

AR-5230 ADSL2+ Router

User Manual



Version A1.2, March 3, 2017



Preface

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

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

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

Important Safety Instructions

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

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

CAUTION:

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

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



User Information

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

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

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

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

This device complies with Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions:

1. This device may not cause interference, and

2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 Canada.

Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisies de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence

norme(s). Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas provoquer d'interférences et

2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.



Copyright

Copyright©2017 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

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

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

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

NOTE: This document is subject to change without notice.

Protect Our Environment

This symbol indicates that when the equipment has reached the end of

its useful life, it must be taken to a recycling centre and processed

separate from domestic waste.

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

Table of Contents

| CHAPTER | 1 INTRODUCTION | |
|--------------------|--------------------------|----|
| CHAPTER | 2 INSTALLATION | 7 |
| | WARE SETUP | |
| 2.2 Front | T PANEL | 9 |
| СНАРТЕР | 3 WEB USER INTERFACE | 10 |
| - | ULT SETTINGS | |
| | NFIGURATION | |
| | N PROCEDURE | |
| | | |
| - | 4 DEVICE INFORMATION | |
| | STICS | |
| 4.2 STATE 4.2.1 | LAN Statistics | |
| 4.2.1 | WAN Service | |
| 4.2.3 | XTM Statistics | |
| 4.2.4 | xDSL Statistics | |
| | E | |
| | _ | - |
| 4.5 DHCE | Р | |
| 4.6 NAT \$ | Session | |
| 4.7 IGMP | PINFO | |
| 4.8 IPv6 | | |
| 4.8.1 | IPv6 Info | |
| 4.8.2 | IPv6 Neighbor | |
| 4.8.3 | IPv6 Route | |
| | & Memory | |
| 4.10 NETV | WORK MAP | |
| CHAPTER | 5 BASIC SETUP | |
| | r 2 Interface | |
| 5.1.1 W | VAN Service Setup | |
| 5.2 NAT | | |
| 5.2.1 | Virtual Servers | |
| 5.2.2 | Port Triggering | |
| 5.2.3 | DMZ Host | |
| 5.2.4 | IP Address Map | |
| 5.2.5 | ALG/Pass-Through | |
| | | |
| 5.3.1 | LAN IPv6 Autoconfig | |
| 5.3.2 5.3.3 | Static IP Neighbor | |
| | UPnP NTAL CONTROL | |
| 5.4 FAREN | Time Restriction | - |
| 5.4.2 | URL Filter | |
| | E NETWORKING. | |
| 5.5.1 | Print Server | - |
| 5.5.2 | DLNA | |
| 5.5.3 | Storage Service | |
| | ° | |
| | A 6 ADVANCED SETUP | |
| | -DETECTION SETUP RITY | |
| 6.2. SECUE | <i>IP Filtering</i> | |
| 6.2.1 6.2.2 | MAC Filtering | |
| | ITY OF SERVICE (QOS) | |
| 6.3.1 | QoS Queue Configuration | |
| 6.3.2 | QoS Classification | |
| | | |

| 6.4 Routi | ING | |
|----------------|-------------------------------|----|
| 6.4.1 | Default Gateway | |
| 6.4.2 | Static Route | |
| 6.4.3 | Policy Routing | |
| 6.4.4 | RIP | |
| 6.5 DNS . | | |
| 6.5.1 | DNS Server | |
| 6.5.2 | Dynamic DNS | |
| 6.5.3 | DNS Entries | |
| 6.5.4 | DNS Proxy/Relay | |
| | | |
| | FACE GROUPING | |
| 6.8 IP TUN | NNEL | |
| 6.8.1 | IPv6inIPv4 | |
| 6.8.2 | IPv4inIPv6 | |
| 6.9 Certi | FICATE | |
| 6.9.1 | Local | |
| 6.9.2 | Trusted CA | |
| | ER MANAGEMENT | |
| 6.11 MUL | TICAST | |
| CHAPTER | 7 DIAGNOSTICS | 97 |
| | NOSTICS – INDIVIDUAL TESTS | |
| | RNET OAM | |
| | IE STATUS | |
| | | |
| | e Route | |
| | | |
| | 8 MANAGEMENT | |
| | NGS | |
| 8.1.1 | Backup Settings | |
| 8.1.2 | Update Settings | |
| 8.1.3 | Restore Default | |
| | EM LOG | |
| | PAGENT | |
| | | |
| | NET TIME | |
| | ss Control | |
| 8.6.1 | Accounts | |
| 8.6.2 8.6.3 | Services | |
| | IP Address | |
| | -on-LAN | |
| | TE SOFTWARE OT | |
| | | |
| CHAPTER | 9 LOGOUT | |
| APPENDIX | KA - FIREWALL | |
| APPENDIX | K B - PIN ASSIGNMENTS | |
| | X C – SPECIFICATIONS | |
| | X D - SSH CLIENT | |
| | X E - CONNECTION SETUP | |
| | K – PRINTER SERVER | |
| | | |

COMTREND Chapter 1 Introduction

AR-5230 is an ADSL2+ router comprising four 10/100 Base-T Ethernet ports and provides many software features including Firewall, and VPN pass through. It is designed for both residential and business applications, wired connectivity to an ADSL broadband network. The AR-5230 is also designed with a TR-068 compliant color panel, which eases the installation of the modem making it more user-friendly.

COMTREND Chapter 2 Installation

2.1 Hardware Setup



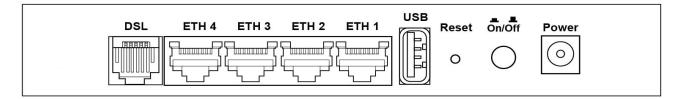
Non-stackable

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

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



DSL

Connect to the DSL port with the DSL RJ11 cable.

LAN (Ethernet) Ports

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

USB Host Port

A USB 2.0 host port supports compatible printers (See Appendix F for setup instructions) or storage devices. If a storage device is connected to the USB host port, it can be used to stream the DLNA service. Support for other devices may be added in future firmware upgrades.

Reset Button

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

NOTE: If pressed down for more than 60 seconds, the AR-5230 will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.



Power ON

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

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

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



2.2 Front Panel

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

| | Power ETH | +1 ETH 2 | E ETH 3 ETH 4 USB DSL Internet | | | | | |
|-----------|----------------|----------|---|--|--|--|--|--|
| LED | Color | Mode | Function | | | | | |
| | Create | On | The device is powered up. | | | | | |
| | Green | Off | The device is powered down. | | | | | |
| POWER | 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. | | | | | |
| | (| On | An Ethernet Link is established. | | | | | |
| ETH 1X-4X | TH 1X-4X Green | | An Ethernet Link is not established. | | | | | |
| | | Blink | Data transmitting or receiving over Ethernet. | | | | | |
| | | On | USB equipment is connected. | | | | | |
| USB | USB Green | | USB equipment is not connected. | | | | | |
| | | | Data transmission. | | | | | |
| | | On | xDSL Link is established. | | | | | |
| ופח | DSL Green | | Modem power off. | | | | | |
| DSL | | | fast: xDSL Link is training or data transmitting. slow: xDSL training failed. | | | | | |
| | | 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. | | | | | |
| INTERNET | Green | Off | Modem power off, modem in bridged mode or ADSL connection not present. In addition, if an IP or PPPoE session is dropped for any reason, other than an idle timeout, the light is turned off. | | | | | |
| | | Blink | IP connected and IP Traffic is passing through the device (either direction) | | | | | |

Note:

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

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

Leading the Communication Trend

COMTREND 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)

Technical Note

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

3.2 IP Configuration

DHCP MODE

When the AR-5230 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

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

- **NOTE:** The following procedure assumes you are running Windows. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.
- **STEP 1**: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.
- **STEP 2**: Select Internet Protocol (TCP/IP) **and click the** Properties button.
- **STEP 3:** Select Obtain an IP address automatically as shown below.

| Internet Protocol (TCP/IP) Proper | ties | <u>?</u> × |
|--|------------------|------------|
| General | | |
| You can get IP settings assigned aut this capability. Otherwise, you need t the appropriate IP settings. | | |
| Obtain an IP address automatic | cally | |
| \square^{\bigcirc} Use the following IP address: – | | |
| [P address: | | |
| S <u>u</u> bnet mask: | | |
| Default gateway: | | |
| Obtain DNS server address au | tomatically | |
| | | |
| Preferred DNS server: | | |
| Alternate DNS server: | | |
| | Ad <u>v</u> ance | :d |
| | ОКС | ancel |

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

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



STATIC IP MODE

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

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

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

- **STEP 1**: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.
- **STEP 2**: Select Internet Protocol (TCP/IP) **and click the** Properties button.
- **STEP 3:** Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.

| Internet Protocol (TCP/IP) Propertie | s <u>? ×</u> |
|---|-------------------|
| General | |
| You can get IP settings assigned autom this capability. Otherwise, you need to a the appropriate IP settings. | |
| O Obtain an IP address automatically | y |
| Use the following IP address | |
| IP address: | 192.168.1.133 |
| S <u>u</u> bnet mask: | 255.255.255.0 |
| Default gateway: | · · · |
| C Obtain DNS server address autom | atically |
| | resses: |
| Preferred DNS server: | · · · |
| <u>A</u> lternate DNS server: | · · · |
| | Ad <u>v</u> anced |
| | OK Cancel |

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 3.1 Default Settings.

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

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Chapter 4 Device Information screen and login with remote username and password.

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

| Windows Security | | | | | | | |
|--|--|--|--|--|--|--|--|
| The server 192.168.1.1 at Broadband 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). | | | | | | | |
| root ••••• ••••• Remember my credentials | | | | | | | |
| OK Cancel | | | | | | | |

Click **OK** to continue.

NOTE: The login password can be changed later (see 8.6.1 Accounts).

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



| COM | TREND | vice Info Basic Setup | Advanced Setup Diagn | Sostics Management | Logout |
|-------------------------------------|-----------------------------|---------------------------------------|--|------------------------------------|--------|
| Summary | | Device | | LAN | |
| WAN | Model | AR-5230 | | | |
| Statistics | Board ID | 96318AT-1441N3 | | | |
| Route | Serial Number | 1635230UXXF-AA000102 | ETH1 ET | TH2 ETH3 ETH4 | |
| ARP | Firmware Version | EE31-416CTU- C01_R01.A2pG039u.d26j | LAN IPv4 Address | 192.168.1.1 | |
| DHCP NAT Session | Bootloader (CFE) Version | 1.0.38-116.228-1 | LAN Subnet Mask | 255.255.255.0 d8:b6:b7:ab:27:a8 | |
| IGMP Info | Up Time | 11 mins:22 secs | DHCP Server | Enabled | |
| IPv6 CPU & Memory Network Map | | • | | | 1 |
| | | | Default Gateway | 0.0.0.0 | |
| | | | Primary DNS Server Secondary DNS Server | | |

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



14 Leading the Communication Trend

Chapter 4 Device Information

COMTREND

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



Device Info

The web user interface window is divided into two frames, the main menu (on the 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.

| COM | | vice Info Basic Setup | Advanced Setup Diagnostic | Management Logout |
|-------------------------------------|-----------------------------|---------------------------------------|---------------------------|------------------------------------|
| Summary | | Device | LA | N |
| WAN | Model | AR-5230 | | |
| Statistics | Board ID | 96318AT-1441N3 | | |
| Route | Serial Number | 1635230UXXF-AA000102 | ETH1 ETH2 | ETH3 ETH4 |
| ARP | Firmware Version | EE31-416CTU- C01_R01.A2pG039u.d26j | LAN IPv4 Address | 192.168.1.1 |
| DHCP NAT Session | Bootloader (CFE) Version | 1.0.38-116.228-1 | LAN Subnet Mask | 255.255.255.0 d8:b6:b7:ab:27:a8 |
| IGMP Info | Up Time | 11 mins:22 secs | DHCP Server | Enabled |
| IPv6 CPU & Memory Network Map | | | | WAN |
| | | | Default Gateway | DOWN |
| | | | Primary DNS Server | 0.0.0.0 |
| | | | Secondary DNS Server | 0.0.0.0 |

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).

| COMTR | | fo Basic Setu | p Advance | ed Setup | Diagnostic | cs Managen | nent Lo | ogout |
|--------------|-----------------------|----------------|-----------|----------|-----------------|----------------|---------|---------|
| Summary | | | WAN | Info | | | | |
| WAN | | | IDuc Igmp | Igmp MLD | MLD | | IPv4 | IPv6 |
| Statistics | Interface Description | Type VlanMuxId | IPv6 Pxy | Src Pxy | Src NAT Enbl | Firewall Statu | Address | Address |
| Route | | 1 | | 1 1 | 1 1 | I I | - 1 | |
| ARP | | | | | | | | |
| DHCP | | | | | | | | |
| NAT Session | | | | | | | | |
| IGMP Info | | | | | | | | |
| IPv6 | | | | | | | | |
| CPU & Memory | | | | | | | | |
| Network Map | | | | | | | | |

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

4.2 Statistics

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

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

4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.

| COMTRI | END | | | Info | Bas | sic Se | tup | Advar | Conced Set | up Dia | g | 3 ostic | s Ma | nage | men | t Lo | gout |
|-------------|--------------|---------|------|------|-------|-------------------|------|---------|------------|---------|------|------------|-------------|---------|---------|-----------|------|
| Summary | Statistics - | - LAN | | | | | | | | | | | | | | | |
| WAN | | | | | R | eceive | d | | | | | | Tra | ansmitt | ed | | |
| Statistics | Interface | | То | tal | | Multicast Unicast | | Unicast | Broadcast | Total | | | Multicast (| | Unicast | Broadcast | |
| LAN | | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts |
| WAN Service | ETH1 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| xTM | ETH2 | 0 | 0 | 0 | 0 | 0 | 0 | - | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | ETH3 | 508694 | 4342 | 0 | 0 | | 85 | | 24 | 2599362 | 4153 | 0 | 0 | 0 | 349 | 3800 | 4 |
| xDSL | ETH4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Route | | | | | | | | | | | | | | | | | |
| ARP | Reset Sta | tistics | | | | | | | | | | | | | | | |

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

4.2.2 WAN Service

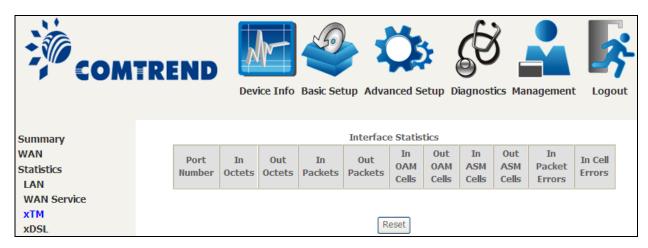
This screen shows data traffic statistics for each WAN interface.

| COM | TREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|---|--|
| Summary WAN Statistics LAN WAN Service xTM xDSL | Statistics WAN Interface Description Received Transmitted Bytes Pkts Errs Drops Bytes Pkts Reset Statistics Reset Statistics |

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

4.2.3 XTM Statistics

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



XTM Interface Statistics

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

4.2.4 xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type. The two examples below (ADSL2 & ADSL2+) show this variation.

ADSL2

| COMT | | Č5 | Ś | | |
|-------------|--|------------|-------------|-----------|-----------|
| / | Device Info Basic Setup Adva | nced Setup | Diagnostics | Managemen | t Logou |
| | | | | | |
| Summary | Statistics xDSL | | | | |
| WAN | | | | | |
| Statistics | Mode: | | ADSL G.dmt. | his | |
| LAN | Traffic Type: | | ATM | | |
| WAN Service | Status: | | Up | _ | |
| | Link Power State: | | LO | _ | |
| хТМ | call for state. | | | | |
| xDSL | | Downstrea | mUpstream | _ | |
| loute | PhyR Status: | Off | Off | _ | |
| RP | Line Coding(Trellis): | On | On | _ | |
| НСР | SNR Margin (0.1 dB): | 98 | 67 | _ | |
| AT Session | Attenuation (0.1 dB): | 40 | 25 | - | |
| | Output Power (0.1 dBm): | 131 | 120 | _ | |
| GMP Proxy | Attainable Rate (Kbps): | 12764 | 1219 | — | |
| Pv6 | Accallance Nace (Nups): | 12/04 | 1217 | 1 | |
| Vireless | | Path 0 | | Path 1 | |
| | | | mUpstream | | mUpstream |
| | Rate (Kbps): | 12767 | 1219 | 0 | |
| | Kate (KDps): | 12/07 | 1219 | μ | μ |
| | MSGc (# of bytes in overhead channel message | A. 54 | 4.4 | 0 | 0 |
| | B (# of bytes in Mux Data Frame): | 227 | 11 75 | 0 | 0 |
| | | 1 | 1 | 0 | 0 |
| | M (# of Mux Data Frames in FEC Data Frame): | 2 | 2 | | 0 |
| | T (Mux Data Frames over sync bytes): | | | 0 | |
| | R (# of check bytes in FEC Data Frame): | 0 | 0 | 0 | 0 |
| | 5 (ratio of FEC over PMD Data Frame length): | 0.5701 | 1.9804 | 0.0 | 0.0 |
| | L (# of bits in PMD Data Frame): | 3199 | 307 | 0 | 0 |
| | D (interleaver depth): | 1 | 1 | 0 | 0 |
| | Delay (msec): | 0 | 0 | 0.0 | 0.0 |
| | INP (DMT symbol): | 0.00 | 0.00 | 0.0 | 0.0 |
| | Super Frames: | 0 | 0 | 0 | 0 |
| | Super Frame Errors: | 929 | 0 | 0 | 0 |
| | RS Words: | 0 | 3459590 | 0 | 0 |
| | RS Correctable Errors: | 0 | 0 | 0 | 0 |
| | RS Uncorrectable Errors: | 0 | 0 | 0 | 0 |
| | HEC Errors: | 23 | 0 | 0 | 0 |
| | OCD Errors: | 0 | 0 | O | 0 |
| | LCD Errors: | ŏ | ő | õ | õ |
| | Total Cells: | 51557064 | 4916868 | O | 0 |
| | Data Cells: | 460 | 0 | O | 0 |
| | Bit Errors: | 0 | 0 | p 0 | 0 |
| | | | | | |
| | Total ES: | 21 | 0 | | |
| | Total SES: | 21 | 0 | | |
| | Total UAS: | 137 | 116 | | |
| | xDSL BER Test Reset Statistics Draw G | Graph | | | |

ADSL2+

| - | | ×. | <i>A</i> | | |
|-------------|--|------------|---|--------------|------------|
| | | 5 | S S S S S S S S S S S S S S S S S S S | | |
| COW! | REND | | 9 | | |
| | Device Info Basic Setup Advar | iced Setup | Diagnosti | cs Managem | ient Logo |
| | | | | | |
| ummary | Statistics xDSL | | | | |
| IAN | | | | | |
| tatistics | Mode: | | ADSL2+ | | |
| LAN | Traffic Type: | | ATM | - | |
| WAN Service | Status: | | Up | - | |
| | Link Power State: | | LO | - | |
| xTM | | | | - | |
| xDSL | | Downstrea | mUpstrear | n | |
| loute | PhyR Status: | Off | Off | _ | |
| RP | Line Coding(Trellis): | On | On | _ | |
| НСР | SNR Margin (0.1 dB): | 63 | 73 | | |
| IAT Session | Attenuation (0.1 dB): | 55 | 25 | | |
| GMP Proxy | Output Power (0.1 dBm): | 60 | 120 | | |
| | Attainable Rate (Kbps): | 26956 | 1211 | | |
| Pv6 | | | | | |
| Vireless | | Path 0 | | Path 1 | |
| | | Downstrea | mUpstrear | n Downstrean | n Upstream |
| | Rate (Kbps): | 26438 | 1207 | 0 | 0 |
| | | | | | |
| | MSGc (# of bytes in overhead channel message |): 55 | 11 | 0 | 0 |
| | B (# of bytes in Mux Data Frame): | 124 | 74 | 0 | 0 |
| | M (# of Mux Data Frames in FEC Data Frame): | 2 | 1 | 0 | 0 |
| | T (Mux Data Frames over sync bytes): | 7 | 2 | 0 | 0 |
| | R (# of check bytes in FEC Data Frame): | 4 | 0 | 0 | 0 |
| | S (ratio of FEC over PMD Data Frame length): | 0.3022 | 1.9736 | 0.0 | 0.0 |
| | L (# of bits in PMD Data Frame): | 6723 | 304 | 0 | 0 |
| | D (interleaver depth): | 32 | 1 | 0 | 0 |
| | Delay (msec): | 2 | 0 | 0.0 | 0.0 |
| | INP (DMT symbol): | 0.00 | 0.00 | 0.0 | 0.0 |
| | Super Frames: | 185303 | 176369 | 0 | 0 |
| | Super Frame Errors: | 831 | 10288 | 0 | 0 |
| | RS Words: | 39561768 | 1768879 | 0 | 0 |
| | RS Correctable Errors: | 18 | 0 | 0 | 0 |
| | RS Uncorrectable Errors: | 0 | 0 | 0 | 0 |
| | HEC Errors: | 16 | 3635 | 0 | 0 |
| | OCD Errors: | 0 | 0 | 0 | ō |
| | LCD Errors: | ő | 0 | 0 | 0 |
| | Total Cells: | 186400453 | 8507172 | 0 | 0 |
| | Data Cells: | 1474 | 3 | 0 | 0 |
| | | | | 0 | ō |
| | Bit Errors: | 0 | 0 | μ | U |
| | Bit Errors: | | | | ų |
| | Bit Errors: Total ES: | 20 | 0 | | <u>р</u> |
| | Bit Errors: | | | | |

