

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 VR-3063 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 wireless settings.

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

Device Info

Basic Setup

Advanced Setup

Diagnostics

Management

Logout

English ▾

- Settings
- System Log
- SNMP Agent
- TR-069 Client
- Internet Time
- Access Control
- Accounts
- Services
- IP Address
- Update Software
- Reboot

Access Control -- Accounts/Passwords

By default, access to your Broadband router is controlled through three user accounts: root,support,and user.

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.

Use the fields below to update passwords for the accounts, add/remove accounts (max of 5 accounts). Note: Passwords may be as long as 16 characters but must not contain a space.

Select an account:

 Create an account:

Old Password:

New Password:

Confirm Password:

Use the options below to enable/disable accounts and privileges.

Feature	root	support	user	apuser
Account access	All	<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="text" value="None"/>
Add/Remove WAN	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wireless - Basic	Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wireless - Advanced	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
LAN Settings	Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Port Mapping	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NAT Settings	Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Update Software	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security	Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Quality of Service	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Management Settings	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advanced Setup	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Accounts	Enable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Diagnostics	Enable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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. The 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.

COMTREND

Device Info Basic Setup Advanced Setup Diagnostics Management Logout

English ▾

Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Accounts
Services
IP Address
Update Software
Reboot

Service Access Control Configuration

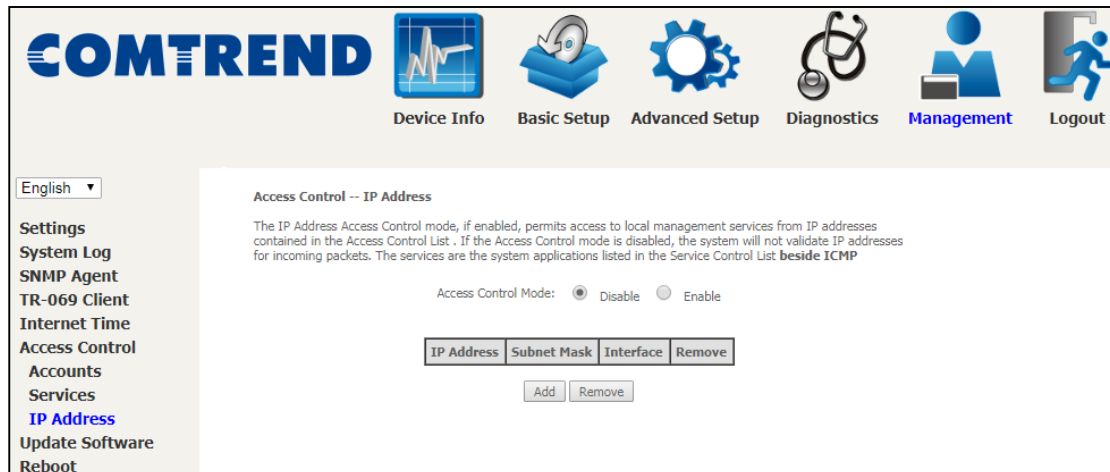
Select each listbox and click save/apply to configure your Setting.

Service	Current	New	Port
HTTP	Lan	LAN ▾	80
SSH	Lan	LAN ▾	22
TELNET	Lan	LAN ▾	23
SNMP	Disable	Disable ▾	161
HTTPS	Lan	LAN ▾	443
FTP	Lan	LAN ▾	21
TFTP	Lan	LAN ▾	69
ICMP	Lan	LAN ▾	0

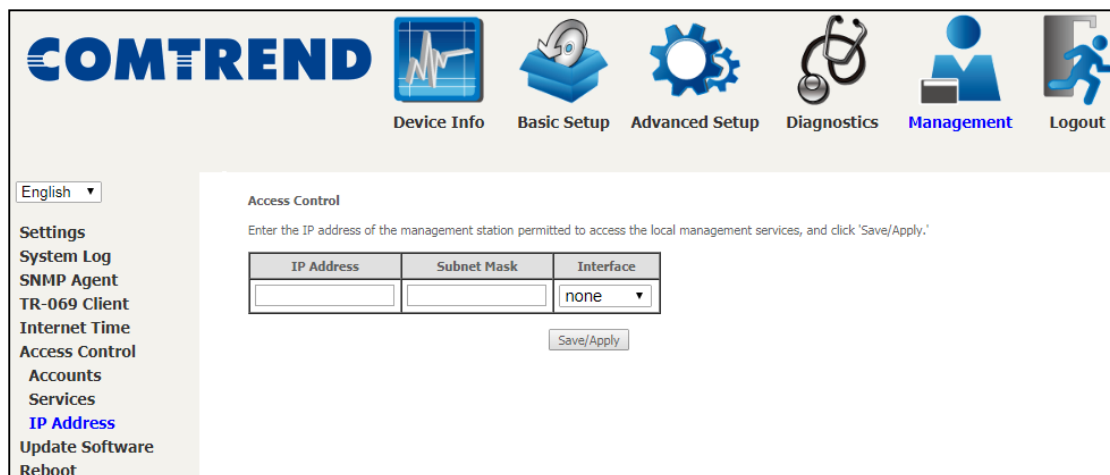
Apply/Save

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.



