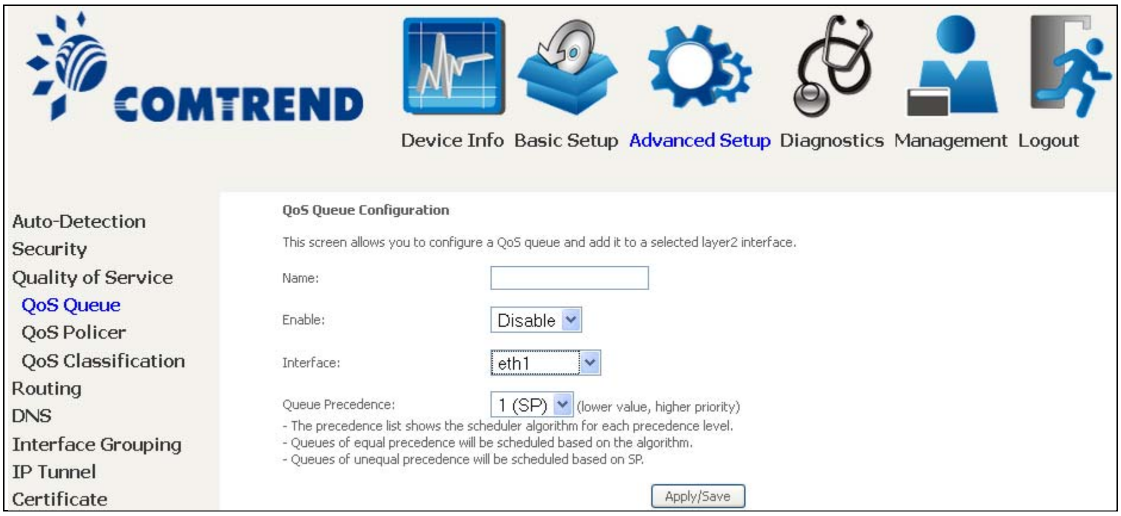
Interface:

**Name:** Identifier for this Queue entry.

**Enable:** Enable/Disable the Queue entry.

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

After selecting an Interface the following will be displayed.



QoS Queue Configuration

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

Name:

Enable: Disable

Interface: eth1

Queue Precedence: 1 (SP) (lower value, higher priority)

- The precedence list shows the scheduler algorithm for each precedence level.
- Queues of equal precedence will be scheduled based on the algorithm.
- Queues of unequal precedence will be scheduled based on SP.

The precedence list shows the scheduler algorithm for each precedence level.
Queues of equal precedence will be scheduled based on the algorithm.
Queues of unequal precedence will be scheduled based on SP.

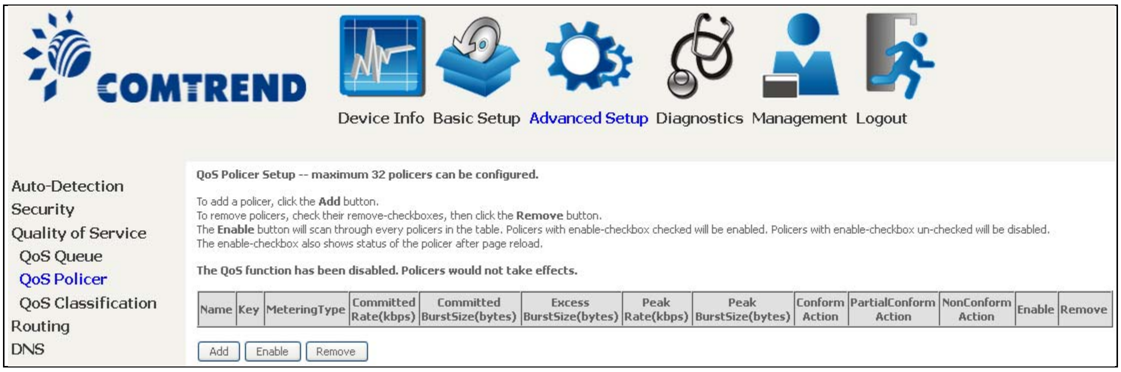
Click **Apply/Save** to apply and save the settings.