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

| Field | Description |
|--------------|----------------------------------|
| Mode | ADSL2, ADSL2+ |
| Traffic Type | АТМ, РТМ |
| Status | Lists the status of the DSL link |

| Field | Description |
|------------------------|---|
| Link Power State | Link output power state. |
| phyR Status | Shows the status of PhyR [™] (Physical Layer Re-Transmission) impulse noise protection |
| Line Coding (Trellis) | Trellis On/Off |
| SNR Margin (0.1 dB) | Signal to Noise Ratio (SNR) margin |
| Attenuation (0.1 dB) | Estimate of average loop attenuation in the downstream direction. |
| Output Power (0.1 dBm) | Total upstream output power |
| Attainable Rate (Kbps) | The sync rate you would obtain. |
| Rate (Kbps) | Current sync rates downstream/upstream |

In ADSL2+ and ADSL2 mode, the following section is inserted.

| MSGc | Number of bytes in overhead channel message |
|-------|--|
| В | Number of bytes in Mux Data Frame |
| Μ | Number of Mux Data Frames in a RS codeword |
| Т | Number of Mux Data Frames in an OH sub-frame |
| R | Number of redundancy bytes in the RS codeword |
| S | Number of data symbols the RS codeword spans |
| L | Number of bits transmitted in each data symbol |
| D | The interleaver depth |
| Ι | The interleaver block size in bytes |
| Ν | RS codeword size |
| Delay | The delay in milliseconds (msec) |
| INP | DMT symbol |

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

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

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

xDSL BER TEST

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

| 🖀 http://192.168.1.1/berstart.tst?berState=0 - M 🔳 🗖 🗙 |
|---|
| ADSL BER Test - Start |
| The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors. |
| Select the test duration below and click "Start". |
| Tested Time (sec): 20 💌 |
| Start Close |
| × |
| 🕘 Done 📀 Internet |

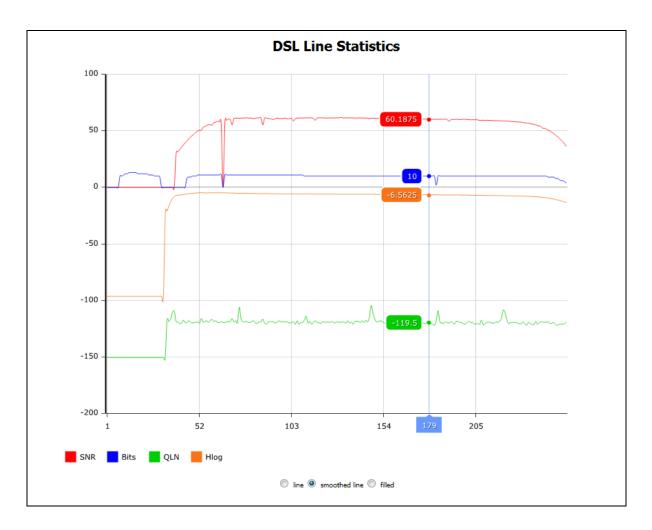
Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.

| 🗿 http://192.168.1.1/berstop.tst?berState=0 - Mi 🔳 🗖 🗙 | | | | | | |
|--|---------------------|--|--|--|--|--|
| ADSL BER Test - Result | | | | | | |
| The ADSL BER test compl | eted successfully. | | | | | |
| Test Time (sec): | 20 | | | | | |
| Total Transferred Bits: | 0x00000000000000000 | | | | | |
| Total Error Bits: | 0x000000000000000 | | | | | |
| Error Ratio: | Not Applicable | | | | | |
| Close | | | | | | |
| e Done | 🥑 Internet | | | | | |



xDSL TONE GRAPH

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



4.3 Route

Choose **Route** to display the routes that the AR-5230 has found.

| COM | REND | Device | Info Basic | Setu | ıp Ad | vanced | Setup | Diagnostics | Management | Logout |
|-------------|-------------|---------|-------------------------------------|------|-----------|---------|-----------|-------------|------------|--------|
| Summary | Device Info | | | | | | | | | |
| WAN | | | gateway, H - ho modified (redire | | reinstate | | | | | |
| Statistics | | | | | | | | | | |
| Route | Destination | Gateway | Subnet Mask | Flag | Metric | Service | Interface | <u> </u> | | |
| ARP | 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | | br0 | | | |
| DHCP | | | | | | | | | | |
| NAT Session | | | | | | | | | | |
| IGMP Info | | | | | | | | | | |

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



4.4 ARP

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

| COM | REND | Device | Info Basic Se | etup / | Advanced Setup | Diagnostics | Management | Logout |
|--------------|---------------|----------|-------------------|--------|----------------|-------------|------------|--------|
| Summary | Device Info - | - ARP | | | | | | |
| WAN | IP address | Flags | HW Address | Device | 1 | | | |
| Statistics | 192.168.1.33 | Complete | 00:50:ba:24:29:bd | br0 | | | | |
| Route ARP | | - | | | a | | | |

| 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.

| COM | REND | Device Info | Basic Set | tup Advanced | d Setup | Diagnostics | Management | Logout |
|------------|-------------|-------------------|--------------|-----------------|---------|-------------|------------|--------|
| Summary | Device Info | DHCP Leases | | | - | | | |
| WAN | Hostname | MAC Address | IP Address | Expires In | 1 | | | |
| Statistics | | 00:50:ba:24:29:bd | 192.168.1.33 | Expired/Unknown |] | | | |
| Route | | | | - | _ | | | |
| ARP | | | | | | | | |
| DHCP | | | | | | | | |
| DHCPv4 | | | | | | | | |
| DHCPv6 | | | | | | | | |

| 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 |



| COM | REND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|------------|-------------|---------------|----------------|----------------|-------------|------------|--------|
| Summary | Device Info | DHCPv6 Leases | | | | | |
| WAN | IPv6 Addres | 5 MAC Address | Duration Expir | res In | | | |
| Statistics | | 1 | 1 | | | | |
| Route | | | | | | | |
| ARP | | | | | | | |
| DHCP | | | | | | | |
| DHCPv4 | | | | | | | |
| DHCPv6 | | | | | | | |

| 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

This page displays all NAT connection session including both UPD/TCP protocols passing through the device.

| COM | REN | | evice Info Bas | ic Setup | Advanced | S etup | Diagnostics | Manageme | ent Logout |
|-------------|-----|---------|----------------|----------------|------------------|---------------|-------------|----------|------------|
| Summary | | | | | NAT Sessio | n | | | |
| WAN | | | Pre | ess "Show All" | will show all NA | T session i | nformation. | | |
| Statistics | So | urce IP | Source Port | Destinatio | n IP | Destinat | ion Port | Protocol | Timeout |
| Route | | | - | | | | | | <u> </u> |
| ARP | | | | R | efresh Sho | ow All | | | |
| DHCP | | | | | | | | | |
| NAT Session | | | | | | | | | |

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 | |
| 192.168.1.33 | 52347 | 192.168.1.1 | 80 | tcp | 86399 | |
| Refresh Show Less | | | | | | |

| 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 Info

Click **IGMP Info** to display the list of IGMP entries broadcasting through the IGMP proxy enabled WAN connection.

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|-------------|---|--------|
| Summary | List of IGMP Proxy Entries | |
| WAN | Interface WAN Groups Member Timeout | |
| Statistics | | |
| Route | | |
| ARP | | |
| DHCP | | |
| NAT Session | | |
| IGMP Info | | |

| 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

Click **IPv6 Info** to display the IPv6 WAN connection info.

| COMT | | Logout |
|--|---|--------|
| Summary WAN Statistics Route ARP DHCP | IPv6 WAN Connection Info Interface Status Address Prefix General Info Device Link-local Address fe80::dab6:b7ff:feab:27a8/64 Default IPv6 Gateway | |
| NAT Session IGMP Info IPv6 IPv6 Info IPv6 Neighbor IPv6 Route | 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

Click **IPv6 Neighbor** to display the list of IPv6 nodes discovered.

| COMT | | nfo Ba | asic Setup Ad | Vanced | S etup | Diagnostics | Management | Logout |
|---------------|---------------------------|----------|-------------------|--------|---------------|-------------|------------|--------|
| Summary | Device Info IPv6 Neigl | ibor Dis | covery table | | | | | |
| WAN | IPv6 address | Flags | HW Address | Device | | | | |
| Statistics | fe80::dab6:b7ff:feab:27a8 | STALE | d8:b6:b7:ab:27:a8 | br0 | | | | |
| Route | | | | | | | | |
| ARP | | | | | | | | |
| DHCP | | | | | | | | |
| NAT Session | | | | | | | | |
| IGMP Info | | | | | | | | |
| IPv6 | | | | | | | | |
| IPv6 Info | | | | | | | | |
| IPv6 Neighbor | | | | | | | | |
| IPv6 Route | | | | | | | | |

| 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

Click **IPv6 Route** to display the IPv6 route info.

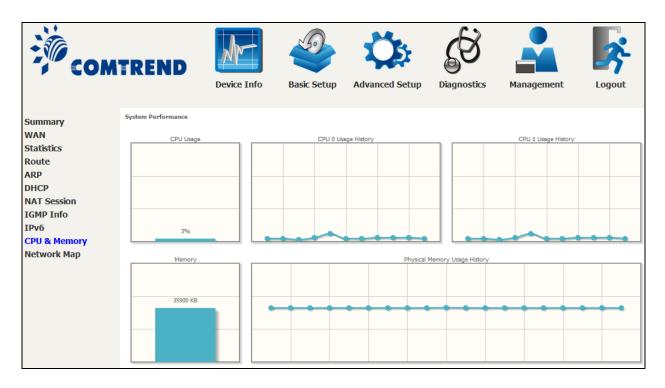
| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|--|---|--------|
| Summary WAN Statistics Route ARP | Device Info IPv6 Route Destination Gateway Metric Interface | |
| DHCP NAT Session IGMP Info IPv6 IPv6 Info IPv6 Neighbor IPv6 Route | | |

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

4.9 CPU & Memory

Displays the system performance graphs. Shows the current loading of the CPU and memory usage with dynamic updates.

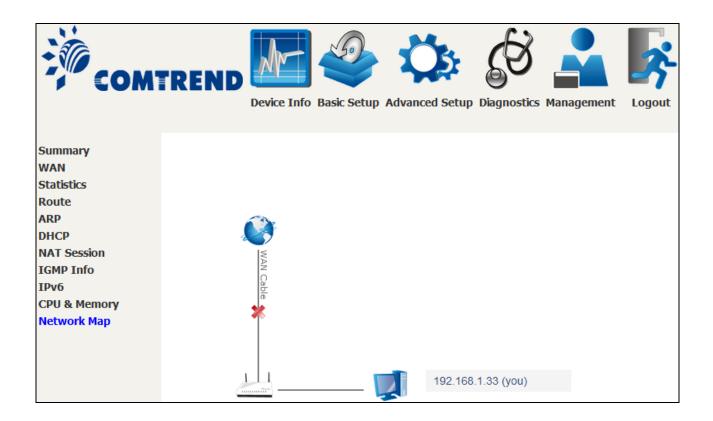
Note: This graph is unavailable for Internet Explorer users.





4.10 Network Map

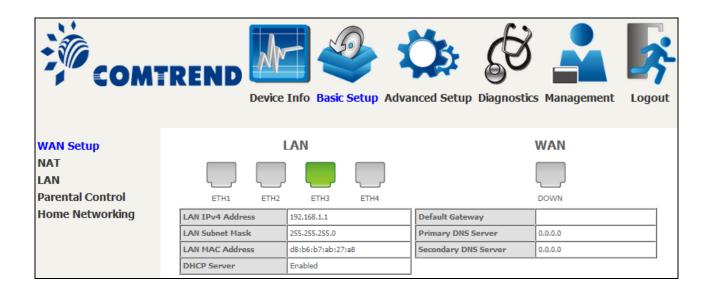
The network map is a graphical representation of router's wan status and LAN devices. The feature is only available using a non-IE browser.



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



This will bring you to the following screen.



5.1 Layer 2 Interface

Click WAN Setup on the on the left of your screen. Add or remove ATM, PTM and ETH WAN interface connections here.

| COM | Image: New Sector Field of Control of Contro of Control of Control of Control of Control o |
|---|---|
| WAN Setup NAT LAN Parental Control | Step 1: Layer 2 Interface Select new interface to add: ATM Interface Add DSL ATM Interface Configuration |
| Home Networking | Interface Vpi Vci DSL Latency Category Peak Cell Rate(cells/s) Sustainable Cell Rate(cells/s) Size(bytes) Type Mode QoS Prec/Alg/Wght Remove |
| | DSL PTM Interface Configuration Interface DSL Latency PTM Priority Conn Mode IP QoS Remove ETH WAN Interface Configuration ETH WAN Interface Configuration Eth WAN Interface Configuration Eth WAN Interface Configuration |
| | Interface/(Name) Connection Mode Remove |
| | Step 2: Wide Area Network (WAN) Service Setup |
| | Interface Description Type Vlan8021p VlanMuxId VlanTpid Igmp Proxy Igmp Source NAT Firewall IPv6 Mld Proxy Mld Source Remove Edit |

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

NOTE: Up to 3 ATM interfaces can be created and saved in flash memory.

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

5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.

| Step 2: W | Step 2: Wide Area Network (WAN) Service Setup | | | | | | | | | | | | | |
|-----------|---|------|-----------|-----------|----------|---------------|----------------|-----|----------|------|--------------|---------------|--------|------|
| Interface | Description | Туре | Vlan8021p | VlanMuxId | VlanTpid | Igmp Proxy | Igmp Source | NAT | Firewall | IPv6 | Mld Proxy | Mld Source | Remove | Edit |
| | Add Remove | | | | | | | | | | | | | |

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

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

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



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.



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

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|--|--|
| WAN Setup NAT Virtual Servers Port Triggering DMZ Host IP Address Map ALG/Pass-Through LAN Parental Control Home Networking | NAT Virtual Servers Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the 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 "External Port Start". Remaining number of entries that can be configured:32 Choose One Interface Concose One Interface Des Enterface Service Name: Select One Custom Service: Server IP Address: 192.168.1. Denable NAT Loopback External Port Start External Port End Protocol Internal Port Start Internal Port End Protocol Internal Port Start Internal Port End |
| | TCP TCP TCP TCP TCP Apply/Save |

Consult the table below for field and header descriptions.

38 Leading the Communication Trend



| Field/Header | Description |
|-------------------------------|---|
| Use Interface | Select a WAN interface from the drop-down box. |
| Select a Service Or | User should select the service from the list. Or |
| Custom Service | 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 Service). When a service is selected, the port ranges are automatically configured. |
| External Port End | Enter the ending external port number (when you select Custom Service). 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 Service). When a service is selected the port ranges are automatically configured |
| Internal Port End | Enter the internal port ending number (when you select Custom Service). 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.

| COM | REND | Device Info | asic Set | up Adv | anced Se | tup Diagr | bostics Man | agement | Logout |
|--|---|--|----------------------------------|--------------------------------|---|--|---------------------------------------|--------------|----------|
| WAN Setup NAT Virtual Servers Port Triggering DMZ Host | Some application dynamically op party using the | riggering Setup ons require that specifi sens up the 'Open Por a 'Triggering Ports'. Th the LAN side using the | ts' in the fire le Router all | wall when a ows the rem | n application of ote party from um 32 entries o | on the LAN initi the WAN side an be configur | iates a TCP/UDP o to establish new | onnection to | a remote |
| IP Address Map ALG/Pass-Through LAN | | Application Name | Tr Protocol | igger Port Rang Start En | Protocol | Dpen Port Range Start End | WAN Interface | Remove | |

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



| COM | Image: Second |
|---|---|
| WAN Setup NAT Virtual Servers Port Triggering DMZ Host IP Address Map ALG/Pass-Through LAN Parental Control | 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 application. 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 Save/Apply |
| Home Networking | Trigger Port Start Trigger Port End Trigger Protocol Open Port Start Open Port End Open Protocol TCP TCP |

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

Consult the table below for field and header descriptions.

| Field/Header | Description |
|---------------------------------|---|
| Use Interface | Select a WAN interface from the drop-down box. |
| Select an Application Or | User should select the application from the list. Or |
| Custom Application | 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.



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).

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|------------------|--|--------|
| WAN Setup | NAT IP Address Mapping Setup | |
| NAT | Rule Type Local Start IP Local End IP Public Start IP Public End IP Remove | |
| Virtual Servers | Add Remove | |
| Port Triggering | | |
| DMZ Host | | |
| IP Address Map | | |
| ALG/Pass-Through | | |

| Field/Header | Description |
|-----------------|------------------------------------|
| Rule | The number of the rule |
| Туре | 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.

| COMI | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|------------------|---|--------|
| WAN Setup | NAT IP Address Mapping Setup Remaining number of entries that can be configured:32 | |
| NAT | Server Name: | |
| Virtual Servers | Select a Service: One to One | |
| Port Triggering | Local Start IP Local End IP Public Start IP Public End IP | |
| DMZ Host | 0.0.0.0 | |
| IP Address Map | | |
| ALG/Pass-Through | Save/Apply | |

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 ALG/Pass-Through

Support ALG Pass-through for the listed protocols.

| COM | RENC | | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|---|--|--|-------------------|------------------------|-------------|------------|--------|
| WAN Setup NAT | | - ALG/Pass-Through is configuration doesr | 't take effect un | il router is rebooted. | | | |
| Virtual Servers Port Triggering DMZ Host IP Address Map ALG/Pass-Through LAN Parental Control | FTP: H323: TFTP: IRC: PPTP: RTSP: SIP: IPSec: | enable Disable Disable Enable Disable | | | | | |
| Home Networking | | | | Save | | | |

To allow/deny the corresponding ALG protocol, select Enable / Disable and then click the **Save** button. After reboot, the protocol will be added/removed from the system module.

5.3 LAN

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

| COM | TREND 🚾 🥝 🔅 🖧 🎼 |
|---|--|
| | Device Info Basic Setup Advanced Setup Diagnostics Management Logou |
| WAN Setup NAT LAN IPv6 Autoconfig Static IP Neighbor UPnP Parental Control Home Networking | Local Area Network (LAN) Setup Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Pefault IP Address: IP IP Address: IP IP Address: IP I |
| | ETH4 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.