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

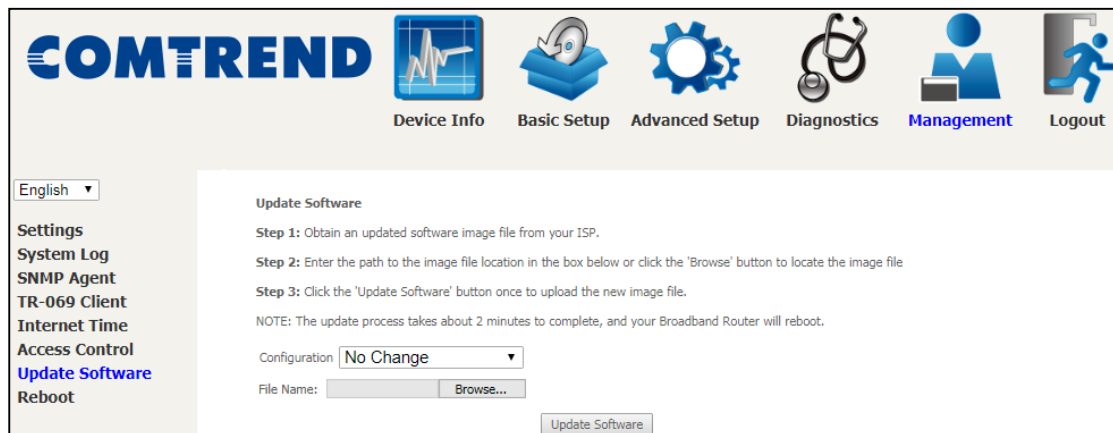
IP Address – IP address of the management station.

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 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.

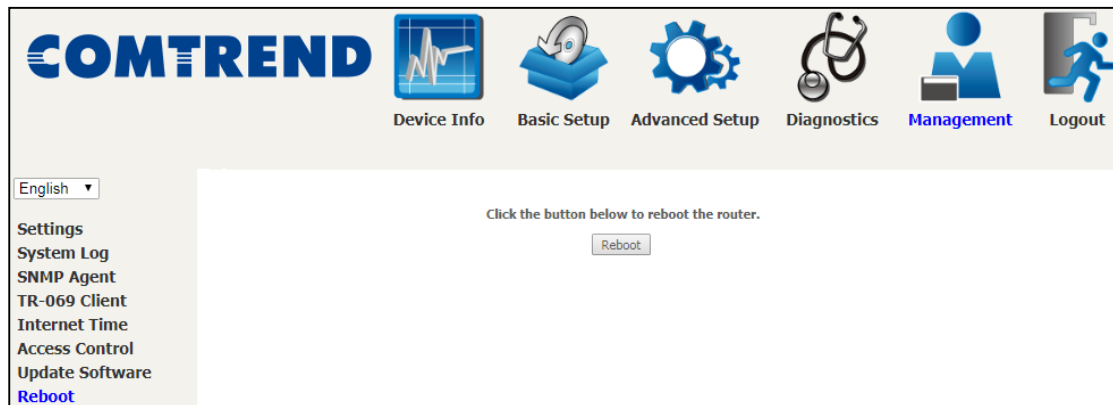
STEP 3: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 4: Click the **Update Software** button once to upload and install the file.

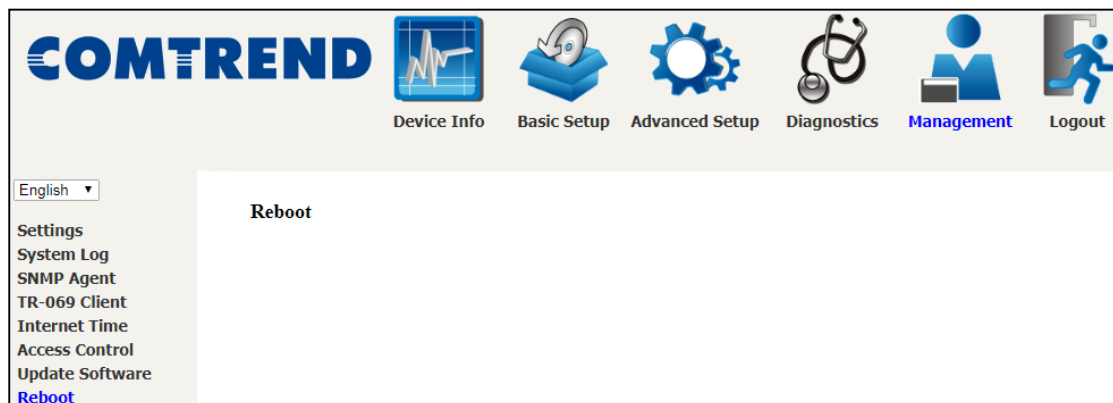
NOTE: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the [Device Information](#) screen with the firmware version installed,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

8.8 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.

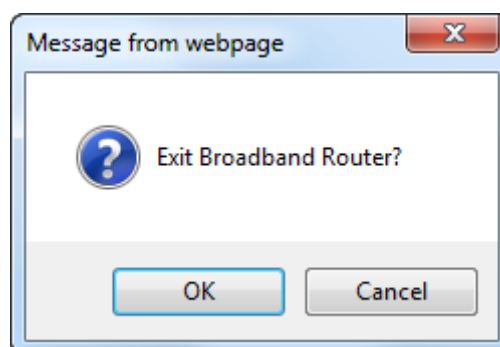


Chapter 9 Logout

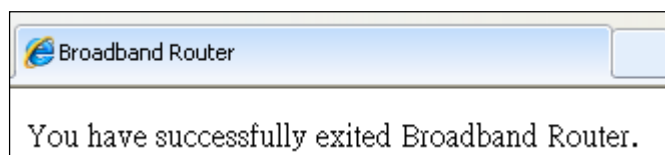
To log out from the device simply click the following icon located at the top of your screen.