### 6.3.2 QoS Policer

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

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

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



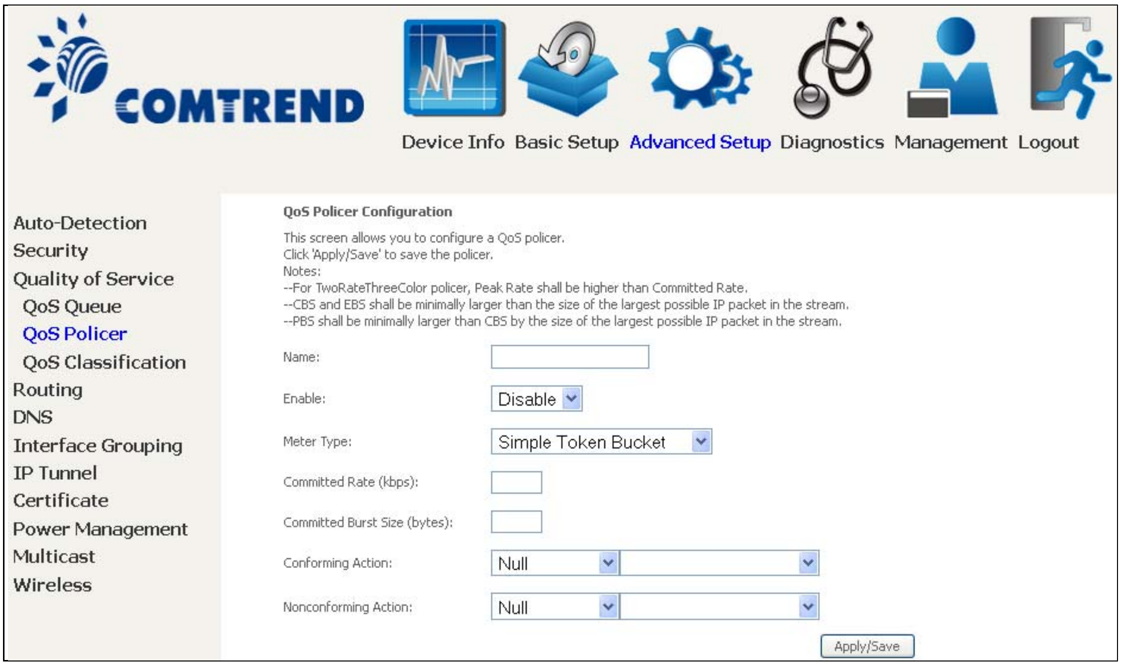
**QoS Policer Setup -- maximum 32 policers can be configured.**

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

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

| Name | Key | MeteringType | Committed Rate(kbps) | Committed BurstSize(bytes) | Excess BurstSize(bytes) | Peak Rate(kbps) | Peak BurstSize(bytes) | Conform Action | PartialConform Action | NonConform Action | Enable | Remove |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

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



QoS Policer Configuration

This screen allows you to configure a QoS policer.
Click 'Apply/Save' to save the policer.
Notes:
--For TwoRateThreeColor policer, Peak Rate shall be higher than Committed Rate.
--CBS and EBS shall be minimally larger than the size of the largest possible IP packet in the stream.
--PBS shall be minimally larger than CBS by the size of the largest possible IP packet in the stream.