Enable 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 IGMP LAN to LAN Multicast: Select Enable from the drop-down menu to allow IGMP LAN to LAN Multicast forwarding

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

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 A | ddress | Remove |
|-----|----------|------|--------|------------|
| | Add Entr | ries | Remo | ve Entries |

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

| DHCP Static IP Lease | | |
|------------------------------|--------------------------------------|------------|
| Enter the Mac address and St | atic IP address then click "Apply/Sa | ve". |
| | | _ |
| MAC Address: | 12:34:56:78:90:12 | |
| IP Address: | 192.168.1.33 | |
| | | |
| | | |
| | | Apply/Save |

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

| MAC Address | IP Address | Remove |
|-------------------|--------------|--------|
| 12:34:56:78:90:12 | 192.168.1.33 | |
| Add Entries | Remove Er | ntries |



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.

| ETH1 | Auto 🔽 |
|------|--------------|
| ETH2 | Auto |
| | 10Mbps-Half |
| ETH3 | 10Mbps-Full |
| ETH4 | 100Mbps-Half |
| | 100Mbps-Full |

5.3.1 LAN IPv6 Autoconfig

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

| COM | TREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|---|---|
| WAN Setup NAT LAN IPv6 Autoconfig Static IP Neighbor UPnP Parental Control Home Networking | Index Index Index State Index Index |
| | Enable ULA Prefix Advertisement Andomly Generate Statically Configure Prefix: Prefix: |

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 | Inte | rface ID | Remove |
|-----|----------|------|----------|-----------|
| | Add Entr | ies | Remove | e Entries |

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

| DHCP Static IP Lease | 1 | |
|-----------------------|--|-----|
| Enter the Mac address | and Static Interface ID then click "Apply/Save | e". |
| | | |
| MAC Address: | 00:11:22:33:44:55 | |
| Interface ID: | 0:0:0:2 | |
| | | |
| | Apply/Save | 2 |

To remove an entry, tick the corresponding checkbox \square 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 | |
| Add Entries | | Remove Entrie | s |

- - -

- -

- - -

_

.

| 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 | Specify the prefix to be used |
| Prefix | 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 |
| Standard Mode | In standard mode, IPv6 multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if MLD snooping is enabled |
| Blocking Mode | In blocking mode, IPv6 multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group |
| Enable MLD LAN To LAN Multicast | Enable/disable IPv6 multicast between LAN ports |

5.3.2 Static IP Neighbor

| COM | | gout |
|--|--|------|
| WAN Setup | Static ARP/IP Neighbor Configuration | |
| NAT | IP Version IP Address MAC Address Interface Remove | |
| LAN IPv6 Autoconfig Static IP Neighbor UPnP | Add Remove | |

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

| COM | TREND Device In | fo Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--------------------|------------------------------|----------------|----------------|-------------|------------|--------|
| WAN Setup | Static IP Neighbor Configura | tion | | | | |
| NAT | IP Version: | | IPv4 | | • | |
| LAN | IP Address: | | | | | |
| IPv6 Autoconfig | MAC Address: | | | | | |
| Static IP Neighbor | Associated Interface: | | LAN/br0 - | | | |
| UPnP | | | Apply/Save | | | |

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.

| COM | TREND Que to the setup Diagnostics Management Lo | ogout |
|--|---|-------|
| WAN Setup | UPnP Configuration | |
| NAT | NOTE: UPnP is activated only when there is a live WAN service with NAT enabled. | |
| LAN IPv6 Autoconfig Static IP Neighbor | Enable UPnP | |
| UPnP | Apply/Save | |

5.4 Parental Control

This selection provides WAN access control functionality.

5.4.1 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.

| COM | TREND | Device Info | Basic Set | Advance | ced Setup | Diagnostics | Management | Logout |
|------------------|-------------------|------------------|-----------------|-----------------|------------|--|------------|--------|
| WAN Setup | Access Time Restr | riction A maximu | ım 32 entries (| an be configure | ed. | | | |
| NAT | | Username MAC | Mar Tur | Wed Thu Fri | Cab Cure (| the state of the s | Remove | |
| LAN | | Username MAC | . Mon Tue | | Sat Sun 3 | Start Stop Enable | e Kemove | |
| Parental Control | | | ſ | Add Enab | Remov | | | |
| Time Restriction | | | l | | | | | |
| URL Filter | | | | | | | | |
| Home Networking | | | | | | | | |

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

| COM | | Info Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--|--|-----------------------------|------------------------------|-----------------------|------------------------|--------------|
| WAN Setup NAT LAN Parental Control Time Restriction URL Filter Home Networking | Access Time Restriction This page adds time of day restr MAC address of the LAN device MAC address of the other LAN of User Name Browser's MAC Address Other MAC Address (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | where the browser is runnin | g. To restrict other LAN dev | ice, click the "Other | MAC Address" button ar | id enter the |
| | Days of the week Click to select Start Blocking Time (hh:mm) End Blocking Time (hh:mm) | Mon Tue Wed Thu | Fri Sat Sun | | | |

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.



5.4.2 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.

| COM | TREND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|------------------|--|--------|
| WAN Setup | URL Filter Please select the list type first then configure the list entries. Maximum 100 entries can be configured. | |
| NAT . | Note: URL filter can be applied only to HTTP protocol that was based on following listed port(s). | |
| LAN | URL List Type: 🔘 Exclude 🔘 Include | |
| Parental Control | | |
| Time Restriction | | |
| URL Filter | Address Port Remove | |
| Home Networking | Add 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 "Apply/Save" to add the entry to the URL filter. | | | | | | | | |
| | | | | | | | | |
| URL Address: | www.yahoo.com | | | | | | | |
| Port Number: | 80 | (If leave blank, default 80 will be applied.) | | | | | | |
| Rule will be applied based on the entere | d port! | | | | | | | |
| Apply/Save | | | | | | | | |

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: | ٢ | Exclude | ۲ | Include | | | | |
| | | | | | Address | Port | Remove | |
| | | | | | www.yahoo.com | 80 | | |
| Add Remove | | | | | | | | |

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

5.5 Home Networking

5.5.1 Print Server

This page allows you to enable or disable printer support.

| COM | TREND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|-------------------------------------|---------------------|------------------------|------------------|----------------|-------------|------------|--------|
| WAN Setup | Print Server sett | 2 | | | | | |
| NAT | This page allows yo | ou to enable / disable | printer support. | | | | |
| LAN | Manufacturer I | Product Serial Num | iber | | | | |
| Parental Control Home Networking | Enable on-bo | ard print server. | | | | | |
| Print Server | | | | | | | |
| DLNA | | | | | | | |
| Storage Service | | | | Apply/Save | | | |

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

5.5.2 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.

| COM | TREND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|---|-------|---|-------------|----------------|--------------------|------------|--------|
| WAN Setup NAT LAN Parental Control Home Networking Print Server DLNA Storage Service | | ver settings ou to enable / disable ard digital media serve | - | upport. | | | |
| | | | | Apply/Save | | | |

5.5.3 Storage Service

This page displays storage devices attached to USB host.

| COM | TREND | Device Info | Basic Setu | Advanced Set | Diagnostics | Management | Logout |
|--|--|-------------|------------|--|--------------------|------------|--------|
| WAN Setup NAT LAN Parental Control | Storage Service The Storage service | | - | n modem to be more easily eSystem Total Space | Free Space Actions |] | |
| Home Networking Print Server DLNA Storage Service | | | | | | | |

Display after storage device attached (for your reference).

| Volumename | FileSystem | Total Space | Free Space | Actions |
|------------|------------|-------------|------------|---------------|
| usb1_1 | fat | 14770 MB | 5762 MB | Safely remove |

COMTREND 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.

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|--|---|
| Auto-Detection Security Quality of Service Routing DNS | Auto-detection setup The auto-detection function is used for CPE to detect WAN service for either ETHWAN or xDSL interfaces 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 |
| DSL Interface Grouping IP Tunnel Certificate Power Management Multicast | Apply/Save Restart |

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



| COM | REND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--|---|--|---|-----------------------------|-------------|---------------------|-------------|
| Auto-Detection Security Quality of Service Routing DNS DSL Interface Grouping IP Tunnel Certificate Power Management Multicast | The feature is design Users shall enter giv function. Auto-detection state | unction is used for CPE t ed for the scenario that t en PPP username/passwo letect us: Waiting , enter the PPP user name name: word: IN Ethernet port for auto | equires only one WAN rd and pre-configure so of or DSL or Ethernet lin a and password that you autoconfig1 -detect | ur ISP has provided to you. | ons, | | o-detect |
| | VPI[0-255] | VCI[32-65535] | Service | | Option | | |
| | 0 | 32 | Disable | • | NAT Firewa | | P extension |
| | 0 | 32 | Disable | • | NAT Firewa | II 🔲 IGMP Proxy 🗌 I | P extension |
| | 0 | 32 | Disable | • | NAT Firewa | II 🗌 IGMP Proxy 🗌 I | P extension |
| | 0 | 32 | Disable | • | NAT Firewa | II 🗌 IGMP Proxy 🗌 I | P extension |
| | 0 | 32 | Disable | • | NAT Firewa | II 🗌 IGMP Proxy 🗌 I | P extension |
| | 0 | 32 | Disable | • | NAT Firewa | II 🗌 IGMP Proxy 🗌 I | P extension |
| | 0 | 32 | Disable | • | NAT Firewa | II 🗌 IGMP Proxy 🗌 I | P extension |
| | 0 | 32 | Default I | Bridge 👻 | | | |
| | - | | | Apply/Save Restart | | | |
| | | | | | | | |

| In the boxes below, enter the PPP user name and p | assword that your ISP has provided to you. |
|---|--|
| PPP Username: | |
| PPP Password: | ••••• |

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

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

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

| Select Service | | ATM - |
|----------------|---------------|------------------|
| VPI[0-255] | VCI[32-65535] | Service |
| 0 | 32 | Disable 💌 |
| 0 | 32 | PPPoE PPPoA |
| 0 | 32 | IPoE Disable |
| 0 | 32 | Disable - |
| 0 | 32 | Disable 👻 |
| 0 | 32 | Disable 🔻 |
| 0 | 32 | Disable 👻 |
| 0 | 32 | Default Bridge 🔻 |

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

| Select Service | PTM/ETHWAN 👻 |
|-----------------|------------------|
| VLAN ID[0-4094] | Service |
| -1 | Disable 💌 |
| -1 | PPPoE IPoE |
| -1 | Disable |
| -1 | Disable 👻 |
| -1 | Disable 🔻 |
| -1 | Disable 🔻 |
| -1 | Disable 🔻 |
| -1 | Default Bridge 👻 |

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

| Apply/Save | Restart |
|------------|---------|
| | |

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



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

| VPI[0-255] | VCI[32-65535] | Service | Option |
|------------|---------------|---------|--------------------------------------|
| 0 | 32 | PPPoE 🔻 | NAT Firewall IGMP Proxy IP extension |

| VLAN ID[0-4094] | Service | Option |
|-----------------|---------|--------------------------------------|
| -1 | PPPoE 🔻 | NAT Firewall IGMP Proxy IP extension |

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.

| Message f | rom webpage |
|-----------|---|
| ? | Are you sure you want to clean up the pre-detected WAN service? |
| | OK Cancel |

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.

| COM | REND | Device Info | Basic Setu | p Advanced Setu | p Diagnostics | Management | Logout |
|-------------------|----------------------|--------------------------|------------------------|------------------------------------|------------------------|------------------|--------|
| Auto-Detection | Outgoing IP Filte | ring Setup | | | | | |
| Security | By default, all outg | oing IP traffic from LAN | is allowed, but some I | P traffic can be BLOCKED by | setting up filters. | | |
| IP Filtering | Choose Add or Rer | move to configure outgo | ing IP filters. | | | | |
| Outgoing | | Filter Name IP \ | ersion Protocol | SrcIP/ PrefixLength SrcP | ort DstIP/ PrefixLengt | h DstPort Remove | |
| Incoming | | 1 1 | - I I | | | 1 1 | |
| Denial of Service | | | | Add 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**.



| COM | REND Device Inf | o Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--------------------|--|---------------------------|--------------------------------|------------------------|-------------------------|-------------|
| Auto-Detection | Add IP Filter Outgoing | | | | | |
| Security | The screen allows you to create a f | | | | | |
| IP Filtering | All of the specified conditions in this | ; filter rule must be sat | isfied for the rule to take ef | fect, Click 'Apply/Sav | e' to save and activate | the filter. |
| Outgoing | Filter Name: | | | | | |
| Incoming | IP Version: | IPv4 | | | | |
| 5 | | 1644 | | | | |
| Denial of Service | Protocol: | | • | | | |
| MAC Filtering | Source IP address[/prefix length]: | | | | | |
| Quality of Service | Source Port (port or port:port): | | | | | |
| Routing | Destination IP address[/prefix lengt Destination Port (port or port:port) | - | | | | |
| DNS | Destination Port (port of portsport) | - | | | | |
| DSL | | | | | | |
| | | | Apply/Save | | | |
| Interface Grouping | | | | | | |

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.

| COM | TREND | | vice Info | Basic | Setup | Adva | nced Setup | Diagnos | Stics Manage | ement | Logout |
|--|---|------------------------------|---------------|----------|--------|---------------------|----------------------------------|-----------|------------------------|--------------------|---------|
| Auto-Detection Security IP Filtering Outgoing | Incoming I When the fir by setting up Choose Add | rewall is enab p filters. | oled on a W | | | all incomi | ng IP traffic is BLO | CKED. How | ever, some IP traff | ìc can be A | CCEPTED |
| Incoming Denial of Service MAC Filtering | Filter Name I | Interfaces | IP Version | Protocol | Action | ICMP Type Add | SrcIP/ PrefixLength Remove | 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**.



| COM | TREND Device Info | Basic Setup | Advanced Setu | Diagnostics | Management | Logout |
|--------------------|---|-----------------------|-------------------------|-----------------------|--------------------------|---------------|
| Auto-Detection | Add IP Filter Incoming | | | | | |
| Security | The screen allows you to create a filter All of the specified conditions in this fil | | | | | |
| IP Filtering | | ter rule must be sati | | arecti Click Apply/Se | ive to save and activate | e the filter. |
| Outgoing | Filter Name: | | | | | |
| Incoming | IP Version: | IPv4 | • | | | |
| Denial of Service | Protocol: | | - | | | |
| MAC Filtering | Policy: | Permit 🝷 | | | | |
| Quality of Service | Source IP address[/prefix length]: | | | | | |
| Routing | Source Port (port or port:port): Destination IP address[/prefix length]: | | | | | |
| DNS | Destination Port (port or port:port): | | | | | |
| DSL | WAN Interfaces (Configured in Ro | uting mode and u | ith firewall enabled) a | | | |
| Interface Grouping | Select one or more WAN/LAN interfac | | | nu LAN Interfaces | | |
| IP Tunnel | Select All 🗹 br0/br0 | | | | | |
| Certificate | ES SECURES DIVIDIO | | | | | |
| Power Management | | | Apply/Save | | | |
| Multicast | | | | | | |

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.



Denial of Service

Denial of Services currently provides Syn-flood protection, furtive port scanner protection and Ping of death protection. This web page allows you to activate/de-activate them and to set the maximum average limit (packet per second) and the maximum burst (packet amount) for each protection.

| COMTR | | ice Inf | fo Basic Setup | Advanced Se | etup D | j iagnostics | Management | Logout |
|-------------------------------|---|---------|-----------------|-----------------|--------|------------------------|------------|--------|
| Auto-Detection | Set Denial of Servio | oes | | | | | | |
| Security | Denial of Services cur web page allows you | | | | | | | |
| IP Filtering | burst (packet amount | | | | | | | |
| Outgoing | DoS Protection E | nable | Maximum average | Maximum burst | | | | |
| Incoming | Syn-flood | | 0 | 0 | | | | |
| Denial of Service | | | ces: br0/br0 | | | | | |
| MAC Filtering | | interfa | ces: 🛄 br0/br0 | | | | | |
| Quality of Service Routing | | | | | -1 | | | |
| DNS | DoS Protection | Enable | Maximum average | e Maximum burst | - | | | |
| DSL | Furtive port scan | | 0 | 0 | | | | |
| Interface Grouping | | interfa | aces: 🔲 br0/br0 | | | | | |
| IP Tunnel | | | | | | | | |
| Certificate | DoS Protection E | nable | Maximum average | Maximum burst | | | | |
| Power Management | Ping of death | | 0 | 0 | | | | |
| Multicast | | interfa | ces: Dr0/br0 | | | | | |
| | | | | Apply/Save |) | | | |

Click the **Apply/Save** button to save and (de)activate the protection.

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 AR-5230 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.

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout | | | | | | |
|-------------------------------------|--|--|--|--|--|--|--|
| Auto-Detection | MAC Filtering Setup | | | | | | |
| Security IP Filtering | 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 Quality of Service | 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. | | | | | | |
| Routing | Interface Policy Change | | | | | | |
| DNS | | | | | | | |
| DSL | atm0.1 FORWARD | | | | | | |
| Interface Grouping IP Tunnel | Change Policy | | | | | | |
| Certificate | Choose Add or Remove to configure MAC filtering rules. | | | | | | |
| Power Management Multicast | Interface Protocol Destination MAC Source MAC Frame Direction Remove | | | | | | |
| | Add 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.



| COM | REND Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--------------------|---------------------------------------|---------------------|----------------|------------------------|-------------------------|------------|
| Auto-Detection | Add MAC Filter | | | | | |
| Security | Create a filter to identify the MAC I | | | ion below. If multiple | conditions are specifie | ed, all of |
| IP Filtering | them take effect. Click "Apply" to s | save and activate t | ne titer. | | | |
| MAC Filtering | Protocol Type: | | - | | | |
| Quality of Service | Destination MAC Address: | | | | | |
| Routing | Source MAC Address: | | | | | |
| DNS | Frame Direction: | LAN<=>V | VAN 👻 | | | |
| DSL | WAN Interfaces (Configured in Bri | idaa mada anku) | | | | |
| Interface Grouping | WANT Interfaces (Conlighted in bit | uge mode only) | | | | |
| IP Tunnel | br_0_0_35/atm0.1 👻 | | | | | |
| Certificate | | | Cours (Appella | | | |
| Power Management | | | Save/Apply | | | |
| Multicast | | | | | | |

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 $\ensuremath{\overline{\square}}$ and select a Default DSCP Mark.

Click Apply/Save to activate QoS.

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout | | | | | | | |
|---------------------------------|---|--|--|--|--|--|--|--|
| Auto-Detection | QoS Queue Management Configuration | | | | | | | |
| Security | 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. | | | | | | | |
| Quality of Service | | | | | | | | |
| QoS Queue QoS Classification | | | | | | | | |
| Routing | | | | | | | | |
| DNS DSL | ☑ Enable QoS | | | | | | | |
| Interface Grouping IP Tunnel | Select Default DSCP Mark No Change(-1) | | | | | | | |
| Certificate Power Management | Apply/Save | | | | | | | |
| Multicast | | | | | | | | |

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.

| Enable QoS | | | |
|--------------------------|---------------|---|------------|
| Select Default DSCP Mark | No Change(-1) | • | |
| | | | Apply/Save |

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 Configuration

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 4 queues can be configured.

| COM | REND | | e Info Basic S | etup Ad | V Ivanced | Setup D | J Viagnostic | s Manager | nent | Logout |
|---------------------|--|---|----------------|---------|---------------------|-----------|------------------------|-------------|--------|--------|
| Auto-Detection | QoS Queue Setup | | | | | | | | | |
| Security | | In ATM mode, maximum 16 queues can be configured. | | | | | | | | |
| Quality of Service | In PTM mode, maximum 8 queues can be configured. For each Ethernet Win Interface, maximum 4 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 queue 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. | | | | | | | | | |
| QoS Queue | | | | | | | | | | |
| Queue Configuration | | | | | | | | | | |
| QoS Classification | | | | | | | | | | |
| Routing | | | | | | | | | | |
| DNS | | | | DSL | РТМ | Shaping | Min Bit | Burst | | |
| DSL | Name Key In | iterface Qid | Prec/Alg/Wght | Latency | Priority | Rate(bps) | Rate(bps) | Size(bytes) | Enable | Remove |
| Interface Grouping | | | | | | | | | | |
| IP Tunnel | Add Enable Remove | | | | | | | | | |
| Certificate | | | | | | | | | | |
| Power Management | | | | | | | | | | |
| Multicast | | | | | | | | | | |

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.

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.



| COM | TREND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|----------------------------------|----------------------|--------------------|-------------------|--------------------------------|-------------|------------|--------|
| Auto-Detection | QoS Queue Config | guration | | | | | |
| Security | This screen allows y | you to configure a | QoS queue and add | it to a selected layer2 interf | ace, | | |
| Quality of Service | Name: | | | | | | |
| QoS Queue Queue Configuration | Enable: | E | nable 🔻 | | | | |
| QoS Classification | Interface: | | - | | | | |
| Routing | | | | | | | |
| DNS | | | | Apply/Save | | | |

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

Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

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

6.3.2 QoS Classification

The network traffic classes are listed in the following table.



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: | Enable 👻 | | |
| Specify Classification Criteria (A blank criterion indicates it is not used for cla | ssification.) | | |
| Ingress 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 Egress Interface (Required): | • | | |
| Specify Egress Queue (Required): | • | | |
| Packets classified into a queue that exit through an interface for which the que is not specified to exist, will instead egress to the default queue on the interface. | le | | |
| 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 (Class vlan packets egress to a non-vlan interface will have the packet p-bits re- Class non-vlan packets egress to a vlan interface will be tagged with the interfa Class vlan packets egress to a vlan interface will be additionally tagged with the | marked by the class rule p-bits. No additional vlan tag is added. ce VID and the class rule p-bits. | | |
| Set Rate Limit: | [Kbits/s] | | |
| Apply/Save |] | | |

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 | |
| Ingress Interface | Select an interface (i.e. Local, eth0-4, wan) |
| 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. |

| Field | Description |
|---|--|
| Destination MAC Mask | This is the mask used to decide how many bits are checked in Destination MAC Address. |
| Classification Results | |
| Specify Egress Interface | Choose the egress interface from the available list. |
| Specify Egress Queue | Choose the egress queue from the list of available for the specified egress interface. |
| 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. 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 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 | 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** and **RIP**.