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



Upon successful exit, the following message will be displayed.



Appendix A - Firewall

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 → Security → 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.

Example 2:

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

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 → Security → 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

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 VR-3063, 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

Giga ETHERNET Ports (RJ45)

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

Appendix C – Specifications

Hardware

- RJ-11 X1 for VDSL2 (35b)/ADSL2+ (Annex A)
- RJ-45 X 4 for GELAN
- RJ-45 X 1 for GEWAN
- SFP cage X 1
- Reset button X 1
- 2.4Ghz (WPS & Wi-Fi On/Off) button X 1
- 5Ghz (WPS & Wi-Fi On/Off) button X 1
- Internal Antenna X 14
- Power switch X 1
- USB 3.0 Host X 1

ADSL

- G.994
- G.992.1 (G.dmt) Annexes A
- G.992.2 (G.lite) Annexes A
- ANSI T1.413
- G.992.3 (ADSL2) Annexes A
- G.992.5 (ADSL2+) Annexes A

VDSL

- G.993.2(VDSL2) 35b, 30a, 17a, 12a, 12b, 8a, 8b, 8c, 8d
- G.993.5 (G.vector)
- G.998.4 (G.INP)
- SRA (Seamless Rate Adaptation)
- UPBO (Upstream Power Back-off)

Ethernet

- IEEE 802.3, IEEE 802.3u IEEE 802.3ab
- 10/100 /1000 BASE-T, auto-sense
- Support MDI/MDX

USB

- USB 3.0 host
- File Sharing & Printer Server

Management

- TR-069/TR-098/TR-104/TR-111/TR-181, SNMP, Telnet, Web- Based Management, Configuration Backup and Restoration
- Software Upgrade via HTTP, TFTP Server, or FTP Server

Firewall/Filtering

- Stateful Packet Inspection Firewall
- Stateless Packet Filter
- URI/URL Filtering
- Denial of Service (DOS): ARP Attacks, Ping Attacks, Ping of Death, LAND, SYNC, Smurf, Unreachable, Teardrop
- Port Scan Detection and Protection
- TCP/IP/Port/Interface Filtering Rules Support Both Incoming and Outgoing Filtering

NAT/PAT

- Support One to One, Many to One, Many to Many (Overload), Many to Many (No Overload) NAT
- NAT Loopback
- Port Triggering
- Port Forwarding (Virtual Server)
- Symmetric port-overloading NAT, Full-Cone NAT
- DMZ host
- VPN Pass Through (PPTP, L2TP, IPSec)

Networking Protocols

- RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Router, RFC 2516 (PPPoE); RFC 1577 (IPoA)
- PPPoE Pass-Through, Multiple PPPoE Sessions on Single WAN Interface
- PPPoE Filtering of Non-PPPoE Packets Between WAN and LAN
- Transparent Bridging Between all LAN and WAN Interfaces
- 802.1p/802.1q VLAN, DSCP
- 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, DLNA
- IPv6 Dual Stack, IPV6 Rapid Deployment (6RD)

Dimensions (without base)

- 269mm (H) x 200 mm (W) x 58 mm (D)

Kit Weight

- (1* VR-3063, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter) = 1 kg

Wireless

- IEEE 802.11n, 2.4GHz, 3T3R
- Backward compatible with 802.11g/b 2412~2472 MHz
- IEEE 802.11ac,5GHz, 4T4R,
- Backward compatible with 802.11n/a U-NII-1 (5150~5250 MHz)
- U-NII-2a (5250~5350 MHz) optional
- U-NII-2c/2e (5470~5725 MHz) optional
- U-NII-3 (5725~5825 MHz)
- WPA/WPA-PSK, WPA2/WPA2-PSK with TKIP & AES

Security Type

- Multiple SSID
- MAC Address Filtering

Power Supply

- External power adapter: 12VDC/ 2.5A

Environment

- Operating Temperature: 0°C ~40°C (32°F ~104°F)
- Operating Humidity: 10%~90% non-condensing
- Storage Temperature: -25°C ~65°C (-23°F ~149°F)
- Storage Humidity: 5%~90% non-condensing

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 → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

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

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

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

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

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

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

Appendix E - Printer Server

These steps explain the procedure for enabling the Printer Server.