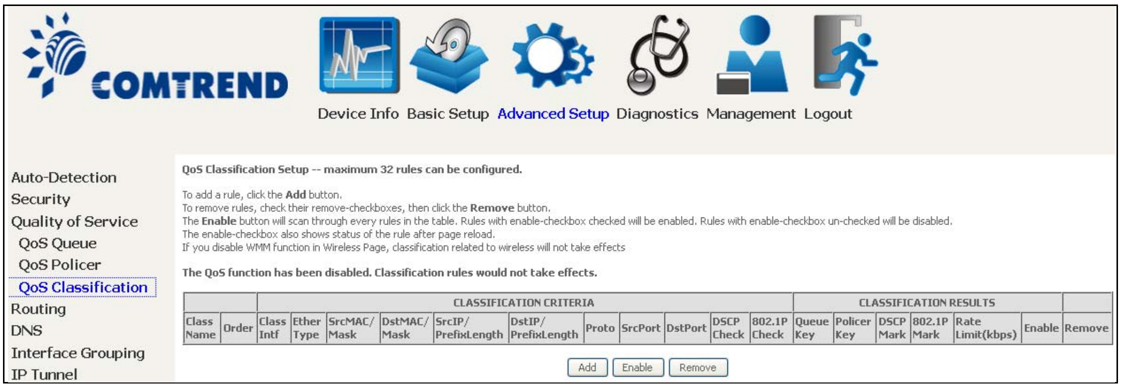
| | |
|---|---|
| Name: | |
| Enable: | Disable |
| Meter Type: | Simple Token Bucket |
| Committed Rate (kbps): | |
| Committed Burst Size (bytes): | |
| Conforming Action: | Null |
| Nonconforming Action: | Null |

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

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

### 6.3.3 QoS Classification

The network traffic classes are listed in the following table.



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

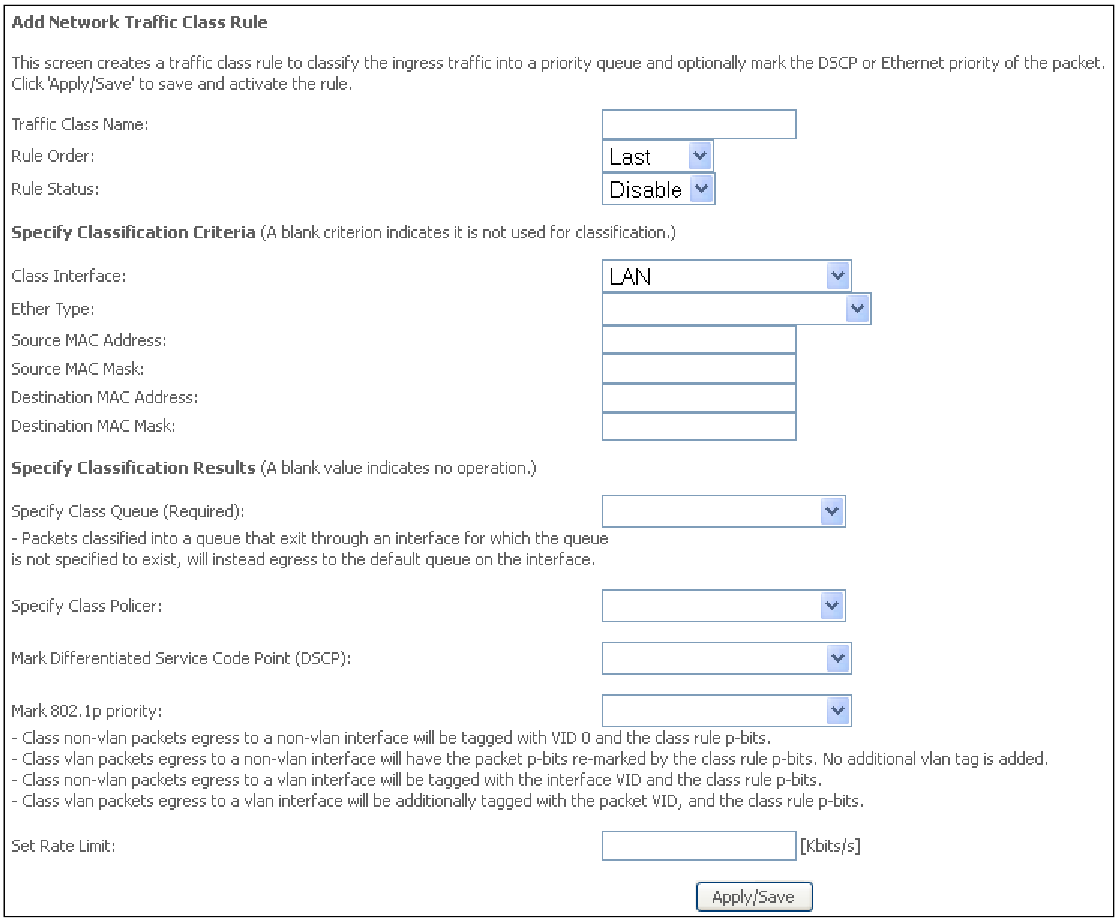
To add a rule, click the **Add** button.
To remove rules, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
The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