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.

| COM | REND Device Info Basi | ic Setup Advanced Setup | Diagnostics M | anagement Logout |
|--|--|---|--------------------------|------------------|
| Auto-Detection | Routing Default Gateway | | | |
| Security Quality of Service Routing | Default gateway interface list can have n according to the priority with the first by Priority order can be changed by remov | eing the highest and the last one the lov | vest priority if the WAN | |
| Default Gateway Static Route | Selected Default Gateway Interfaces | Available Routed WA Interfaces | N | |
| Policy Routing RIP DNS DSL | ۸ ۲- | | | |
| Interface Grouping IP Tunnel Certificate | ₹ | | | |
| Power Management Multicast | | Ŧ | | |
| | TODO: IPV6 ********** Select a pre | | ult IPv6 gateway. | |
| | Selected WAN Interface NO CONFIG | Apply/Save | | |



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.

| COM | Image: Construction of the second | Logout |
|--------------------------------|--|--------|
| Auto-Detection | Routing Static Route (A maximum 32 entries can be configured) NOTE: For system created route, the 'Remove' checkbox is disabled. | |
| Security Quality of Service | IP Version DstIP/ PrefixLength Gateway Interface metric Remove | |
| Routing Default Gateway | Add Remove | |
| Static Route Policy Routing | | |
| RIP | | |

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

| COM | REND Device Info Basic S | Setup Advan | nced Setup | G Diagnostics | Management | Logout |
|--------------------|--|---------------------|------------------|-------------------------|-------------------------|--------|
| Auto-Detection | Routing Static Route Add | | | | | |
| Security | Enter the destination network address, subnet the entry to the routing table. | et mask, gateway | AND/OR available | WAN interface the | n click "Apply/Save" to |) add |
| Quality of Service | the entry to the routing table. | | | | | |
| Routing | IP Version: | | IPv4 | • | | |
| Default Gateway | Destination IP address/prefix length: | | | | | |
| Static Route | Interface: | | | - | | |
| Policy Routing | Gateway IP Address: | | | | | |
| RIP | (optional: metric number should be greater t | than or equal to ze | ero) | | | |
| DNS | Metric: | An | ply/Save | | | |
| DSL | | App | руураче | | | |

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

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

6.4.3 Policy Routing

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

| COM | REND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--------------------|----------------|----------------|-------------------|-------------------|-------------------|------------|--------|
| Auto-Detection | Policy Routing | g Setting A ma | ximum 7 entries o | an be configured. | | | |
| Security | | | | | | | |
| Quality of Service | | Polie | cy Name Source | IP LAN Port WAN | Default GW Remove | e | |
| Routing | | | | Add Remove | | | |
| Default Gateway | | | | Kenove | | | |
| Static Route | | | | | | | |
| Policy Routing | | | | | | | |
| RIP | | | | | | | |

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

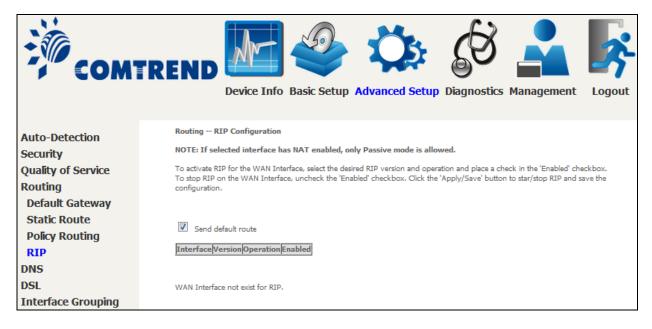
| COM | | Logout |
|--|---|--------|
| Auto-Detection Security Quality of Service | Policy Routing Settup Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table. Note: If selected "IPOE" as WAN interface, default gateway must be configured. | |
| Routing Default Gateway Static Route | Policy Name: Physical LAN Port: | |
| Policy Routing RIP DNS | Source IP: | |
| DSL Interface Grouping IP Tunnel | Default Gateway IP: Apply/Save | |

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



6.4.4 RIP

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



6.5 DNS

6.5.1 DNS Server

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

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

| COMI | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|---|--|
| Auto-Detection Security Quality of Service Routing DNS DNS Server Dynamic DNS DNS Entries DNS Proxy/Relay DSL Interface Grouping IP Tunnel Certificate Power Management Multicast | DIS Server Configuration Sets DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM for do, if only a single PVC with IPoA or static IPOE protocol is configured, Static DNS server IP addresses must be entered. Dis Server Interfaces can have multiple WAN interfaces served as system dons servers but only one will be used according to the protocol is configured. Dis Server IP addresses must be entered. Dis Server Interfaces can have multiple WAN interfaces served as system dons servers but only one will be used according to the protocol is configured. Dis Server IP addresses must be entered. Dis Server Interfaces to the used according to the used according to the protocol is configured. Dis Server IP addresses must be entered. Dis Server Interfaces to the used according to the used according to the protocol is configured. Dis Server IP addresses must be entered. Dis Server IP addresses Sected DNS Server Interface Satiable WAN Interfaces Sected DNS Server Interface Satiable WAN Interfaces |
| | Secondary DNS server: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface. Obtain IPv6 DNS info from a WAN interface: WAN Interface selected: NO CONFIGURED INTERFACE WAN Interface selected: NO CONFIGURED INTERFACE Secondary IPv6 DNS server: Apply/Save |

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

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



6.5.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the AR-5230 to be more easily accessed from various locations on the Internet.



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

| COMI | | Basic Setup A | Advanced Setup | Diagnostics | Management | Logout |
|--------------------|---------------------------------|------------------------|---------------------|-----------------------|---------------------------|----------|
| Auto-Detection | Add Dynamic DNS | | | | | |
| Security | This page allows you to add a D | unamic DNS addross for | Durp DNE org. TZQ | or no-in com Additic | and within possible to a | onfiguro |
| Quality of Service | a Custom Dynamic DNS service. | | 5m 5yn543.0rg, 120, | or no-ipiconii Addide | many, it is possible to t | onigure |
| Routing | D-DNS provider | DynDNS.org | g 👻 | | | |
| DNS | | | | | | |
| DNS Server | Hostname | | | | | |
| Dynamic DNS | Interface | • | | | | |
| DNS Entries | DynDNS Settings | | | | | |
| | Username | | | | | |
| DNS Proxy/Relay | Password | | | | | |
| DSL | | | | | | |
| Interface Grouping | | | | | | |
| IP Tunnel | | | | | | |
| Certificate | | | | | | |
| Power Management | | | Apply/Save | | | |
| Multicast | | | | | | |

Click **Apply/Save** to save your settings.

Consult the table below for field descriptions.

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



6.5.3 DNS Entries

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

| COM | Image: Construction of the second | Logout |
|---|--|--------|
| Auto-Detection Security Quality of Service Routing DNS DNS Server Dynamic DNS DNS Entries DNS Proxy/Relay | DNS Entries The DNS Entry page allows you to add domain name and IP address pairs desired to be resolved by the DSL router. Choose or Remove to configure DNS Entry. The entries will become active after save/reboot. A maximum 16 entries can be configured. Domain Name IP Address Remove Add Remove | Add |

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

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|--|---|--------|
| Auto-Detection Security Quality of Service Routing | DNS Entry Enter the domain name and IP address that needs to be resolved locally, and click 'Add Entry.' Domain Name IP Address | |
| DNS DNS Server Dynamic DNS DNS Entries DNS Proxy/Relay | Add Entry | |

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



6.5.4 DNS Proxy/Relay

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

| COMI | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logo | ut |
|--------------------------------|--|----|
| Auto-Detection | DNS Proxy Configuration | |
| Security Quality of Service | Enable DNS Proxy | |
| Routing | Host name of the Broadband Router: Comtrend | |
| DNS | Domain name of the LAN network: Home | |
| DNS Server | | |
| Dynamic DNS | DNS Relay Configuration This controls the DHCP Server to assign public DNS. | |
| DNS Entries | Enable DNS Relay | |
| DNS Proxy/Relay | Apply/Save | |



6.6 DSL

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

| COM | REEND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|--------------------|--|--------|
| Auto-Detection | DSL Settings | |
| Security | Select the modulation below. | |
| Quality of Service | G.Dmt Enabled | |
| Routing | G.lite Enabled | |
| DNS | T1.413 Enabled | |
| DSL | ADSL2 Enabled | |
| Interface Grouping | AnnexL Enabled | |
| IP Tunnel | | |
| Certificate | ADSL2+ Enabled | |
| Power Management | AnnexM Enabled | |
| Multicast | Capability | |
| | ☑ Bitswap Enable | |
| | SRA Enable | |
| | G.997.1 EOC xTU-R Serial Number | |
| | Equipment Serial Number | |
| | Equipment MAC Address | |
| | Apply/Save | |

| DSL Mode | Data Transmission Rate - Mbps (Megabits per second) | | | | |
|-----------------------------------|---|--|--|--|--|
| G.Dmt | Downstream: 12 Mbps Upstream: 1.3 Mbps | | | | |
| G.lite | Downstream: 4 Mbps Upstream: 0.5 Mbps | | | | |
| T1.413 | Downstream: 8 Mbps Upstream: 1.0 Mbps | | | | |
| ADSL2 | Downstream: 12 Mbps Upstream: 1.0 Mbps | | | | |
| AnnexL | Supports longer loops but with reduced transmission rates | | | | |
| ADSL2+ | Downstream: 24 Mbps Upstream: 1.0 Mbps | | | | |
| AnnexM | Downstream: 24 Mbps Upstream: 3.5 Mbps | | | | |
| Options | Description | | | | |
| Bitswap Enable | Enables adaptive handshaking functionality | | | | |
| SRA Enable | Enables Seamless Rate Adaptation (SRA) | | | | |
| G997.1 EOC xTU-R Serial Number | Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages | | | | |

6.7 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.

The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

| COMT | RE | | | nfo Basic Se | etup Advanc | ed Setup Diag | Juostics Management | Logout |
|--|-------------|--------------------------------------|---------------------------|---|-------------------|---|--|--------|
| Auto-Detection Security Quality of Service Routing DNS | 1 5 1 | Interface Group support this feat | ing suppor ture, you m | ts multiple ports to just create mapping | groups with appro | roups. Each group w priate LAN and WAN | vill perform as an independent ne interfaces using the Add button. ault group. Only the default grow | The |
| DSL | | Group Name | Remove | WAN Interface | LAN Interfaces | DHCP Vendor IDs | | |
| Interface Grouping | | | | | ETH1 | | | |
| IP Tunnel | | Default | | | ETH2 | | | |
| Certificate | | Derault | | | ETH3 | | _ | |
| Power Management | | | | | ETH4 | | | |
| Multicast | | Add Rer | move | | | | | |

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

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|--|---|
| Auto-Detection Security Quality of Service Routing DNS DSL Interface Grouping IP Tunnel Certificate Power Management Multicast | Interface grouping Configuration To create a new interface group: 1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below: 2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string, By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server. 3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses 4. Click Apply/Save button to make the changes effective immediately IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address. |
| | Grouped WAN Interfaces Grouped WAN Interfaces Available WAN Interfaces |
| | Grouped LAN Interfaces Available LAN Interfaces ETH1 ETH2 ETH3 ETH4 <-> ETH4 - |
| | Automatically Add Clients With the following DHCP Vendor IDs |

Automatically Add Clients With Following DHCP Vendor IDs:

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

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ETH1, ETH2, ETH3, and ETH4.

The Interface Grouping configuration will be:



1. Default: ETH1, ETH2, ETH3, and ETH4.

2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

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

If a set-top box is connected to ETH1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ETH2, ETH3, and ETH4

2. Video: nas_0_36, nas_0_37, nas_0_38, and ETH1



6.8 IP Tunnel

6.8.1 IPv6inIPv4

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

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|--------------------|--|--------|
| Auto-Detection | IP Tunneling 6in4 Tunnel Configuration | |
| Security | Name WAN LAN Dynamic IPv4 Mask Length 6rd Prefix Border Relay Address Remove | |
| Quality of Service | | |
| Routing | Add Remove | |
| DNS | | |
| DSL | | |
| Interface Grouping | | |
| IP Tunnel | | |
| IPv6inIPv4 | | |
| IPv4inIPv6 | | |

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

| COM | REND Device Info Basic S | Setup Advanced S | Setup Diagnostic | s Management | Logout |
|---------------------------------|--|------------------|------------------|--------------|--------|
| Auto-Detection Security | IP Tunneling 6in4 Tunnel Configuration | | | | |
| Quality of Service | Tunnel Name | | | | |
| Routing DNS | Mechanism: Associated WAN Interface: | 6RD | | • • | |
| DSL Interface Grouping | Associated LAN Interface: Manual Manual | LAN/ | br0 👻 | | |
| IP Tunnel | IPv4 Mask Length: | | | | |
| IPv6inIPv4 IPv4inIPv6 | 6rd Prefix with Prefix Length: Border Relay IPv4 Address: | | | | |
| Certificate Power Management | | Apply/Save | | | |

Consult the table below for field descriptions.

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



6.8.2 IPv4inIPv6

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

| COM | Image: Construction of the second | gout |
|--|--|------|
| Auto-Detection Security Quality of Service Routing DNS DSL Interface Grouping IP Tunnel IPv6inIPv4 IPv4inIPv6 | IP Tunneling 4in6 Tunnel Configuration Name WAN LAN Dynamic AFTR Remove Add Remove | |

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

| COM | REND Device Info | Basic Setup Ad | Ivanced Setup | Diagnostics | Management | Logout |
|--------------------|--------------------------------------|-----------------|---------------|-------------|------------|--------|
| Auto-Detection | IP Tunneling 4in6 Tunnel Co | nfiguration | | | | |
| Security | Currently, only DS-Lite configuratio | n is supported. | | | | |
| Quality of Service | Tunnel Name | | | | | |
| Routing | Mechanism: | | DS-Lite | | - | |
| DNS | Associated WAN Interface: | | | | • | |
| DSL | Associated LAN Interface: | | LAN/br0 - | | | |
| Interface Grouping | Manual Automatic | | | | | |
| IP Tunnel | AFTR: | | | | | |
| IPv6inIPv4 | | | Apply/Save | | | |
| IPv4inIPv6 | | | | | | |

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



6.9 Certificate

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

6.9.1 Local

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|--|---|--------|
| Auto-Detection Security Quality of Service Routing DNS DSL Interface Grouping IP Tunnel Certificate Local Trusted CA | Local Certificates Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored. Name In Use Subject Type Action Create Certificate Request Import Certificate | |

CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.



| COM | TREND Device Info E | asic Setup Advance | ed Setup Diagnostics | s Management | Logout |
|---------------------|--|-------------------------------|---------------------------------|--------------------------|-------------|
| Auto-Detection | Create new certificate request | | | | |
| Security | To generate a certificate signing requ | uest you need to include Comm | on Name, Organization Name, Sta | ate/Province Name, and t | he 2-letter |
| Quality of Service | Country Code for the certificate. | | | | |
| Routing | Certificate Name: | | | | |
| DNS | Common Name: | | | | |
| DSL | Organization Name: State/Province Name: | | | | |
| Interface Grouping | Country/Region Name: | US (United States) | | - | |
| IP Tunnel | | oo (oniced otaces) | | • | |
| Certificate | | | | | |
| | | Ap | pply | | |
| Local Trusted CA | | | | | |

The following table is provided for your reference.

| Field | Description |
|---------------------|---|
| Certificate Name | A user-defined name for the certificate. |
| Common Name | Usually, the fully qualified domain name for the machine. |
| Organization Name | The exact legal name of your organization. Do not abbreviate. |
| State/Province Name | The state or province where your organization is located. It cannot be abbreviated. |
| Country/Region Name | The two-letter ISO abbreviation for your country. |



IMPORT CERTIFICATE

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

| COM | TREND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--|--|---|---|----------------|-------------|------------|--------|
| Auto-Detection Security Quality of Service Routing DNS DSL Interface Grouping IP Tunnel Certificate Local | Import certificate Enter certificate name, Certificate Name: Certificate: | <insert< th=""><th>IN CERTIFICATE- certificate her CERTIFICATE</th><th>e></th><th></th><th></th><th></th></insert<> | IN CERTIFICATE- certificate her CERTIFICATE | e> | | | |
| Trusted CA Power Management Multicast | Private Key: | <insert< th=""><th>IN RSA PRIVATE 1 private key her RSA PRIVATE KE</th><th>e></th><th>Apply</th><th>њ. њ</th><th></th></insert<> | IN RSA PRIVATE 1 private key her RSA PRIVATE KE | e> | Apply | њ. њ | |

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



6.9.2 Trusted CA

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

| COM | TREND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|---|--|--------|
| Auto-Detection Security Quality of Service Routing | Name Subject Type Action | |
| DNS DSL Interface Grouping IP Tunnel Certificate Local Trusted CA | [Import Certificate | |

Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.

| COM | TREND | Device Info | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--------------------|---------------------|---|-------------|----------------|-------------|------------|--------|
| Auto-Detection | Import CA certi | ficate | | | | | |
| Security | Enter certificate n | ame and paste certificate c | ontent. | | | | |
| Quality of Service | Certificate Name: | | | | | | |
| Routing | | | TIFICATE | | | | |
| DNS | | <insert certif<="" th=""><th></th><th></th><th></th><th></th><th></th></insert> | | | | | |
| DSL | | END CERTI | FICATE | | | | |
| Interface Grouping | | | | | | | |
| IP Tunnel | Certificate: | | | | | | |
| Certificate | Certificate: | | | | | | |
| Local | | | | | | | |
| Trusted CA | | | | | | | |
| Power Management | | | | | | | |
| Multicast | | | | Apply | | | |

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

6.10 Power Management

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

| COM | | gout |
|--------------------|---|------|
| Auto-Detection | Power Management | |
| Security | This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response. | |
| Quality of Service | | |
| Routing | | |
| DNS | Wait instruction when Idle Image: status: Enable Status: Enabled | |
| DSL | Enable Status: Enabled | |
| Interface Grouping | | |
| IP Tunnel | Energy Efficient Ethernet | |
| Certificate | Enable Status: Enabled | |
| Power Management | | |
| Multicast | Ethernet Auto Power Down and Sleep | |
| | Enable Status: Enabled | |
| | Apply refresh | |

6.11 Multicast

Input new IGMP or MLD protocol configuration fields if you want modify default values shown. Then click **Apply/Save**.

| COMI | REND Device Info Ba | sic Setup Advanced Setup Diagnostics Management Logout |
|--|--|--|
| Auto-Detection Security Quality of Service | Multicast Precedence: Multicast Strict Grouping Enforcement: | Disable Violation lower value, higher priority Disable Violation |
| Routing DNS DSI | IGMP Configuration Enter IGMP protocol configuration fie | lds if you want modify default values shown below. |
| Interface Grouping IP Tunnel | Default Version : Query Interval: Query Response Interval: | 3 125 10 |
| Certificate Power Management Multicast | Last Member Query Interval: Robustness Value: Maximum Multicast Groups: | 10 2 25 |
| Mulucast | Maximum Multicast Data Sources (for IGMPv3): Maximum Multicast Group Members: | 10 |
| | Fast Leave Enable: MLD Configuration Enter MLD protocol (IPv6 Multicast) c | onfiguration fields if you want modify default values shown below. |
| | Default Version : Query Interval: Query Response Interval: | 2 125 10 |
| | Last Member Query Interval: Robustness Value: Maximum Multicast Groups: Maximum Multicast Data Sources (for | 10 2 10 10 |
| | mldv2): Maximum Multicast Group Members: Fast Leave Enable: | |

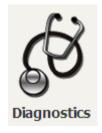
Multicast Precedence: Select precedence of multicast packets.