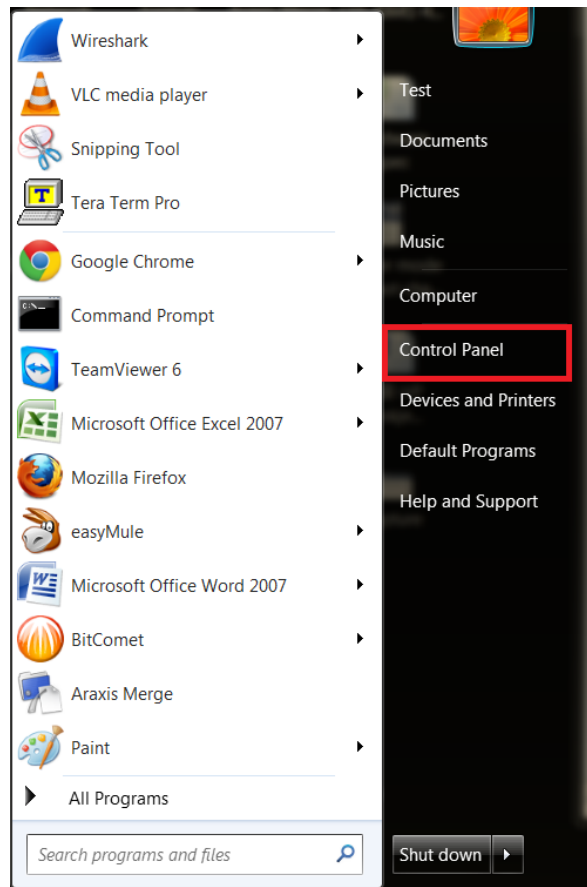
NOTE: This function only applies to models with a USB host port.

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 **Save/Apply** button.

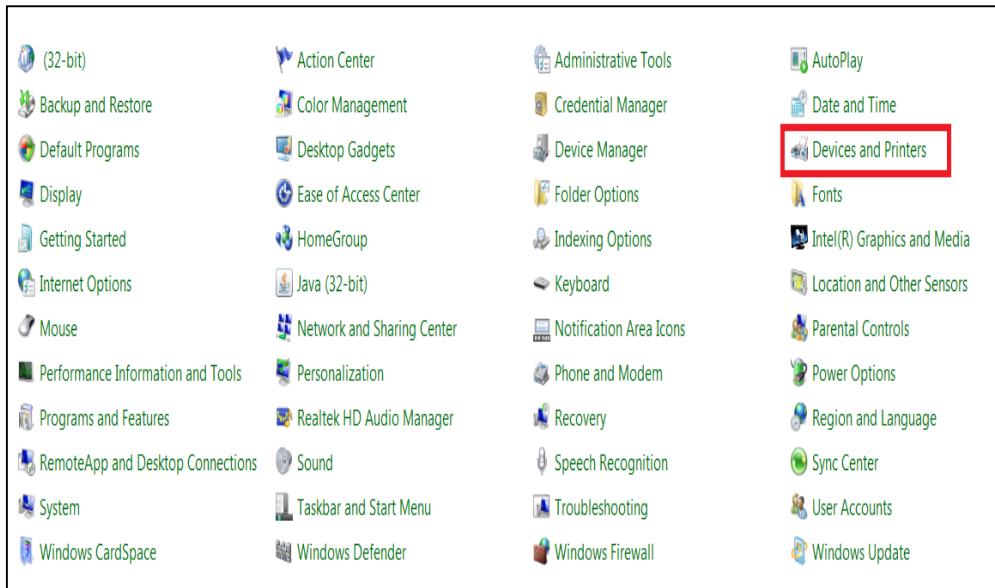
NOTE: The **Printer name** can be any text string up to 40 characters.
The **Make and model** can be any text string up to 128 characters.

The screenshot displays the COMTREND web interface. At the top, there is a navigation bar with the COMTREND logo and several icons representing different settings: Device Info, Basic Setup, Advanced Setup, Diagnostics, Management, and Logout. Below the navigation bar, there is a sidebar menu on the left with options: English (language), WAN Setup, NAT, LAN, Wireless, Parental Control, Home Networking, Print Server (highlighted), DLNA, and Storage Service. The main content area shows the 'Print Server settings' page. It includes a heading 'Print Server settings' and a sub-heading 'This page allows you to enable / disable printer support.' Below this, there are three tabs: 'Manufacturer', 'Product', and 'Serial Number'. A checkbox labeled 'Enable on-board print server.' is checked. There are two input fields: 'Printer name' with the value 'hpdeskjet' and 'Make and model' with the value '321123'. A 'Save/Apply' button is located at the bottom right of the settings area.

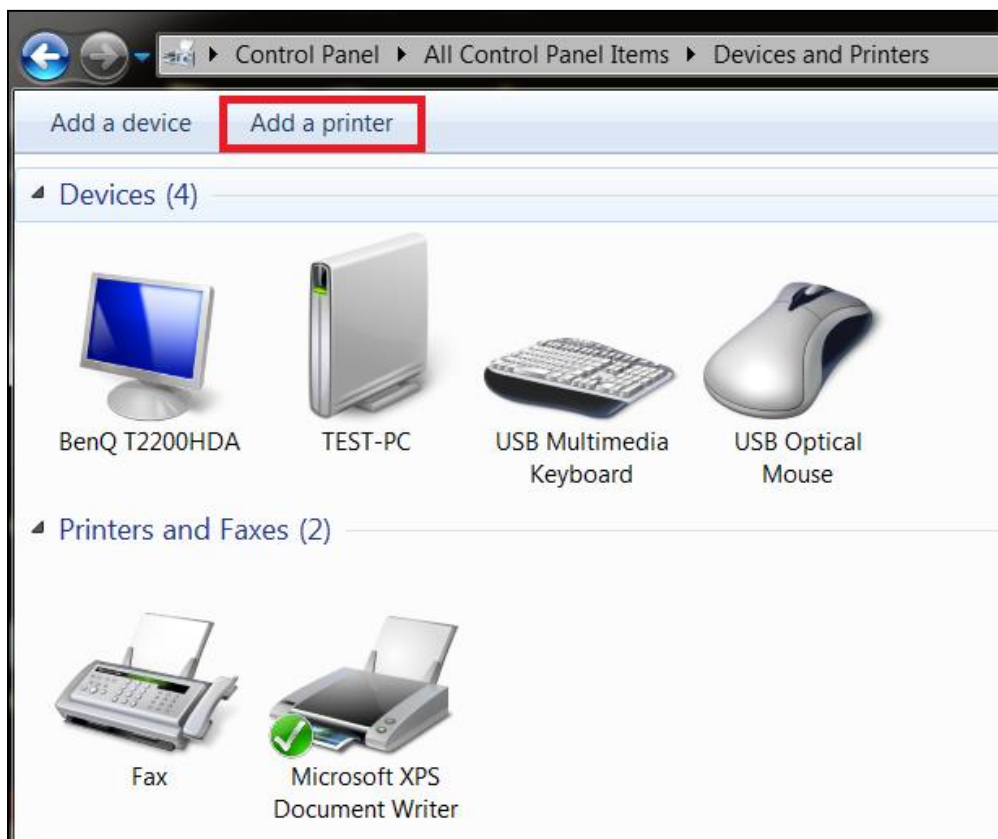
STEP 2: Click the Windows start  button. → Then select **Control Panel**.