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

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

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

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



**Add Network Traffic Class Rule**

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

Traffic Class Name:
Rule Order: Last
Rule Status: Disable

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

Class Interface: LAN
Ether Type:
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:

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

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

Specify Class Policer:

Mark Differentiated Service Code Point (DSCP):

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

Set Rate Limit: [Kbits/s]

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

| Field | Description |
|---|---|
| Traffic Class Name | Enter a name for the traffic class. |
| Rule Order | Last is the only option. |
| Rule Status | Disable or enable the rule. |
| **Classification Criteria** | |
| Class Interface | Select an interface: (i.e.LAN, WAN, local, ETH1, ETH2, ETH3, wl0) |
| Ether Type | Set the Ethernet type (e.g. IP, ARP, IPv6). |
| Source MAC Address | A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field. |
| Source MAC Mask | This is the mask used to decide how many bits are checked in Source MAC Address. |
| Destination MAC Address | A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask. |
| Destination MAC Mask | This is the mask used to decide how many bits are checked in Destination MAC Address. |
| **Classification Results** | |
| Specify Class Queue | Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface. |
| Specify Class Policer | Packets classified into a policer will be marked based on the conforming action of the policer |
| Mark Differentiated Service Code Point | The selected Code Point gives the corresponding priority to packets that satisfy the rule. |
| Mark 802.1p Priority | Select between 0-7. |
| Set Rate Limit | The data transmission rate limit in kbps. |

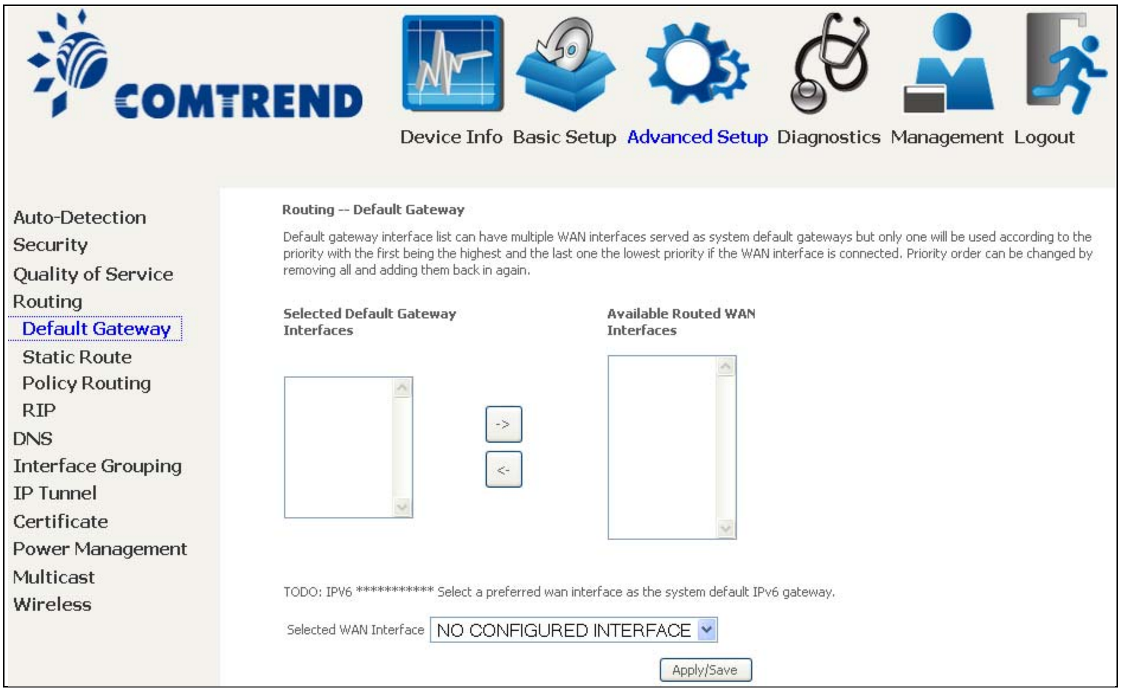
# 6.4 Routing

The following routing functions are accessed from this menu:
**Default Gateway, Static Route, Policy Routing, RIP** and **IPv6 Static Route**.