Multicast Strict Grouping Enforcement: Enable/Disable multicast strict grouping.

| Field | Description |
|-----------------|---|
| Default Version | Define IGMP using version with video server. |
| Query Interval | The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds. |

| Field | Description | | | |
|--|---|--|--|--|
| Query Response Interval | The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval. | | | |
| Last Member Query Interval | The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 10 seconds. | | | |
| Robustness Value | The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2. | | | |
| Maximum Multicast Groups | Setting the maximum number of Multicast groups. | | | |
| Maximum Multicast Data Sources (for IGMPv3) | Define the maximum multicast video stream number. | | | |
| Maximum Multicast Group Members | Setting the maximum number of groups that ports can accept. | | | |
| Fast Leave Enable | When you enable IGMP fast-leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. | | | |

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

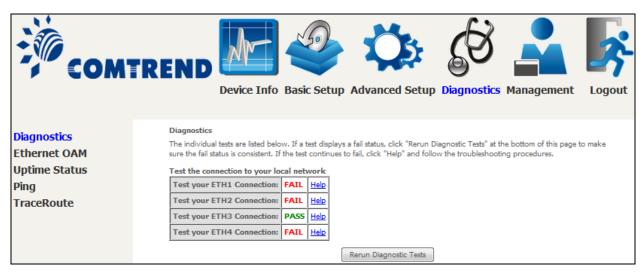


7.1 Diagnostics – Individual Tests

The first Diagnostics screen is a dashboard that shows overall connection status.

| COM | REND Device | Info Basic Setu | p Advan | ced Setup Diagno | Stics Management | Logout |
|-----------------------------|-------------------------------------|--------------------------------|---------|-----------------------------|-----------------------------|--------|
| Diagnostics Ethernet OAM | | LAN | | | Device | |
| Uptime Status | | | | Model | AR-5230 | |
| Ping | ETH1 E | ETH2 ETH3 | ETH4 | Serial Number | 1635230UXXF-AA000102 | |
| TraceRoute | | | | Firmware Version | EE31-416CTU-C01_R01.A2pG039 | u.d26j |
| | LAN IPv4 Address LAN Subnet Mask | 192.168.1.1 255.255.255.0 | | Bootloader (CFE) Version | 1.0.38-116.228-1 | |
| | LAN MAC Address | d8:b6:b7:ab:27:a8 | | Up Time | 4 mins:43 secs | |
| | DHCP Server | Enabled | | System Log | Show | |
| | DHCP IP Range | 192.168.1.2 - 192.168.1.254 | | 1 | | |

Click the Diagnostics Menu item on the left side of the screen to display the individual connections.



97 Leading the Communication Trend



7.2 Ethernet OAM

The Ethernet OAM page provides settings to enable/disable 802.3ah, 802.1ag/Y1.731 OAM protocols.

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|-------------------------------------|---|--------|
| Diagnostics Ethernet OAM | Ethernet Link OAM (802.3ah) | |
| Uptime Status Ping TraceRoute | Ethernet Service OAM (802.1ag / V.1731) Enabled 802.1ag Y.1731 Apply/Save | |

To enable Ethernet Link OAM (802.3 ah), click Enabled to display the full configuration list. At least one option must be enabled for 802.1ah.

| Ethernet Link OAM (802.3ah) | | | |
|-----------------------------|--------------------|---|--------------------|
| 1 | Enabled | | |
| | WAN Interface: | - | |
| | OAM ID: | 1 | (positive integer) |
| | Auto Event | | |
| | Variable Retrieval | | |
| | Link Events | | |
| | Remote Loopback | | |
| | Active Mode | | |

| WAN Interface | Select layer 2 WAN interface for outgoing OAM packets |
|--------------------|---|
| OAM ID | OAM Identification number |
| Auto Event | Supports OAM auto event |
| Variable Retrieval | Supports OAM variable retrieval |
| Link Events | Supports OAM link events |
| Remote Loopback | Supports OAM remove loopback |
| Active mode | Supports OAM active mode |



To enable Ethernet Service OAM (802.1ag/Y1731), click Enabled to display the full configuration list.

| Ethernet Service OAM (802.1ag / Y.1731) | | | | | |
|---|-----------|-------------------------------|--------|--------------|------------------|
| V Enabled (0) 802.1ag (0) Y.1731 | | | | | |
| WAN Interface: | • | | | | |
| MD Level: | 0 🔻 [0-7] | | | | |
| MD Name: | Broadcom | [e.g. Broadcom] | | | |
| MA ID: | BRCM | [e.g. BRCM] | | | |
| Local MEP ID: | 1 | [1-8191] | | | |
| Local MEP VLAN ID: | -1 | [1-4094] (-1 means no VLAN ta | g) | | |
| CCM Transmission | | | | | |
| Remote MEP ID: | -1 | [1-8191] (-1 means no Remote | MEP) | | |
| Loopback and Linktrace T | est | | | | |
| Target MAC: | | [e.g. 02:10:18:aa:bb:cc] | | | |
| Linktrace TTL: | -1 | [1-255] (-1 means no max hop | limit) | | |
| Loopback Result: | N/A | | | | |
| Linktrace Result: | N/A | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | Send Loopbac | k Send Linktrace |

| WAN Interface | Select from the list of WAN Interfaces to send OAM packets |
|-------------------|--|
| MD Level | Maintenance Domain Level |
| MD Name | Maintenance Domain name |
| MA ID | Maintenance Association Identifier |
| Local MEP ID | Local Maintenance association End Point Identifier |
| Local MEP VLAN ID | VLAN IP used for Local Maintenance End point |

Click CCM Transmission to enable CPE sending Continuity Check Message (CCM) continuously.

| Remote MEP ID | Maintenance association End Point Identifier for the remote receiver |
|---------------|--|
|---------------|--|

To perform Loopback/Linktrace OAM test, enter the Target MAC of the destination and click "Send Loopback" or "Send Linktrace" button.

| Target MAC | MAC Address of the destination to send OAM loopback/linktrace packet |
|---------------|--|
| Linktrace TTL | Time to Live value for the loopback/linktrace packet |



7.3 Uptime Status

This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer.

| COM | Image: Construction of the second setup Image: Construction of the second s |
|---|---|
| Diagnostics Ethernet OAM <mark>Uptime Status</mark> Ping TraceRoute | Uptime Status This page shows System, DSL, ETH and Layer 3 uptime. If the DSL line, ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the DSL or ETH timer. The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down. System Up Time 8 mins:8 secs |
| | DSL Group: DSL Up Time Not Connected ClearAll |

The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.



7.4 Ping

Input the IP address/hostname and click the **Ping** button to execute ping diagnostic test to send the ICMP request to the specified host.

| COM | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|--------------------|--|
| Diagnostics | Ping |
| Ethernet OAM | Send ICMP ECHO_REQUEST packets to network hosts. |
| Uptime Status | Ping IP Address / Hostname: Ping |
| Ping TraceRoute | PING 192.168.1.1 (192.168.1.1): 56 data bytes 64 bytes from 192.168.1.1: seq=0 tH=64 time=0.948 ms 64 bytes from 192.168.1.1: seq=1 tH=64 time=0.579 ms 64 bytes from 192.168.1.1: seq=2 tH=64 time=0.492 ms 64 bytes from 192.168.1.1: seq=3 tH=64 time=0.493 ms 192.168.1.1 ping statistics 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.492/0.628/0.948 ms |

7.5 Trace Route

Input the IP address/hostname and click the **TraceRoute** button to execute the trace route diagnostic test to send the ICMP packets to the specified host.

| COM | REND Wice Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|---------------|---|--------|
| Diagnostics | TraceRoute | |
| Ethernet OAM | Trace the route ip packets follow going to "host". | |
| Uptime Status | TraceRoute IP Address / Hostname: | |
| Ping | traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets | |
| TraceRoute | 1 192.168.1.1 (192.168.1.1) 0.754 ms | |

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



The Management menu has the following maintenance functions and processes:

8.1 Settings

This includes Backup Settings, Update Settings, and Restore Default screens.

8.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.

| COMI | TREND Revice Info Basic Setup Advanced Setup Diagnostics Management | Logout |
|---|---|--------|
| Settings Backup Update Restore Default System Log SNMP Agent TR-069 Client Internet Time Access Control Wake-on-LAN Update Software Reboot | Settings - Backup Backup Broadband Router configurations. You may save your router configurations to a file on your PC. Backup Settings | |



8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Press **Browse...** to search for the file, or enter the file name (including folder path) in the **Settings File Name** box, and then click **Update Settings** to recover settings.

| COM | Image: Setup Advanced Setup Diagnostics Image: Setup Advanced Setup Advanced Setup Diagnostics Image: Setup Advanced Setup Advanced Setup Diagnostics Image: Setup Advanced Advanced Setup Advanced Setup Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanc | gout |
|---|---|------|
| Settings Backup Update Restore Default System Log SNMP Agent TR-069 Client Internet Time | Tools Update Settings Update Broadband Router settings. You may update your router settings using your saved files. Settings File Name: Browse Update Settings | |
| Access Control Wake-on-LAN Update Software Reboot | | |

8.1.3 Restore Default

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

| COM | Image: Construction of the second | Logout |
|---|--|--------|
| Settings Backup Update Restore Default System Log SNMP Agent TR-069 Client Internet Time Access Control Wake-on-LAN Update Software Reboot | Tools Restore Default Settings Restore Broadband Router settings to the factory defaults. Restore Default Settings | |

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

Broadband Router Restore

The Broadband Router configuration has been restored to default settings and the router is rebooting.

Close the Broadband Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

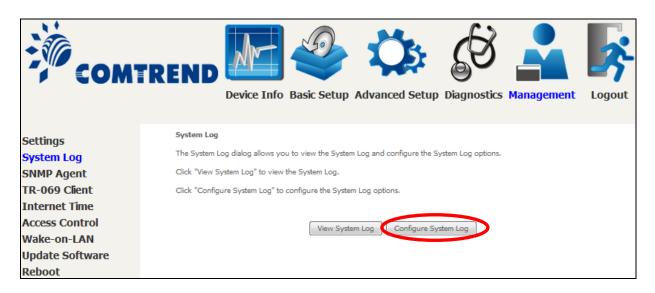
NOTE: This entry has the same effect as the **Reset** button. The AR-5230 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the boot loader will erase the configuration data saved in flash memory.

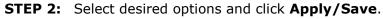
8.2 System Log

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

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

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





| COMI | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout | | | | | |
|--|---|--|--|--|--|--|
| Settings System Log SNMP Agent TR-069 Client Internet Time | System Log Configuration If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory. Select the desired values and click 'Apply/Save' to configure the system log options. | | | | | |
| Access Control Wake-on-LAN Update Software Reboot | Log: O Disable C Enable Log Level: Debugging V Display Level: Error V Mode: Local V | | | | | |

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

| Option | Description |
|--------|--|
| Log | Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the Enable radio button and then click Apply/Save . |

| Option | Description | | |
|------------------|---|--|--|
| Log Level | Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the AR-5230 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. | | |
| | The log levels are defined as follows: | | |
| | Emergency = system is unusable Alert = action must be taken immediately Critical = critical conditions Error = Error conditions Warning = normal but significant condition Notice= normal but insignificant condition Informational= provides information for reference Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged. | | |
| Display Level | Allows the user to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level. | | |
| Mode | Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port. | | |

STEP 3: Click **View System Log**. The results are displayed as follows.

| System Log | | | | | | |
|----------------|----------|----------|---|--|--|--|
| Date/Time | Facility | Severity | Message | | | |
| Jan 1 00:00:12 | syslog | emerg | BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0000) | | | |
| Jan 1 00:00:17 | user | crit | klogd: USB Link UP. | | | |
| Jan 1 00:00:19 | user | crit | klogd: eth0 Link UP. | | | |
| Refresh Close | | | | | | |

8.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options, and click **Save/Apply** to activate SNMP.

| COM | | fo Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|-----------------|---|-------------------------|----------------------------|------------------------|------------------------|--------|
| Settings | SNMP - Configuration | | | | | |
| System Log | Simple Network Managemen agent in this device. | t Protocol (SNMP) allow | s a management application | to retrieve statistics | and status from the SN | IMP |
| SNMP Agent | 2 | | the CNMD and and | | | |
| TR-069 Client | Select the desired values and | Click Apply to config | ure the SIVMP options. | | | |
| Internet Time | SNMP Agent O Disabl | e 🔘 Enable | | | | |
| Access Control | Read Community: | public | | | | |
| Wake-on-LAN | Set Community: | private | | | | |
| Update Software | System Name: | Comtrend | | | | |
| Reboot | System Location: | unknown | | | | |
| neboot | System Contact: | unknown | | | | |
| | Trap Manager IP: | 0.0.0.0 | | | | |
| | | | Save/Apply | | | |



8.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.

| COM | REND Device Info Basic Se | etup Advanced Setup Diagnostics Management |
|-----------------------------|--|---|
| Settings | TR-069 client - Configuration | |
| System Log | WAN Management Protocol (TR-069) allows a collection, and diagnostics to this device. | Auto-Configuration Server (ACS) to perform auto-configuration, provision, |
| SNMP Agent TR-069 Client | Select the desired values and click "Apply/Sav | re" to configure the TR-069 client options. |
| Internet Time | Enable TR-069 | |
| Access Control | OUI-serial | MAC Serialnumber |
| Wake-on-LAN | Inform | Disable Denable |
| Update Software | Inform Interval: | 300 |
| Reboot | ACS URL: | |
| | ACS User Name: | admin |
| | ACS Password: | 00000 |
| | WAN Interface used by TR-069 client: | Any_WAN - |
| | Connection Request Authentication | |
| | Connection Request User Name: | admin |
| | Connection Request Password: | ***** |
| | Connection Request URL: | |
| | | Apply/Save Send Inform |

The table below is provided for ease of reference.

| Option | Description |
|-----------------|--|
| Enable TR-069 | Tick the checkbox ☑ to enable. |
| OUI-serial | The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with ACS or select serial number to use router's serial number. |
| Inform | Disable/Enable TR-069 client on the CPE. |
| Inform Interval | The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method. |
| ACS URL | URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication. |
| ACS User Name | Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE. |

| Option | Description | | |
|-------------------------------------|---|--|--|
| ACS Password | Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE. | | |
| WAN Interface used by TR-069 client | Choose Any_WAN, LAN, Loopback or a configured connection. | | |
| Connection Request | | | |
| Authentication | Tick the checkbox $ earrow$ to enable. | | |
| User Name | Username used to authenticate an ACS making a Connection Request to the CPE. | | |
| Password | Password used to authenticate an ACS making a Connection Request to the CPE. | | |
| URL | IP address and port the ACS uses to connect to router. | | |

The **Send Inform** button forces the CPE to establish an immediate connection to the ACS.



8.5 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox \Box , choose your preferred time server(s), select the correct time zone offset, and click **Save/Apply**.

| COMI | | Basic Setup | Advanced Setup | Diagnostics | Management | Logout |
|--------------------------------|---|---------------------------------|---------------------|-------------|------------|--------|
| Settings System Log | Time settings This page allows you to the mo | dem's time configuration | n. | | | |
| SNMP Agent | Automatically synchronize | with Internet time serv | ers | | | |
| TR-069 Client Internet Time | First NTP time server: Second NTP time server: | time.nist.gov ntp1.tummy.com | • n • | | | |
| Access Control Wake-on-LAN | Third NTP time server: | None | - | | | |
| Update Software | Fourth NTP time server: Fifth NTP time server: | None None | • • | | | |
| Reboot | Time zone offset: | (GMT-08:00) Pa | cific Time, Tijuana | | | • |
| | | | Apply/Save | | | |

NOTE: Internet Time must be activated to use Parental Control. In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

8.6 Access Control

8.6.1 Accounts

This screen is used to configure the user account access passwords for the device. Access to the AR-5230 is controlled through the following user accounts:

- The root account has unrestricted access to view and change the configuration of your Broadband router.
- The support account is typically utilized by Carrier/ISP technicians for maintenance and diagnostics.
- The user account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure certain settings.
- The apuser account is typically utilized by End-Users to view configuration settings and statistics, with limited ability to configure settings.

Use the fields to update passwords for the accounts, add/remove accounts (max of 5 accounts) as well as adjust their specific privileges.

| COMI | | | | • 4 | | B | | \$ |
|-----------------------------|---|----------------|-------------------|-----------------|-------------------|----------------------------|--------------------------|-----------|
| | Access Control Acc | | | up Auvai | iceu Secuj |) Diagnostics | management | Logout |
| Settings | By default, access to yo | | | ontrolled throu | gh three user a | ccounts: root,support | ,and user. | |
| System Log | The root account has u | nrestricted | access to view | and change th | e configuration | of your Broadband r | router. | |
| SNMP Agent TR-069 Client | The support account is | typically ut | tilized by Carrie | r/ISP technicia | ins for mainten | ance and diagnostics. | | |
| Internet Time | The user account is typ | ically utilize | d by End-User | s to view confi | guration setting | s and statistics, with lin | mited ability to configu | re |
| Access Control | certain settings. | | | | | | | |
| Accounts | Use the fields below to u as long as 16 characters | | | | remove accou | nts (max of 5 accounts | ;). Note: Passwords ma | iy be |
| Services | - | | iot contain a s | | | | | |
| IP Address | Select an account Create an account | | | | • | | | |
| Wake-on-LAN | _ | | | | | | | |
| Update Software | Old Password: | | | | | | | |
| Reboot | Confirm Password: | | | | | | | |
| | | | | | | | | |
| | Save/Apply Del | ete | | | | | | _ |
| | Use the fields below to e | nable/disa | ble accounts as | well as adjust | their specific pr | ivileges. | | |
| | Feature | root | support | user | apuser | | | |
| | Account access | Both | None 👻 | None 👻 | None 👻 | | | |
| | Add/Remove WAN | Enabled | V | | | | | |
| | Wireless - Basic | Enabled | | | | | | |
| | Wireless - Advanced | Enabled | V | | | | | |
| | LAN Settings | Enabled | V | V | | | | |
| | LAN Port Mapping | Enabled | V | | | | | |
| | NAT Settings | Enabled | V | V | | | | |
| | Update Software | Enabled | | | | | | |
| | Security | Enabled | | | | | | |
| | Quality of Service | Enabled | | | | | | |
| | Management Settings | Enabled | V | | | | | |
| | Advanced Setup | Enabled | V | | | | | |
| | Home Networking | Enabled | V | | | | | |
| | Parental Control | Enabled | V | V | | | | |
| | Save/Apply | | | | | | | |

Note: Passwords may be as long as 16 characters but must not contain a space. Click **Save/Apply** to continue.



8.6.2 Services

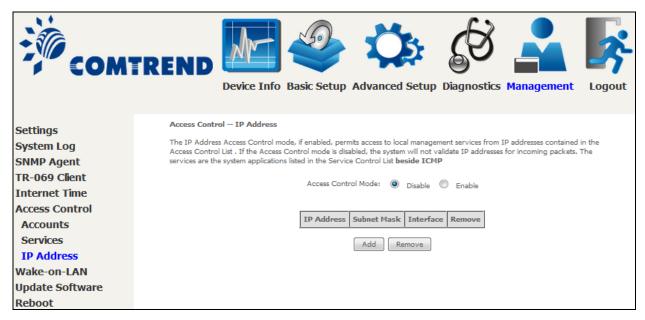
The Services option limits or opens the access services over the LAN or WAN. These access services available are: HTTP, SSH, TELNET, SNMP, HTTPS, FTP, TFTP and ICMP. Enable a service by selecting its dropdown listbox. Click **APPLY/SAVE** to activate.

| COM | REND | Device Info | Basic Setup | Advance | ted Setup Diag | S Juostics | Management | Logout |
|---------------------------------|------|-------------|------------------------|---------------|----------------------|----------------------|------------|--------|
| Settings | | | Service | Access Con | trol Configuration | | | |
| System Log | | S | ielect each listbox ar | d click save/ | apply to configure y | our Setting. | | |
| SNMP Agent | | | Service | Current | New | 1 | | |
| TR-069 Client | | | нттр | Lan | LAN - | | | |
| Internet Time Access Control | | | SSH | Lan | LAN - | - | | |
| Accounts | | | TELNET | | | - | | |
| Services | | | TELNET | Lan | | - | | |
| IP Address | | | SNMP | Disable | Disable 🔻 | _ | | |
| Wake-on-LAN | | | HTTPS | Lan | LAN 🔻 | | | |
| Update Software | | | FTP | Lan | LAN - | | | |
| Reboot | | | TFTP | Lan | LAN - | - | | |
| | | | ICMP | Lan+Wan | LAN+WAN - | | | |
| | | | - | Apply/ | (Save | _ | | |



8.6.3 IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List **beside ICMP**.



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

| COMT | REND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|------------------------|---|
| Settings System Log | Access Control Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.' |
| SNMP Agent | IP Address Subnet Mask Interface |
| TR-069 Client | none 🔻 |
| Internet Time | |
| Access Control | Save/Apply |
| Accounts | |
| Services | |
| IP Address | |
| Wake-on-LAN | |
| Update Software | |
| Reboot | |

Configure the address and subnet of the management station permitted to access the local management services, and click **Save/Apply**.