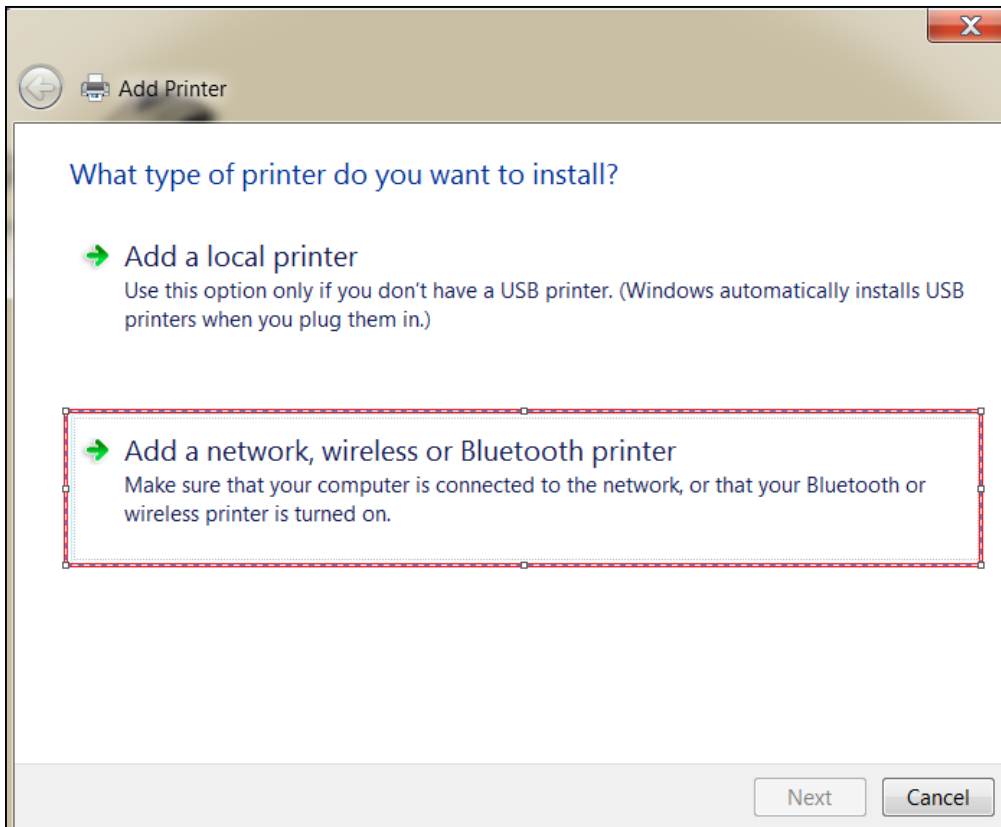
STEP 3: Select Devices and Printers.



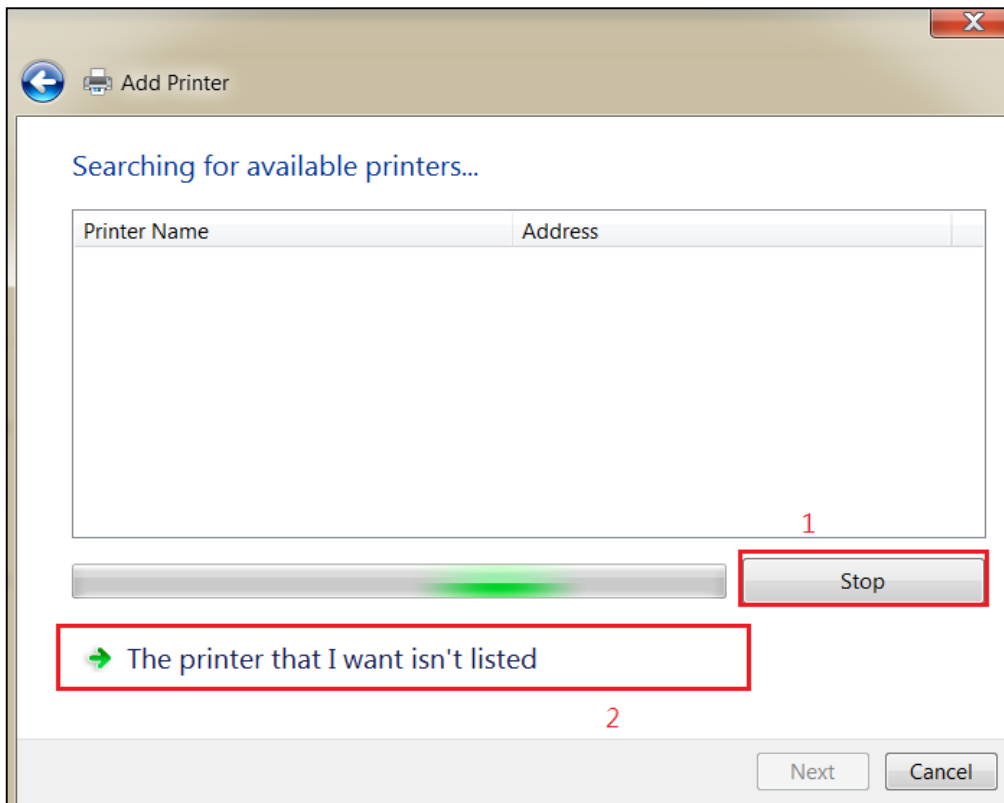
STEP 4: Select Add a printer.