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

## 6.4.1 Default Gateway

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



**Routing -- Default Gateway**

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

**Selected Default Gateway Interfaces**

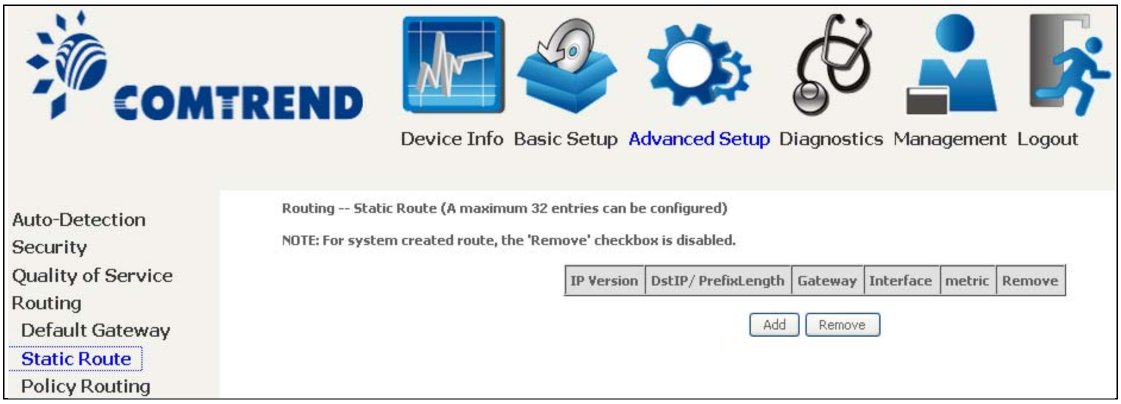
**Available Routed WAN Interfaces**

TODO: IPV6 *********** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: NO CONFIGURED INTERFACE

### 6.4.2 Static Route

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

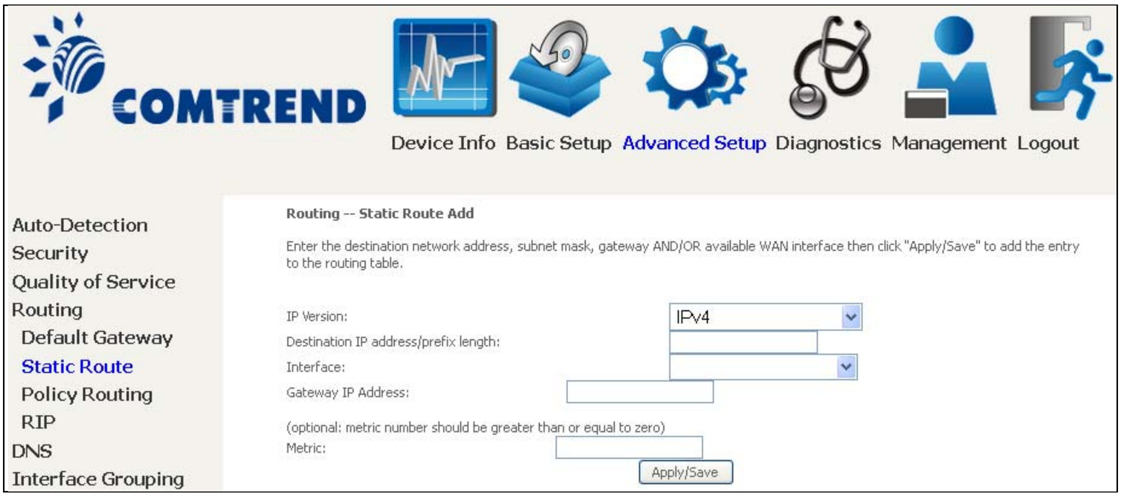


Routing -- Static Route (A maximum 32 entries can be configured)

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

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

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



Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

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

Metric:

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

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