IP Address – IP address of the management station.

Subnet Mask – Subnet address for the management station.

Interface – Access permission for the specified address, allowing the address to access the local management service from none/lan/wan/lan&wan interfaces.



8.7 Wake-on-LAN

This tool allows you to wake up (power on) computers connected to the Broadband Router LAN interface by sending special "magic packets".

The network interface card in the computer or device that is going to be woken up must support Wake-on-LAN.

| COM | REEND Device Info Basic Setup Advanced Setup Diagnostics Management Logout |
|-----------------|--|
| Settings | Wake-on-LAN |
| System Log | This tool allows you to wake up (power on) computers connected to the Broadband Router LAN interface by sending special "magic |
| SNMP Agent | packets". The network interface card in the computer or device that is going to be woken up must support Wake-on-LAN. |
| TR-069 Client | |
| Internet Time | Enter the device MAC address in the format xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx |
| Access Control | LAN Interface (default br0): br0 |
| Wake-on-LAN | |
| Update Software | MAC Address: |
| Reboot | Send WoL magic packet to the Broadcast address. |
| | Wake Up! |

LAN Interface – Select the LAN interface to send the Wake-on-LAN packet.

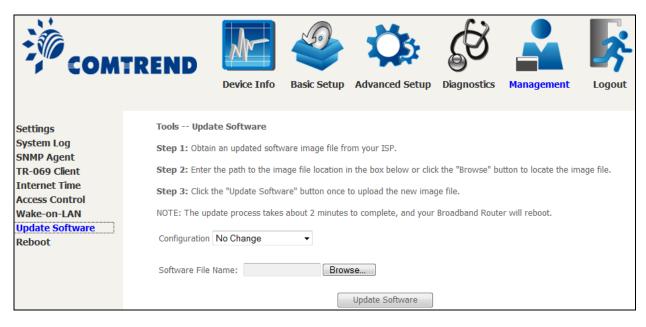
MAC Address – Specify the MAC address of the device that is going to be woken up.

Click **"Send WoL magic packet to the Broadcast address**" if the WoL packets should be sent to the broadcast address.

Click the **Wake Up!** button to send the magic packet out to the LAN interface.

8.8 Update Software

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



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

STEP 2: Select the configuration from the drop-down menu.

Configuration options:

No change - upgrade software directly.

Erase current config – If the router has save_default configuration, this option will erase the current configuration and restore to save_default configuration after software upgrade.

Erase All – Router will be restored to factory default configuration after software upgrade.

- **STEP 3**: Enter the path and filename of the firmware image file in the **Software File Name** field or click the **Browse** button to locate the image file.
- STEP 4: Click the Update Software button once to upload and install the file.
- **NOTE**: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the Device Information screen with the firmware version installed, to confirm the installation was successful.

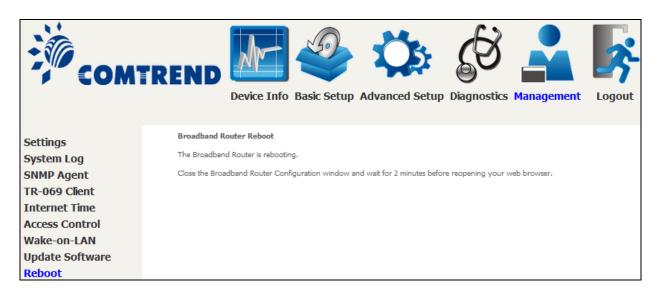


8.9 Reboot

To save the current configuration and reboot the router, click **Reboot**.



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





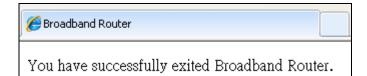
To log out from the device simply click the following icon located at the top of your screen.



When the following window pops up, click the **OK** button to exit the router.



Upon successful exit, the following message will be displayed.



STATEFUL PACKET INSPECTION

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

DENIAL OF SERVICE ATTACK

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

TCP/IP/PORT/INTERFACE FILTER

These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup \rightarrow Security \rightarrow IP Filtering.

OUTGOING IP FILTER

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

| Example 1: | Filter Name | : Out_Filter1 |
|------------|--------------------|-----------------|
| | Protocol | : TCP |
| | Source IP address | : 192.168.1.45 |
| | Source Subnet Mask | : 255.255.255.0 |
| | Source Port | : 80 |
| | Dest. IP Address | : NA |
| | Dest. Subnet Mask | : NA |
| | Dest. Port | : NA |

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

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

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



INCOMING IP FILTER

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

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

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

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

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

MAC LAYER FILTER

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

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

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

| Example 2: | Global Policy | : Blocked |
|------------|--------------------|---------------------|
| | Protocol Type | : PPPoE |
| | Dest. MAC Address | : 00:12:34:56:78:90 |
| | Source MAC Address | : 00:34:12:78:90:56 |
| | Src. Interface | : eth1 |
| | Dest. Interface | : eth2 |
| | | 1 CUIL |

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

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the AR-5230 , as per chosen days of the week and the chosen times.

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

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

Appendix B - Pin Assignments

ETHERNET Ports (RJ45)

ETHERNET LAN Ports (10/100Base-T)

Table 1

| Pin | Definition | Pin | Definition |
|-----|----------------|-----|---------------|
| 1 | Transmit data+ | 5 | NC |
| 2 | Transmit data- | 6 | Receive data- |
| 3 | Receive data+ | 7 | NC |
| 4 | NC | 8 | NC |

DSL Port Table 2

| Pin | Signal definition |
|-----|-------------------|
| 1 | LINE2 TIP |
| 2 | LINE1 TIP |
| 3 | LINE1 RING |
| 4 | LINE2 RING |

Appendix C – Specifications

Hardware Interface

- RJ-11 X 1 for ADSL
- RJ-45 X 4 for LAN (10/100 Base-T auto-sense)
- On/Off Button X 1
- Reset Button X 1
- USB Host X 1

WAN Interface

- Downstream up to 12M for ADSL, 24 Mbps for ADSL2+; Upstream up to 1.3 Mbps,
- ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, Annex A/L/M

LAN Interface

- Standard IEEE 802.3, IEEE 802.3u
- Support MDI/MDX
- 10/100 Base T Auto-sense

Management

- Remote upgrade
- TFTP/FTP upgrade
- Telnet remote access support
- Support Web based configuration
- Support for backup & restore configuration to/from PC

Networking Protocols

- RFC 2684 VC-MUX, LLC/SNAP encapsulations for bridged or routed packet
- RFC 2364 PPP over AAL5
- IPoA, PPPoA, PPPoE, Multiple PPPoE sessions on single PVC, PPPoE pass-through
- PPPoE filtering of on-PPPoE packets between WAN and LAN
- Transparent bridging between all LAN and WAN interfaces
- 802.1p/802.1q VLAN support
- Spanning Tree Algorithm
- IGMP Proxy V1/V2/V3, IGMP Snooping V1/V2/V3, Fast leave
- Static route, RIP v1/v2, ARP, RARP, SNTP
- DHCP Server/Client/Relay,
- DNS Proxy/Relay, Dynamic DNS,
- UPnP IGD v1.0
- IPv6 subset
- DLNA server

Security Functions

- PAP, CHAP, Packet and MAC address filtering, SSH
- Three level login including local admin, local user and remote technical support access



QoS

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

Firewall/Filtering

- Stateful Inspection Firewall
- Stateless Packet Filter
- Denial of Service (DOS): ARP attacks, Ping attacks, Ping of Death, LAND,SYNC, Smurf, Unreachable, Teardrop
- TCP/IP/Port/interface filtering rules Support both incoming and outgoing filtering

NAT/NAPT

- Support Port Triggering and Port forwarding
- Symmetric port-overloading NAT, Full-Cone NAT
- Dynamic NAPT (NAPT N-to-1)
- Support DMZ host
- Virtual Server (Port forwarding)
- VPN Passthrough (PPTP, L2TP, IPSec)

Application Passthrough

SIP, H.323, Yahoo messenger, ICQ, RealPlayer, Net2Phone, NetMeeting, MSN, X-box, Microsoft DirectX gamesetc.

| Power Supply | Input: | 100 - 240 Vac |
|--------------|---------|---------------|
| | Output: | 12V/1A |

Environment Condition

Dimensions......173 mm (W) x 39 mm (H) x 135.8 mm (D)

Certifications..... FCC, IC

Kit Weight

(1*AR-5230, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM)

NOTE: Specifications are subject to change without notice

COMTREND Appendix D - SSH Client

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

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

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

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

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

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

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

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

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

Appendix E - Connection Setup

Creating a WAN connection is a two-stage process.

- **1** Setup a Layer 2 Interface (ATM, PTM or Ethernet).
- **2** Add a WAN connection to the Layer 2 Interface.

The following sections describe each stage in turn.

E1 ~ Layer 2 Interfaces

Every layer2 interface operates in Multi-Service Connection (VLAN MUX) mode, which supports multiple connections over a single interface. Note that PPPoA and IPoA connection types are not supported for Ethernet WAN interfaces. After adding WAN connections to an interface, you must also create an Interface Group to connect LAN/WAN interfaces.

E1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.



STEP 1: Go to Basic Setup → WAN Setup → Select ATM Interface from the drop-down menu.

| COM | TREND Device Info Device Info Device Setup D | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|
| WAN Setup NAT LAN Parental Control | Step 1: Layer 2 Interface Select new interface to add ATM Interface DSL ATM Interface Configuration | | | | | | | | |
| Home Networking | Interface Vpi Vci DSL Latency Category Peak Cell Rate(cells/s) Sustainable Cell Size(bytes) Max Burst Size(bytes) Link Type Conn Mode IP MPAAL Prec/Alg/Wght Remove | | | | | | | | |
| | DSL PTM Interface Configuration Interface DSL Latency PTM Priority Conn Mode IP QoS Remove | | | | | | | | |
| | ETH WAN Interface Configuration Interface/(Name) Connection Mode Remove | | | | | | | | |

This table is provided here for ease of reference.

| Heading | Description | | | | | |
|-----------|--------------------|--|--|--|--|--|
| Interface | WAN interface name | | | | | |
| VPI | ATM VPI (0-255) | | | | | |
| VCI | ATM VCI (32-65535) | | | | | |

| Heading | Description |
|--------------------------|--|
| DSL Latency | ${Path0} \rightarrow portID = 0$ |
| Category | ATM service category |
| Peak Cell Rate | Maximum allowed traffic rate for the ATM PCR service connection |
| Sustainable Cell Rate | The average allowable, long-term cell transfer rate on the VBR service connection |
| Max Burst Size | The maximum allowable burst size of cells that can be transmitted contiguously on the VBR service connection |
| Link Type | Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA. |
| Connection Mode | Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection |
| IP QoS | Quality of Service (QoS) status |
| MPAAL | QoS Scheduler algorithm and queue weight defined for the connection |
| Remove | Select items for removal |

STEP 2: Click **Add** to proceed to the next screen.

NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

| ATM PVC Configuration | |
|---|--|
| This screen allows you to configure a ATM P | WC. |
| VPI: 0 [0-255] | |
| VPI: 0 [0-255] | |
| VCI: 35 [32-65535] | |
| | |
| Select DSL Link Type (EoA is for PPPoE, IPc | E, and Bridge.) |
| EoA | |
| PPPoA | |
| © IPoA | |
| Encapsulation Mode: | LLC/SNAP-BRIDGING - |
| | |
| Service Category: | UBR Without PCR 👻 |
| Minimum Cell Rate: | -1 [cells/s] (-1 indicates no shaping) |
| Select Scheduler for Queues of Equal Preced | dence as the Default Queue |
| Weighted Round Robin | - |
| Weighted Fair Queuing | |
| Default Queue Weight: | 1 [1-63] |
| Default Queue Precedence: | 8 [1-8] (lower value, higher priority) |
| Default Queue Precedence: | 8 [1-6] (lower value, nigher phoney) |
| VC WRR Weight: | 1 [1-63] |
| VC Precedence: | 8 [1-8] (lower value, higher priority) |
| | ual precedence VC's and WRR among equal precedence VC's. |
| | edence and weight will be used for arbitration. |
| For multi-queue VC, its VC precedence and | weight will be used for arbitration. |
| | Back Apply/Save |

There are many settings here including: VPI/VCI, DSL Link Type, Encapsulation Mode, Minimum Cell Rate, Service Category and Queue Weight.

Here are the available encapsulations for each xDSL Link Type:

- EoA- LLC/SNAP-BRIDGING, VC/MUX
- ◆ PPPoA- VC/MUX, LLC/ENCAPSULATION
- ♦ IPoA- LLC/SNAP-ROUTING, VC MUX

STEP 3: Click **Apply/Save** to confirm your choices.

On the next screen, check that the ATM interface is added to the list. For example, an ATM interface on PVC 0/35 in Default Mode with an EoA Link type is shown below.

| | DSL ATM Interface Configuration | | | | | | | | | | | |
|-----------|---------------------------------|-----|----------------|----------|----------------------------|--------------------------------------|--------------------------|--------------|-------------|---------|------------------------|--------|
| Interface | Vpi | Vci | DSL Latency | Category | Peak Cell Rate(cells/s) | Sustainable Cell Rate(cells/s) | Max Burst Size(bytes) | Link Type | Conn Mode | IP QoS | MPAAL Prec/Alg/Wght | Remove |
| atm0 | 0 | 35 | Path0 | UBR | | | | EoA | VlanMuxMode | Support | 8/WRR/1 | Remove |

To add a WAN connection go to $E2 \sim WAN$ Connections.

E1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.



STEP 1: Go to Basic Setup → WAN Setup → Select PTM Interface from the drop-down menu.

| COM | TREND | Device I | nfo E | Sasic Setup | Advanced Se | etup Diag | | s I | Manag | gement | Logout |
|---|---------------|--------------------|----------|----------------------------|--------------------|--------------|-----|--------------|-----------|------------------------|--------|
| WAN Setup NAT LAN Parental Control | Step 1: Layer | 2 Interface | S | elect new interface DSI | to add: PTM Inter | | Add | | | | |
| Home Networking | Interface Vpi | Vci DSL Latency | Category | face DSL Laten | I WAN Interface Co | Conn Mode IP | | Conn Mode | IP QoS | MPAAL Prec/Alg/Wght | Remove |

This table is provided here for ease of reference.

| Heading | Description |
|-----------------|---|
| Interface | WAN interface name. |
| DSL Latency | ${Path0} \rightarrow portID = 0$ |
| PTM Priority | Normal or High Priority (Preemption). |
| Connection Mode | Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface. |
| IP QoS | Quality of Service (QoS) status. |
| Remove | Select interfaces to remove. |

STEP 2: Click **Add** to proceed to the next screen.

NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

| PTM Configuration | | |
|---|------------|--------------------------------------|
| This screen allows you to configure a PTM flow. | | |
| | | |
| Select Scheduler for Queues of Equal Precedence | e as the [| Default Queue |
| Weighted Round Robin | | |
| Weighted Fair Queuing | | |
| Default Queue Weight: | 1 | [1-63] |
| Default Queue Precedence: | 8 | [1-8] (lower value, higher priority) |
| Default Queue Minimum Rate: | -1 | [1-0 Kbps] (-1 indicates no shaping) |
| Default Queue Shaping Rate: | -1 | [1-0 Kbps] (-1 indicates no shaping) |
| Default Queue Shaping Burst Size: | 3000 | [bytes] (shall be >=1600) |
| | | Back Apply/Save |

Default PTM interface Quality of Service can be configured here, including Scheduler, Queue Weight and Rate Limit.

STEP 3: Click **Apply/Save** to confirm your choices.

On the next screen, check that the PTM interface is added to the list.

For example, an PTM interface in Default Mode is shown below.

| DSL PTM Interface Configuration | | | | | | | | |
|---------------------------------|-------------|--------------|-------------|---------|--------|--|--|--|
| Interface | DSL Latency | PTM Priority | Conn Mode | IP QoS | Remove | | | |
| ptm0 | Path0 | Normal&High | VlanMuxMode | Support | Remove | | | |

To add a WAN connection go to section E2 WAN Connections.

E1.3 ETHERNET Interfaces

Follow these procedures to configure a PTM interface.



This table is provided here for ease of reference.

| Heading | Description |
|-------------------|---|
| Interface/ (Name) | WAN interface name. |
| Connection Mode | Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface. |
| Remove | Select interfaces to remove. |

Interface DSL Latency PTM Priority Conn Mode IP QoS Remove
ETH WAN Interface Configuration
Interface/(Name) Connection Mode Remove

STEP 2: Click Add to proceed to the next screen.

| ETH WAN Configuration This screen allows you to configure a ETH port | | | | | | |
|---|--|--|--|--|--|--|
| Select a ETH port: | | | | | | |
| eth0/ETH1 - | | | | | | |
| Back Apply/Save | | | | | | |

STEP 3: Select an Ethernet port and Click **Apply/Save** to confirm your choices. On the next screen, check that the ETHERNET interface is added to the list.

| ETH WAN Interface Configuration | | | | | | | |
|---------------------------------|-----------------|--------|--|--|--|--|--|
| Interface/(Name) | Connection Mode | Remove | | | | | |
| eth0/ETH1 | VlanMuxMode | Remove | | | | | |

E2 ~ WAN Connections

The AR-5230 supports one WAN connection for each interface, up to a maximum of 8 connections.

To setup a WAN connection follow these instructions.



STEP 1: Go to Basic Setup $\xrightarrow{\text{Bask Setup}} \rightarrow$ WAN Setup.

| | Step 2: Wide Area Network (WAN) Service Setup | | | | | | | | | | | | | | |
|---|---|-------------|------|-----------|-----------|----------|---------------|----------------|-----|----------|------|--------------|---------------|--------|------|
| | Interface | Description | Туре | Vlan8021p | VlanMuxId | VlanTpid | Igmp Proxy | Igmp Source | NAT | Firewall | IPv6 | Mld Proxy | Mld Source | Remove | Edit |
| - | Add Remove | | | | | | | | | | | | | | |

STEP 2: Click **Add** to create a WAN connection. The following screen will display.

| WAN Service Interface Configuration |
|--|
| |
| Select a layer 2 interface for this service |
| Note: For ATM interface, the descriptor string is (portId_vpi_vci) For PTM interface, the descriptor string is (portId_high_low) Where portId=0> DSL Latency PATH0 portId=1> DSL Latency PATH1 portId=4> DSL Latency PATH0&1 low =0> Low PTM Priority not set low =1> Low PTM Priority set high =0> High PTM Priority not set ligh =1> High PTM Priority set |
| atm0/(0_0_35) - |
| Back Next |



STEP 3: Choose a layer 2 interface from the drop-down box and click **Next**. The WAN Service Configuration screen will display as shown below.

| WAN Service Configuration | |
|---|-----------------|
| Select WAN service type: PPP over Ethernet (PPPoE) IP over Ethernet (DHCP/ Static IP) Bridging | |
| Enter Service Description: pppoe_0_0_35 | |
| For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID. | |
| Enter 802.1P Priority [0-7]: | -1 |
| Enter 802.1Q VLAN ID [0-4094]: | -1 |
| Select VLAN TPID: | Select a TPID 🔻 |
| | |
| Internet Protocol Selection: | |
| IPv4 Only 👻 | |
| | Back Next |

- **NOTE:** The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the **Back** button and select a different layer 2 interface.
- **STEP 4:** You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:
 - (1) PPP over ETHERNET (PPPoE) IPv4
 (2) IP over ETHERNET (IPoE) IPv4
 (3) Bridging– IPv4
 (4) PPP over ATM (PPPoA) IPv4
 (5) IP over ATM (IPoA) IPv4
 (6) PPP over ETHERNET (PPPoE) IPv6
 (7) IP over ETHERNET (IPoE) IPv6
 (8) Bridging IPv6 (Not Supported)
 (9) PPP over ATM (PPPoA) IPv6
 (10) IPoA IPv6 (Not Supported)

The subsections that follow continue the WAN service setup procedure.

E2.1 PPP over ETHERNET (PPPoE) – IPv4

| STEP 1: Select the PPP over Ethernet radio button and click N |
|---|
|---|

| WAN Service Configuration | |
|--|-----------------|
| Select WAN service type: PPP over Ethernet (PPPoE) IP over Ethernet (DHCP/ Static IP) Bridging | |
| Enter Service Description: pppoe_0_0_35 For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID. | |
| Enter 802.1P Priority [0-7]: | -1 |
| Enter 802.1Q VLAN ID [0-4094]: | -1 |
| Select VLAN TPID: | Select a TPID 🔻 |
| Internet Protocol Selection: IPv4 Only | Back |

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

For VLAN tag Q-in-Q service, select the TPID from the list.

STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.

| PPP Usernam | PPP Username and Password | | |
|------------------|--|--|--|
| | quires that you have a user name and password to establish your connection. slow, enter the user name and password that your ISP has provided to you. | | |
| PPP Username: | | | |
| PPP Password: | | | |
| PPPoE Service | Name: | | |
| Authentication I | Method: AUTO | | |
| Enable F | ullcone NAT | | |
| Dial on d | demand (with idle timeout timer) | | |
| PPP IP e | extension | | |
| Enable N | AT | | |
| | | | |
| Enable F | Firewall | | |
| Use Stati | ic IPv4 Address | | |
| | | | |
| Fixed MT | τυ | | |
| MTU: 1492 | | | |
| Enable P | PPP Debug Mode | | |
| Bridge P | PPoE Frames Between WAN and Local Ports | | |
| | | | |
| IGMP Multica | ast Proxy | | |
| Enable I | IGMP Multicast Proxy | | |
| Enable I | IGMP Multicast Source | | |
| | Back | | |

The settings shown above are described below.

PPP SETTINGS

The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND

The AR-5320 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox \square . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

| ◄ | Dial on demand (with idle timeout timer) | |
|------|--|--|
| Inac | tivity Timeout (minutes) [1-4320]: | |

PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox \square . The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox \square should not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox \square is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox \square should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox \square . If selected, enter the static IP address in the **IPv4 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2.

FIXED MTU

Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1492 for PPPoE.



ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS

(This option is hidden when PPP IP Extension is enabled)

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The AR-5230 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE MLD MULTICAST PROXY

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

ENABLE MLD MULTICAST SOURCE

Click to allow use of this WAN interface as Multicast Listener Discovery (MLD) multicast source.

STEP 3: Choose an interface to be the default gateway.

| Routing Default Gateway | |
|---|--|
| Default gateway interface list can have multiple WAN gateways but only one will be used according to the p and the last one the lowest priority if the WAN interfa changed by removing all and adding them back in again | priority with the first being the higest ace is connected. Priority order can be |
| Selected Default Gateway Interfaces | Available Routed WAN Interfaces |
| ppp0.1 ^ | * |
| -> | |
| Ŧ | - |
| Back | t |

Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

| DNS Server Configuration | | | | |
|--|--------------------------|--|--|--|
| Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest 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. | | | | |
| Colort DNC Community for a first series in the | | | | |
| Select DNS Server Interface from available | | | | |
| Selected DNS Server Interfaces | Available WAN Interfaces | | | |
| | | | | |
| ppp0.1 ^ | <u>^</u> | | | |
| -> | | | | |
| <- | | | | |
| v | | | | |
| Use the following Static DNS IP address: | | | | |
| Primary DNS server: | | | | |
| Secondary DNS server: | | | | |
| Back | t | | | |

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

| WAN Setup - Summary | | |
|--|----------|--|
| Make sure that the settings below match the settings provided by your ISP. | | |
| Connection Type: | PPPoE | |
| NAT: | Enabled | |
| Full Cone NAT: | Disabled | |
| Firewall: | Disabled | |
| IGMP Multicast Proxy: | Disabled | |
| IGMP Multicast Source Enabled: | Disabled | |
| MLD Multicast Proxy: | Disabled | |
| MLD Multicast Source Enabled: | Disabled | |
| Quality Of Service: | Enabled | |
| Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications. Back Apply/Save | | |

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management \rightarrow Reboot and click **Reboot**.

E2.2 IP over ETHERNET (IPoE) - IPv4

STEP 1: Select the IP over Ethernet radio button and click **Next.**

| WAN Service Configuration | |
|--|-----------------|
| Select WAN service type: | |
| PPP over Ethernet (PPPoE) | |
| IP over Ethernet (DHCP/ Static IP) | |
| C Bridging | |
| | |
| | |
| | |
| Enter Service Description: ipoe_0_0_35 | |
| | |
| For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. | |
| For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID. | |
| Enter 802.1P Priority [0-7]: | -1 |
| Enter 802.1Q VLAN ID [0-4094]: | -1 |
| Select VLAN TPID: | Select a TPID 🔻 |
| | |
| Internet Protocol Selection: | |
| IPv4 Only | |
| | |
| Back | Next |

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

For VLAN Mux Connections only, you must enter Priority & VLAN ID tags.

| Enter 802.1P Priority [0-7]: | -1 |
|--------------------------------|-----------------|
| Enter 802.1Q VLAN ID [0-4094]: | -1 |
| Select VLAN TPID: | Select a TPID 🔻 |

For VLAN tag Q-in-Q service, select the TPID from the list.



STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can instead use the **Static IP address** method to assign WAN IP address, Subnet Mask and Default Gateway manually.

| WAN IP Settings | | | |
|--|-----------|------------------------|--|
| Enter information provided to you by your ISP to configure the WAN IP settings. Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway. | | | |
| Obtain an IP address automa | tically | | |
| Option 60 Vendor ID: | | | |
| Option 61 IAID: | | (8 hexadecimal digits) | |
| Option 61 DUID: | | (hexadecimal digit) | |
| Option 77 User ID: | | | |
| Option 125: | Oisable | C Enable | |
| Use the following Static IP ad | dress: | | |
| WAN IP Address: | |] | |
| WAN Subnet Mask: | | | |
| WAN gateway IP Address: | |] | |
| | Back Next | | |

Click **Next** to continue or click **Back** to return to the previous step.

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.

| Network Address Translation Settings | |
|---|--|
| Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN). | |
| Enable NAT | |
| Enable Fullcone NAT | |
| Enable Firewall | |
| IGMP Multicast | |
| Enable IGMP Multicast Proxy | |
| Enable IGMP Multicast Source | |
| Back | |

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox \square . The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox \square should not be selected, so as to free up system resources for improved performance.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

ENABLE FIREWALL

If this checkbox \square is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox \square should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST PROXY

Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

ENABLE IGMP MULTICAST SOURCE

Enable the WAN interface to be used as IGMP multicast source.

STEP 4: To choose an interface to be the default gateway.

| 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 higest 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 | |
| atm0.1 | * | |
| -> | | |
| <- | Ŧ | |
| Back | d | |

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

| DNS Server Configuration | |
|---|--|
| Select DNS Server Interface from available WAN inter server IP addresses for the system. In ATM mode, if static IPoE protocol is configured, Static DNS server I DNS Server Interfaces can have multiple WAN inter servers but only one will be used according to the prior higest and the last one the lowest priority if the WAN order can be changed by removing all and adding the | only a single PVC with IPoA or P addresses must be entered. erfaces served as system dns prity with the first being the interface is connected. Priority |
| Select DNS Server Interface from availa | ble WAN interfaces: |
| Selected DNS Server Interfaces | Available WAN Interfaces |
| atm0.1 | * |
| Use the following Static DNS IP address: Primary DNS server: | |
| Secondary DNS server: | |
| Back |] |

Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

| Connection Type: | IPoE | |
|--------------------------------|----------|--|
| NAT: | Enabled | |
| Full Cone NAT: | Disabled | |
| Firewall: | Disabled | |
| IGMP Multicast Proxy: | Disabled | |
| IGMP Multicast Source Enabled: | Disabled | |
| MLD Multicast Proxy: | Disabled | |
| MLD Multicast Source Enabled: | Disabled | |
| Quality Of Service: | Enabled | |

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management \rightarrow Reboot and click **Reboot**.



E2.3 Bridging- IPv4

NOTE: This connection type is not available on the Ethernet WAN interface.

STEP 1: Select the Bridging radio button and click **Next**.

| WAN Service Configuration | |
|---|-----------------|
| Select WAN service type: | |
| PPP over Ethernet (PPPoE) | |
| IP over Ethernet (DHCP/ Static IP) | |
| Bridging | |
| Allow as IGMP Multicast Source | |
| Allow as MLD Multicast Source | |
| | |
| Enter Service Description: br_0_0_35 | |
| | |
| For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. | |
| For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID | |
| Enter 802.1P Priority [0-7]: | -1 |
| Enter 802.1Q VLAN ID [0-4094]: | -1 |
| Select VLAN TPID: | Select a TPID 🔻 |
| | |
| Back Next | |

Allow as IGMP Multicast Source

Click to allow use of this bridge WAN interface as IGMP multicast source.

Allow as MLD Multicast Source

Click to allow use of this bridge WAN interface as MLD multicast source.

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

For VLAN tag Q-in-Q service, select the TPID from the list.



STEP 2: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to return to the previous screen.

| WAN Setup - Summary | | |
|---|--------------------|----------------------|
| Make sure that the settings below mat | tch the settings p | rovided by your ISP. |
| Connection Type: | Bridge | |
| NAT: | N/A | |
| Full Cone NAT: | Disabled | |
| Firewall: | Disabled | |
| IGMP Multicast Proxy: | Not Applicable | |
| IGMP Multicast Source Enabled: | Disabled | |
| MLD Multicast Proxy: | Not Applicable | |
| MLD Multicast Source Enabled: | Disabled | |
| Quality Of Service: | Enabled | |
| Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications Back Apply/Save | | |

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management \rightarrow Reboot and click **Reboot**.

NOTE: If this bridge connection is your only WAN service, the AR-5230 will be inaccessible for remote management or technical support from the WAN.

E2.4 PPP over ATM (PPPoA) - IPv4

| WAN Service Configuration |
|--|
| |
| Enter Service Description: pppoa_0_0_35 |
| |
| Network Protocol Selection: IPv4 Only |
| I VI Olity |
| Back Next |

- **STEP 1:** Click **Next** to continue.
- **STEP 2:** On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.

| PPP Username and Password | | |
|---|--|--|
| PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you. | | |
| PPP Username: | | |
| PPP Password: | | |
| Authentication Method: AUTO - | | |
| Enable Fullcone NAT | | |
| Dial on demand (with idle timeout timer) | | |
| | | |
| PPP IP extension | | |
| Enable NAT | | |
| Enable Firewall | | |
| Use Static IPv4 Address | | |
| Fixed MTU MTU: 1500 | | |
| Enable PPP Debug Mode | | |
| | | |
| IGMP Multicast Proxy | | |
| Enable IGMP Multicast Proxy | | |
| Enable IGMP Multicast Source | | |
| Back Next | | |

PPP SETTINGS

The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.



DIAL ON DEMAND

The AR-5230 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox \square . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

| Dial on demand (with idle timeout timer) | |
|--|--|
| Inactivity Timeout (minutes) [1-4320]: | |

PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox \square . The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox \square should not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox \square is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox \square should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox \square . If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2.

Fixed MTU

Fixed Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.



ENABLE IGMP MULTICAST PROXY

Tick the checkbox \square to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

ENABLE IGMP MULTICAST SOURCE

Enable the WAN interface to be used as IGMP multicast source.

STEP 3: Choose an interface to be the default gateway.

| 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 higest 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 | |
| pppoa0 ^ | * | |
| -> | | |
| <- | | |
| - | Ŧ | |
| Back | | |

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

| DNS Server Configuration | |
|--|--|
| Select DNS Server Interface from available WAN int addresses for the system. In ATM mode, if only a si protocol is configured, Static DNS server IP address DNS Server Interfaces can have multiple WAN int only one will be used according to the priority with one the lowest priority if the WAN interface is com- removing all and adding them back in again. | ngle PVC with IPoA or static IPoE es must be entered. terfaces served as system dns servers but the first being the higest and the last |
| Select DNS Server Interface from available | ble WAN interfaces: |
| Selected DNS Server Interfaces | Available WAN Interfaces |
| pppoa0 | |
| -> | |
| <- | |
| | - |
| Use the following Static DNS IP address | |
| Primary DNS server: | |
| Secondary DNS server: | |
| Back | ext |

Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

| NAT: Enabled Full Cone NAT: Disabled Firewall: Disabled IGMP Multicast Proxy: Disabled IGMP Multicast Proxy: Disabled MLD Multicast Proxy: Disabled | |
|---|--|
| Firewall: Disabled IGMP Multicast Proxy: Disabled IGMP Multicast Source Enabled: Disabled | |
| IGMP Multicast Proxy: Disabled IGMP Multicast Source Enabled: Disabled | |
| IGMP Multicast Source Enabled: Disabled | |
| | |
| MLD Multicact Depage Disabled | |
| Disabled | |
| MLD Multicast Source Enabled: Disabled | |
| Quality Of Service: Enabled | |

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management \rightarrow Reboot and click **Reboot**.

E2.5 IP over ATM (IPoA) - IPv4

| WAN Service Configuration | |
|-------------------------------------|-----------|
| Enter Service Description: ipoa_0_0 | _35 |
| | Back Next |

STEP 1: Click **Next** to continue.

STEP 2: Enter the WAN IP settings provided by your ISP. Click **Next** to continue.

| WAN IP Settings | | |
|-----------------------------------|-------------------------|------------------------|
| Enter information provided to you | by your ISP to configur | e the WAN IP settings. |
| WAN IP Address: | 0.0.0.0 | |
| WAN Subnet Mask: | 0.0.0 | |
| | Back Next | |

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.

| Network Address Translation Settings | | |
|---|--|--|
| Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN). | | |
| Enable NAT | | |
| Enable Fullcone NAT | | |
| Enable Firewall | | |
| IGMP Multicast | | |
| Enable IGMP Multicast Proxy | | |
| Enable IGMP Multicast Source | | |
| Back | | |

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox \square . The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox \square should not be selected, so as to free up system resources for improved performance.



ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host by sending a packet to the mapped external address.

ENABLE FIREWALL

If this checkbox \square is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox \square should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST PROXY

Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

ENABLE IGMP MULTICAST SOURCE

Enable the WAN interface to be used as IGMP multicast source.

STEP 4: Choose an interface to be the default gateway.

| 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 higest 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 | |
| ipoa0 | A | |
| -> | | |
| v | v | |
| Back Next | | |

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

| DNS Server Configuration | | |
|--|--------------------------|--|
| Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest 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. | | |
| Select DNS Server Interface from available WAN interfaces: | | |
| Selected DNS Server Interfaces | Available WAN Interfaces | |
| | A | |
| -> | | |
| | - | |
| Use the following Static DNS IP address: | | |
| Primary DNS server: | | |
| Secondary DNS server: | | |
| Back | t | |



STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

| WAN Setup - Summary | | |
|--|----------|--|
| Make sure that the settings below match the settings provided by your ISP. | | |
| Connection Type: | IPoA | |
| NAT: | Enabled | |
| Full Cone NAT: | Disabled | |
| Firewall: | Disabled | |
| IGMP Multicast Proxy: | Disabled | |
| IGMP Multicast Source Enabled: | Disabled | |
| MLD Multicast Proxy: | Disabled | |
| MLD Multicast Source Enabled: | Disabled | |
| Quality Of Service: | Enabled | |
| Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications. Back Apply/Save | | |

After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management \rightarrow Reboot and click **Reboot**.



E2.6 PPP over ETHERNET (PPPoE) – IPv6

STEP 1: Select the PPP over Ethernet radio button. Then select IPv6 only from the drop-down box at the bottom off the screen and click **Next**.

| WAN Service Configuration | |
|--|-----------------|
| Select WAN service type: | |
| PPP over Ethernet (PPPoE) | |
| IP over Ethernet (DHCP/ Static IP) | |
| Bridging | |
| | |
| | |
| | |
| Enter Service Description: pppoe 0_0_35 | |
| | |
| For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. | |
| For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID. | |
| Enter 802.1P Priority [0-7]: | -1 |
| Enter 802.1Q VLAN ID [0-4094]: | -1 |
| Select VLAN TPID: | Select a TPID 💌 |
| | |
| Internet Protocol Selection: | |
| IPv6 Only | |
| | |
| Back | |

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

For VLAN tag Q-in-Q service, select the TPID from the list.



STEP 2: On the next screen, enter the PPP settings as provided by your ISP.

| PPP Username and Password |
|--|
| PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you. |
| PPP Username: |
| PPP Password: |
| PPPoE Service Name: |
| Authentication Method: AUTO - |
| Enable Fullcone NAT |
| Dial on demand (with idle timeout timer) |
| PPP IP extension |
| Enable Firewall |
| Use Static IPv4 Address |
| Use Static IPv6 Address |
| Enable IPv6 Unnumbered Model |
| Launch Dhcp6c for Address Assignment (IANA) |
| Launch Dhcp6c for Prefix Delegation (IAPD) |
| Launch Dhcp6c for Rapid Commit |
| Fixed MTU |
| MTU: 1492 |
| Enable PPP Debug Mode |
| Bridge PPPoE Frames Between WAN and Local Ports |
| Enable MLD Multicast Proxy |
| Enable MLD Multicast Source |
| Back |

Click **Next** to continue or click **Back** to return to the previous step.

The settings shown above are described below.



PPP SETTINGS

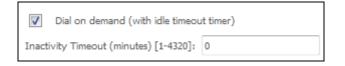
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND

The AR-5230 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox \square . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE FIREWALL

If this checkbox \square is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox \square should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox \square . If selected, enter the static IP address in the **IPv4 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2 IP Configuration.



USE STATIC IPv6 ADDRESS

Unless your service provider specially requires it, do not select this checkbox \square . If selected, enter the static IP address in the **IPv6 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2 IP Configuration.

ENABLE IPv6 UNNUMBERED MODEL

The IP unnumbered configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The IP unnumbered interface can "borrow" the IP address of another interface already configured on the router, which conserves network and address space.

LAUNCH DHCP6C FOR ADDRESS ASSIGNMENT (IANA)

The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet.

IANA's various activities can be broadly grouped in to three categories:

- Domain Names
- IANA manages the DNS Root, the .int and .arpa domains, and an IDN practices resource.Number Resources
- IANA coordinates the global pool of IP and AS numbers, providing them to Regional Internet Registries.
- Protocol Assignments
 - Internet protocols' numbering systems are managed by IANA in conjunction with standards bodies.

LAUNCH DHCP6C FOR PREFIX DELEGATION (IAPD)

An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting device. A requesting device may have more than one IAPD; for example, one for each of its interfaces.

A prefix-delegating router (DHCPv6 server) selects prefixes to be assigned to a requesting router (DHCPv6 client) upon receiving a request from the client. The server can select prefixes for a requesting client by using static and dynamic assignment mechanisms. Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID.

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

LAUNCH DHCP6C FOR RAPID COMMIT

Rapid-Commit; is the process (option) in which a Requesting Router (DHCP Client) obtains "configurable information" (configurable parameters) from a Delegating Router (DHCP Server) by using a rapid DHCPv6 two-message exchange. The messages that are exchanged between the two routers (RR and DR) are called the DHCPv6 "SOLICIT" message and the DHCPv6 "REPLY" message.



FIXED MTU

Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1492 for PPPoE.

ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS

(This option is hidden when PPP IP Extension is enabled)

When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The AR-5230 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE MLD MULTICAST PROXY

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

ENABLE MLD MULTICAST SOURCE

Click to allow use of this WAN interface as Multicast Listener Discovery (MLD) multicast source.

STEP 3: Choose an interface to be the default gateway. Also, select a preferred WAN interface as the system default IPv6 gateway (from the drop-down box).

| 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 higest 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 | Available Routed WAN | |
| Interfaces | Interfaces | |
| | | |
| ppp0.1 ^ | * | |
| -> | | |
| Ŧ | ~ | |
| IPv6: Select a preferred wan interface as the system default IPv6 gateway. | | |
| Selected WAN Interface pppoe_0_0_35/ppp0.1 - | | |
| Back | | |

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

| DNS Server Configuration | | |
|---|--|--|
| Select DNS Server Configuration Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest 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. | | |
| Select DNS Server Interface from available WAN interfaces: | | |
| Selected DNS Server Interfaces Available WAN Interfaces | | |
| ppp0.1 | | |
| Use the following Static DNS IP address: | | |
| Primary DNS server: | | |
| Secondary DNS server: | | |
| IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface. | | |
| Obtain IPv6 DNS info from a WAN interface: | | |
| WAN Interface selected: pppoe_0_0_35/ppp0.1 - | | |
| Use the following Static IPv6 DNS address: | | |
| Primary IPv6 DNS server: | | |
| Secondary IPv6 DNS server: | | |
| Back Next | | |



STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

| WAN Setup - Summary | | |
|--|----------|--|
| Make sure that the settings below match the settings provided by your ISP. | | |
| Constant Toront | PPPoE | |
| Connection Type: | PPPOE | |
| NAT: | Disabled | |
| Full Cone NAT: | Disabled | |
| Firewall: | Disabled | |
| IGMP Multicast Proxy: | Disabled | |
| IGMP Multicast Source Enabled: | Disabled | |
| MLD Multicast Proxy: | Disabled | |
| MLD Multicast Source Enabled: | Disabled | |
| Quality Of Service: | Enabled | |
| Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications. Back Apply/Save | | |

After clicking **Apply/Save**, the new service should appear on the main screen.