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



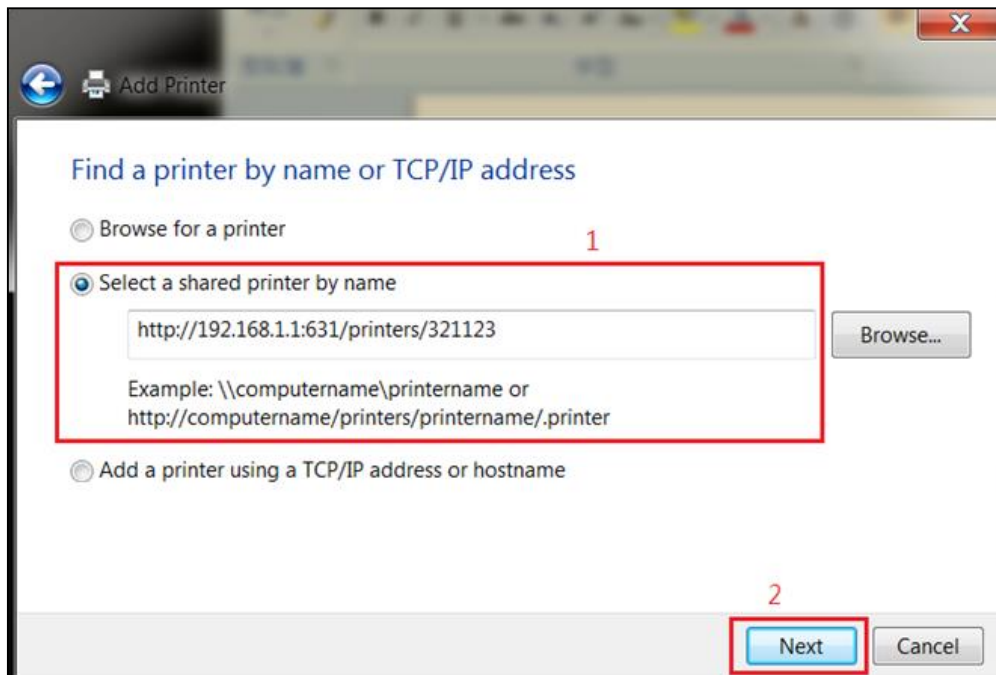
STEP 6: Click the **Stop** button. → Select **The printer that I want isn't listed.**



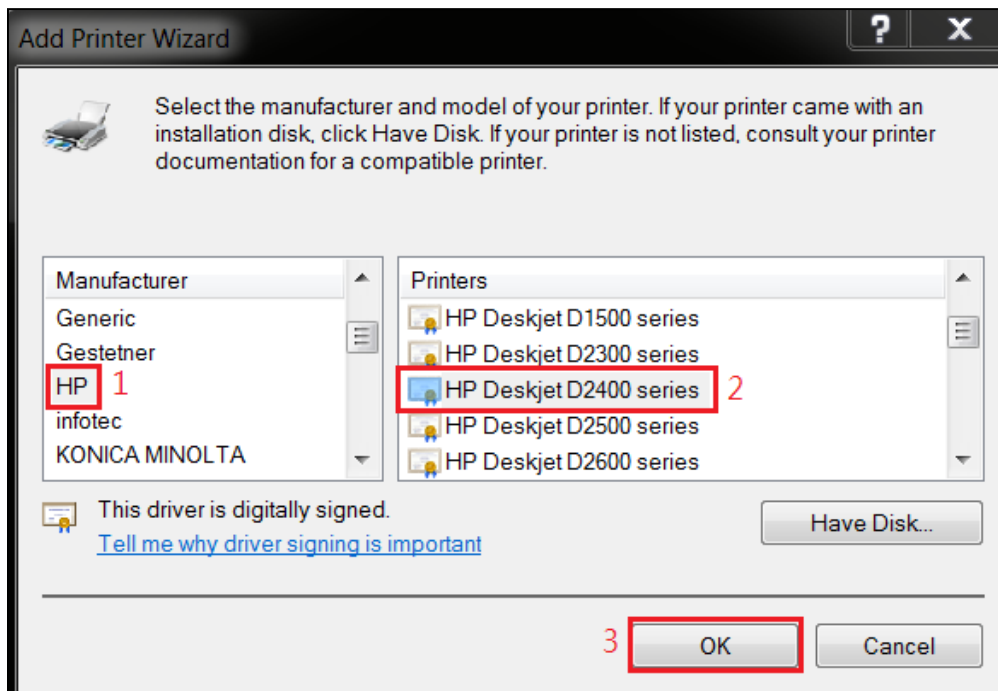
STEP 7: Choose **Select a shared printer by name**. Then input the printer link and click **Next**.