E2.7 IP over ETHERNET (IPoE) - IPv6

STEP 1: Select the IP over Ethernet radio button and click **Next.** Then select IPv6 only from the drop-down box at the bottom off the screen and click **Next**.

| WAN Service Configuration | |
|---|-----------------|
| Select WAN service type: | |
| PPP over Ethernet (PPPoE) | |
| IP over Ethernet (DHCP/ Static IP) | |
| Bridging | |
| | |
| | |
| | |
| Enter Service Description: ipoe_0_0_35 | |
| | |
| For tagged service, enter valid 802.1P Priority and 802.1Q VLAN I | D. |
| For untagged service, set -1 to both 802.1P Priority and 802.1Q V | LAN ID. |
| Enter 802.1P Priority [0-7]: | -1 |
| Enter 802.1Q VLAN ID [0-4094]: | -1 |
| Select VLAN TPID: | Select a TPID 🔻 |
| | |
| Internet Protocol Selection: | |
| IPv6 Only 👻 | |
| | |
| Bac | k Next |

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

For VLAN tag Q-in-Q service, select the TPID from the list.



STEP 2: The WAN IP settings screen provides access to the DHCP server settings.

You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can use the **Static IP address** method instead to assign WAN IP address, Subnet Mask and Default Gateway manually.

Enter information provided to you by your ISP to configure the WAN IPv6 settings.

Notice: If "Obtain an IPv6 address automatically" is chosen, DHCP client will be enabled on this WAN interface.

If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

| WAN IP Settings | | | |
|---|------------|------------------------|--|
| Enter information provided to you by your ISP to configure the WAN IP settings. Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway. | | | |
| Obtain an IP address autom | ationly | | |
| Option 60 Vendor ID: | | | |
| Option 61 IAID: | | (8 hexadecimal digits) | |
| Option 61 DUID: | | (hexadecimal digit) | |
| Option 77 User ID: | | | |
| Option 125: | Disable | Enable | |
| Use the following Static IP a | ddress: | | |
| WAN IP Address: | | | |
| WAN Subnet Mask: | | | |
| WAN gateway IP Address: | | | |
| Enter information provided to you by your ISP to configure the WAN IPv6 settings. Notice: If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface. If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64. | | | |
| Obtain an IPv6 address auto | omatically | | |
| Dhcpv6 Address Assignment (IANA) | | | |
| Dhcpv6 Prefix Delegation (IAPD) | | | |
| Dhcpv6 Rapid Commit | | | |
| Use the following Static IPve | address: | | |
| WAN IPv6 Address/Prefix Length: | | | |
| Specify the Next-Hop IPv6 address for this WAN interface. Notice: This address can be either a link local or a global unicast IPv6 address. WAN Next-Hop IPv6 Address: | | | |
| Back Next | | | |

Click **Next** to continue or click **Back** to return to the previous step.

DHCP6C FOR ADDRESS ASSIGNMENT (IANA)

The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet.

IANA's various activities can be broadly grouped in to three categories:

- Domain Names
- IANA manages the DNS Root, the .int and .arpa domains, and an IDN practices resource.Number Resources
- IANA coordinates the global pool of IP and AS numbers, providing them to Regional Internet Registries.
- Protocol Assignments

Internet protocols' numbering systems are managed by IANA in conjunction with standards bodies.

DHCP6C FOR PREFIX DELEGATION (IAPD)

An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting device. A requesting device may have more than one IAPD; for example, one for each of its interfaces.

A prefix-delegating router (DHCPv6 server) selects prefixes to be assigned to a requesting router (DHCPv6 client) upon receiving a request from the client. The server can select prefixes for a requesting client by using static and dynamic assignment mechanisms. Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID.

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

DHCP6C FOR RAPID COMMIT

Rapid-Commit; is the process (option) in which a Requesting Router (DHCP Client) obtains "configurable information" (configurable parameters) from a Delegating Router (DHCP Server) by using a rapid DHCPv6 two-message exchange. The messages that are exchanged between the two routers (RR and DR) are called the DHCPv6 "SOLICIT" message and the DHCPv6 "REPLY" message.

WAN NEXT-HOP IPv6 ADDRESS

Specify the Next-Hop IPv6 address for this WAN interface. This address can be either a link local or a global unicast IPv6 address.



STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑.

| Netw | Network Address Translation Settings | | | | |
|---|--------------------------------------|--|--|--|--|
| Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN). | | | | | |
| | Enable NAT | | | | |
| | Enable Firewall | | | | |
| | Enable MLD Multicast Proxy | | | | |
| | Enable MLD Multicast Source | | | | |
| Back Next | | | | | |

Click **Next** to continue or click **Back** to return to the previous step.

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox \square . The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox \square should not be selected, so as to free up system resources for improved performance.

ENABLE FIREWALL

If this checkbox \square is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox \square should not be selected so as to free up system resources for better performance.

ENABLE MLD MULTICAST PROXY

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

ENABLE MLD MULTICAST SOURCE

Click to allow use of this WAN interface as Multicast Listener Discovery (MLD) multicast source.

STEP 4: To choose an interface to be the default gateway. Also, select a preferred WAN interface as the system default IPv6 gateway (from the drop-down box).

| Routing Default Gateway | | | | | | |
|--|------------------------------------|--|--|--|--|--|
| Nouting 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 higest 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 | | | | | |
| atm0.1 * -> | | | | | | |
| IPv6: Select a preferred wan interface as the system default IPv6 gateway. | | | | | | |
| Selected WAN Interface ipoe_0_0_35/atm0.1 | | | | | | |
| Back | ext | | | | | |

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter Static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

| DNS Server Configuration | | | | | |
|--|--------------------|-------------------|-----|--|--|
| Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest 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. | | | | | |
| Select DNS Server Inte | rface from availa | ble WAN interfac | 25: | | |
| Selected DNS Server Interfaces | | Available WAN Int | | | |
| | | | | | |
| atm0.1 ^ | | | ^ | | |
| | | | | | |
| | -> | | | | |
| | | | | | |
| - | | | - | | |
| | | | | | |
| Use the following Static | c DNS IP address: | | | | |
| Primary DNS server: | | | | | |
| | | | | | |
| Secondary DNS server: | | | | | |
| IPv6: Select the configured WA enter the static IPv6 DNS server Note that selecting a WAN interf on that interface. | Addresses. | | | | |
| Obtain IPv6 DNS info fro | om a WAN interface | : | | | |
| WAN Interface selected: | ipoe_0_0_35/a | tm0.1 🔻 | | | |
| Use the following Static 1 | IPv6 DNS address: | | | | |
| Primary IPv6 DNS server: | | | | | |
| Secondary IPv6 DNS server: | | | | | |
| | Back | | | | |



STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

| WAN Setup - Summary | | | | | | | |
|--|----------|--|--|--|--|--|--|
| Make sure that the settings below match the settings provided by your ISP. | | | | | | | |
| Connection Type: IPoE | | | | | | | |
| NAT: | Disabled | | | | | | |
| Full Cone NAT: | Disabled | | | | | | |
| Firewall: | Disabled | | | | | | |
| IGMP Multicast Proxy: | Disabled | | | | | | |
| IGMP Multicast Source Enabled: | Disabled | | | | | | |
| MLD Multicast Proxy: | Disabled | | | | | | |
| MLD Multicast Source Enabled: | Disabled | | | | | | |
| Quality Of Service: Enabled | | | | | | | |
| Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications. Back Apply/Save | | | | | | | |

After clicking **Apply/Save**, the new service should appear on the main screen.



E2.8 PPP over ATM (PPPoA) - IPv6

STEP 1: Select IPv6 Only from the drop-down box at the bottom of this screen and click **Next**.

| WAN Service Configuration |
|--|
| |
| Enter Service Description: pppoa_0_0_35 |
| Network Protocol Selection: IPv6 Only |
| Back Next |



| STEP | 2: | On the | next screen, | enter | the PPP | settings as | provided | by | your ISP | ۰. |
|------|----|--------|--------------|-------|---------|-------------|----------|----|----------|----|
|------|----|--------|--------------|-------|---------|-------------|----------|----|----------|----|

| PPP Username and Password | | | | | | |
|--|--|--|--|--|--|--|
| PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you. | | | | | | |
| PPP Username: | | | | | | |
| PPP Password: Authentication Method: AUTO - | | | | | | |
| Autoritication method: | | | | | | |
| Enable Fullcone NAT | | | | | | |
| Dial on demand (with idle timeout timer) | | | | | | |
| PPP IP extension | | | | | | |
| Enable Firewall | | | | | | |
| Use Static IPv4 Address | | | | | | |
| Use Static IPv6 Address | | | | | | |
| Enable IPv6 Unnumbered Model | | | | | | |
| Launch Dhcp6c for Address Assignment (IANA) | | | | | | |
| Launch Dhcp6c for Prefix Delegation (IAPD) | | | | | | |
| Launch Dhcp6c for Rapid Commit | | | | | | |
| | | | | | | |
| Fixed MTU | | | | | | |
| MTU: 1500 | | | | | | |
| Enable PPP Debug Mode | | | | | | |
| | | | | | | |
| Enable MLD Multicast Proxy | | | | | | |
| Enable MLD Multicast Source | | | | | | |
| Back | | | | | | |

Click **Next** to continue or click **Back** to return to the previous step.

PPP SETTINGS

The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)



ENABLE FULLCONE NAT

This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND

The AR-5230 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox \square . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

| 1 | Dial on demand (with idle timeout timer) | | | |
|--------|--|---|--|--|
| Inacti | vity Timeout (minutes) [1-4320]: | 0 | | |

PPP IP EXTENSION

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE FIREWALL

If this checkbox \square is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox \square should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS

Unless your service provider specially requires it, do not select this checkbox \square . If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in 3.2 IP Configuration.

USE STATIC IPv6 ADDRESS

Unless your service provider specially requires it, do not select this checkbox \square . If selected, enter the static IP address in the **IPv6 Address** field.

Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2 IP Configuration.



ENABLE IPv6 UNNUMBERED MODEL

The IP unnumbered configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The IP unnumbered interface can "borrow" the IP address of another interface already configured on the router, which conserves network and address space.

LAUNCH DHCP6C FOR ADDRESS ASSIGNMENT (IANA)

The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet.

IANA's various activities can be broadly grouped in to three categories:

- Domain Names
- IANA manages the DNS Root, the .int and .arpa domains, and an IDN practices resource.Number Resources
- IANA coordinates the global pool of IP and AS numbers, providing them to Regional Internet Registries.
- Protocol Assignments

Internet protocols' numbering systems are managed by IANA in conjunction with standards bodies.

LAUNCH DHCP6C FOR PREFIX DELEGATION (IAPD)

An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting device. A requesting device may have more than one IAPD; for example, one for each of its interfaces.

A prefix-delegating router (DHCPv6 server) selects prefixes to be assigned to a requesting router (DHCPv6 client) upon receiving a request from the client. The server can select prefixes for a requesting client by using static and dynamic assignment mechanisms. Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID.

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

LAUNCH DHCP6C FOR RAPID COMMIT

Rapid-Commit; is the process (option) in which a Requesting Router (DHCP Client) obtains "configurable information" (configurable parameters) from a Delegating Router (DHCP Server) by using a rapid DHCPv6 two-message exchange. The messages that are exchanged between the two routers (RR and DR) are called the DHCPv6 "SOLICIT" message and the DHCPv6 "REPLY" message.

FIXED MTU

Fixed Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

ENABLE PPP DEBUG MODE

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.



ENABLE MLD MULTICAST PROXY

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

ENABLE MLD MULTICAST SOURCE

Click to allow use of this WAN interface as Multicast Listener Discovery (MLD) multicast source.

STEP 3: Choose an interface to be the default gateway.

| 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 higest 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 | | | | | |
| pppoa0 -> < | | | | | | |
| IPv6: Select a preferred wan interface as the system default IPv6 gateway. | | | | | | |
| Selected WAN Interface pppoa_0_0_35/pppoa0 - | | | | | | |
| Back | Next | | | | | |

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter Static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

| DNS Server Configuration | | | | | | |
|--|--|--------------------------|--|--|--|--|
| Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest 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. | | | | | | |
| Select DNS Server In | terface from availa | able WAN interfaces: | | | | |
| Selected DNS Server Interface | is i | Available WAN Interfaces | | | | |
| pppoa0 ^ | | * | | | | |
| ~ | -> | ~ | | | | |
| Use the following Sta | atic DNS IP address | : | | | | |
| Primary DNS server: | Primary DNS server: | | | | | |
| Secondary DNS server: | | | | | | |
| IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface. | | | | | | |
| Obtain IPv6 DNS info fro | Obtain IPv6 DNS info from a WAN interface: | | | | | |
| WAN Interface selected: | pppoa_0_0_35/ | pppoa0 👻 | | | | |
| Use the following Static IPv6 DNS address: | | | | | | |
| Primary IPv6 DNS server: | | | | | | |
| Secondary IPv6 DNS server: | | | | | | |
| Back Next | | | | | | |



STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

| WAN Setup - Summary | | | | | | |
|--|----------|--|--|--|--|--|
| Make sure that the settings below match the settings provided by your ISP. | | | | | | |
| Connection Type: | PPPoA | | | | | |
| NAT: | Disabled | | | | | |
| Full Cone NAT: | Disabled | | | | | |
| Firewall: | Disabled | | | | | |
| IGMP Multicast: | Disabled | | | | | |
| Quality Of Service: | Enabled | | | | | |
| Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications. Back Apply/Save | | | | | | |

After clicking **Apply/Save**, the new service should appear on the main screen.

Appendix F – Printer Server

COMTREND

These steps explain the procedure for enabling the Printer Server.

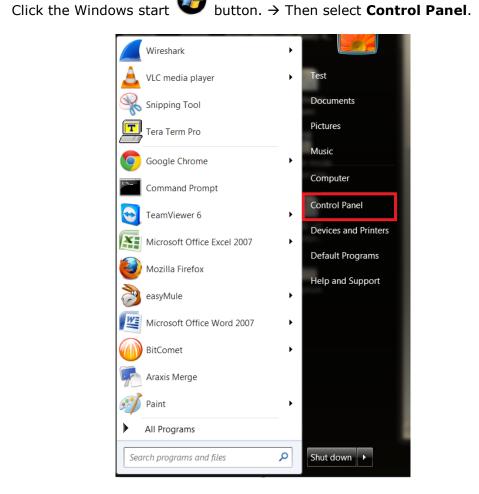
NOTE: This function only applies to models with a USB host port.

STEP 1: Enable Print Server from Web User Interface. Select the Enable on-board print server checkbox ☑ and input Printer name & Make and model. Click the **Apply/Save** button.

NOTE: The **Printer name** can be any text string up to 40 characters. The **Make and model** can be any text string up to 128 characters.

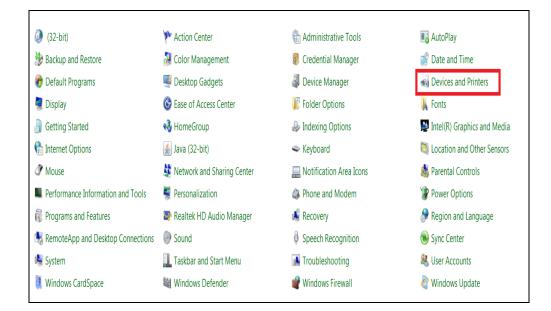
| COMI | | fo Basic Setup Advanced Setup Diagnostics Manag | ement Logout |
|---|--|---|--------------|
| WAN Setup NAT | Print Server settings This page allows you to a | enable / disable printer support. | |
| LAN Wireless | Manufacturer Produ | ct Serial Number | |
| Parental Control Home Networking | 🖉 Enable on-board pr | int server. | |
| Print Server DLNA Storage Service | Printer name Make and model | hpdeskjet 321123 | |
| otorage out the | | Apply/Save | |





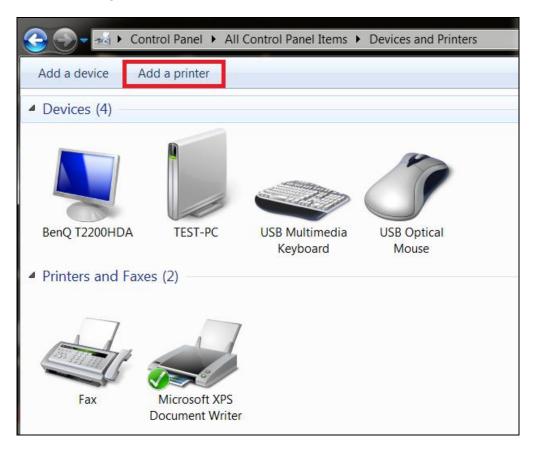
STEP 2: Click the Windows start U button. \rightarrow Then select **Control Panel**.

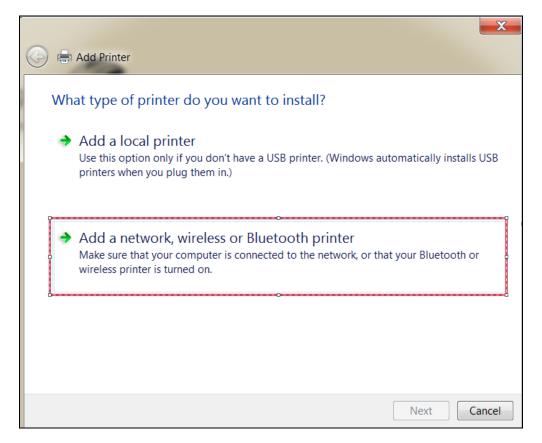




STEP 3: Select **Devices and Printers**.

STEP 4: Select Add a printer.





STEP 5: Select **Add a network, wireless or Bluetooth printer**.

STEP 6: Click the **Stop** button. → Select **The printer that I want isn't listed**.

| | | X |
|-------------------------|------------------|-------------|
| 🚱 🖶 Add Printer | | |
| Searching for available | printers | |
| Printer Name | Address | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | 1 |
| | | |
| | | Stop |
| ➔ The printer that I w | ant isn't listed | |
| | 2 | |
| | | Next Cancel |

STEP 7: Choose **Select a shared printer by name**. Then input the printer link and click **Next**.

http://LAN IP:631/printers/the name of the printer

NOTE: The printer name must be the same name inputted in the WEB UI "printer server settings" as in step 1.

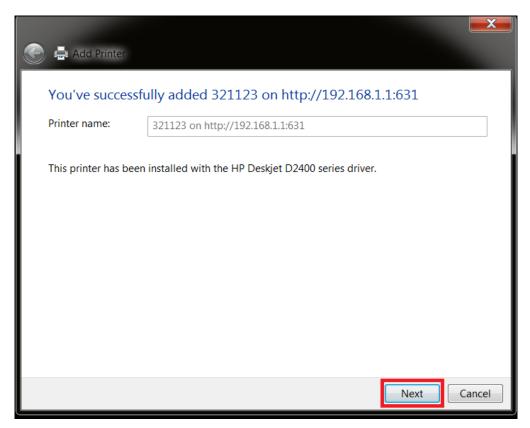
| Add Printer | | × |
|---|---------------|-------------|
| Find a printer by name or TCF | P/IP address | |
| Browse for a printer | 1 | |
| Select a shared printer by name | | |
| http://192.168.1.1:631/printers/ | 321123 | Browse |
| Example: \\computername\print http://computername/printers/p | | |
| Add a printer using a TCP/IP addres | s or hostname | |
| | | |
| | | 2 |
| | | 2 |
| | | Next Cancel |

STEP 8: Select the manufacturer \rightarrow and model of your printer \rightarrow then, click **OK**.

| Add Printer Wizard | ? | x |
|--|---|---|
| installation disk, cli | turer and model of your printer. If your printer came with an ck Have Disk. If your printer is not listed, consult your printer a compatible printer. | T |
| Manufacturer Generic Gestetner HP 1 infotec KONICA MINOL TA | Have Disk | |
| | 3 OK Cancel | |



STEP 9: The printer has been successfully installed. Click the **Next** button.



STEP 10: Click Finish (or print a test page if required).

| 🕞 📮 Add Printer |
|--|
| You've successfully added 321123 on http://192.168.1.1:631 |
| To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page. Print a test page |
| Finish Cancel |

STEP 11: Go to \rightarrow **Control Panel** \rightarrow **All Control Panel Items** \rightarrow **Devices and Printers** to confirm that the printer has been configured.