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

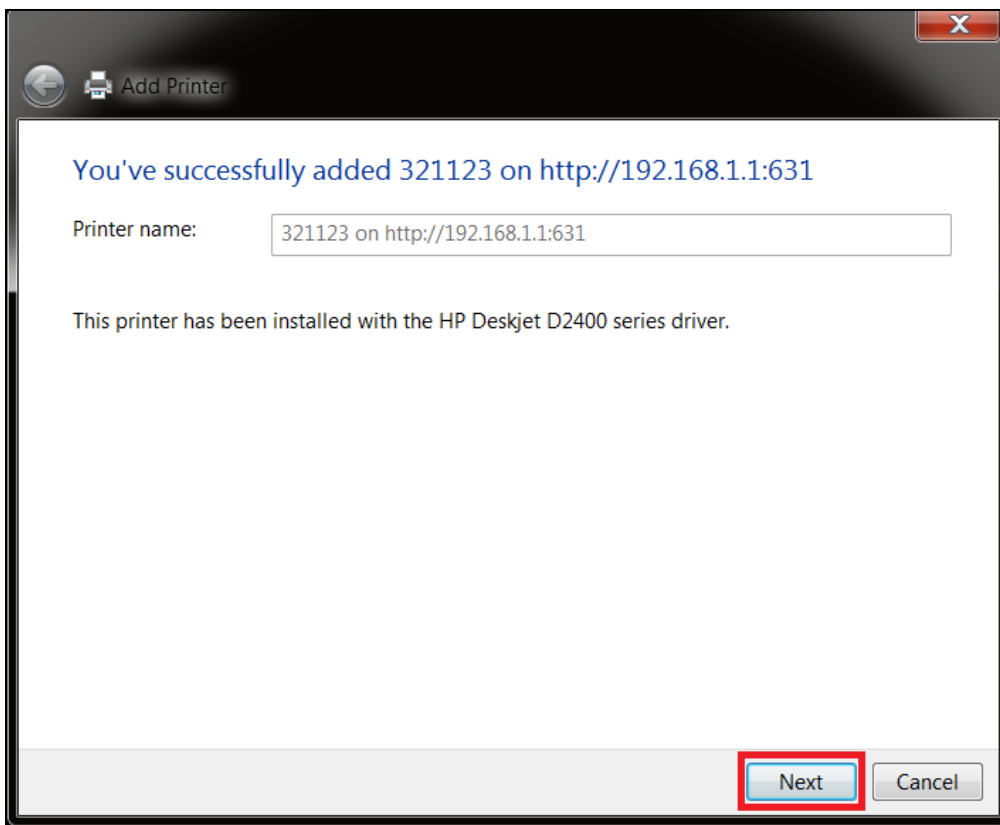
NOTE: The printer name must be the same name inputted in the WEB UI “printer server settings” as in step 1.



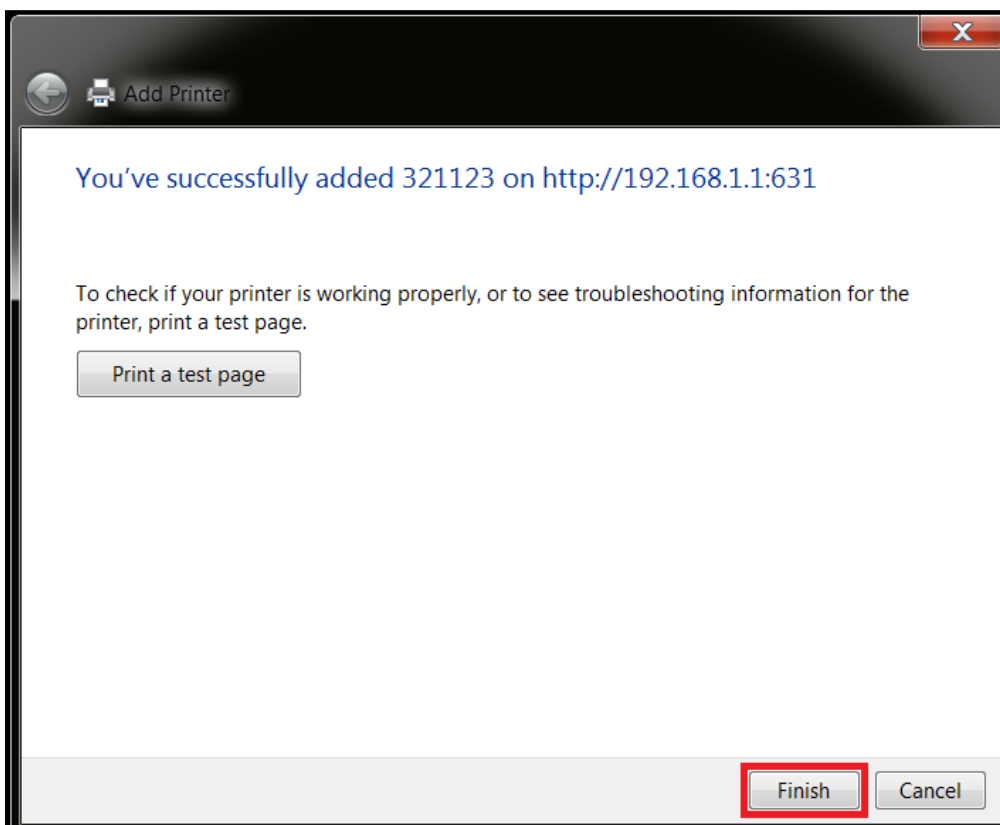
STEP 8: Select the **manufacturer** → and **model** of your printer → then, click **OK**.



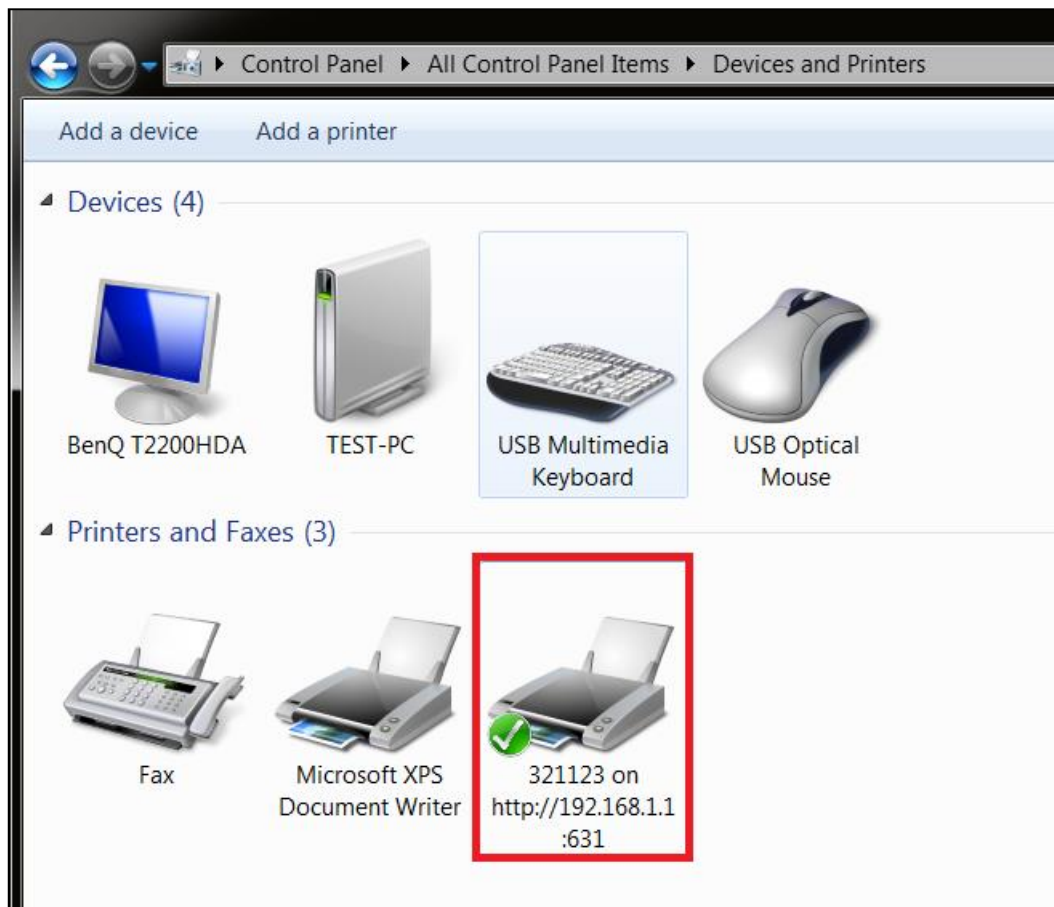
STEP 9: The printer has been successfully installed. Click the **Next** button.



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



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



Appendix F - 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.

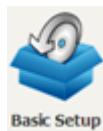
F1 ~ Layer 2 Interfaces

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.

F1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE: The VR-3063 supports up to 16 ATM interfaces.



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

Step 1: Layer 2 Interface

Select new interface to add: **ATM Interface** Add

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	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)
DSL Latency	{Path0} → 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 continuously 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
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 PVC.

VPI: [0-255]
 VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA
 PPPoA
 IPoA

Encapsulation Mode: ▾

Service Category: ▾

Select Scheduler for Queues of Equal Precedence

Round Robin (weight=1)
 Weighted Fair Queuing
 Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)

Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

There are many settings here including: VPI/VCI, DSL Link Type, Encapsulation Mode, 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 **Save/Apply** 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.

Select new interface to add:

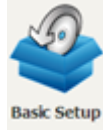
DSL ATM Interface Configuration

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	Remove
atm0	0	35	Path0	UBR				EoA	VlanMuxMode	Support	<input type="button" value="Remove"/>

To add a WAN connection go to [Section F2 ~ WAN Connections](#).

F1.2 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.

This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
DSL Latency	{Path0} → 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

Round Robin (weight=1)
 Weighted Fair Queuing
 Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)
 Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

The default scheduler mechanism for the PTM interface can be configured here by selecting the corresponding algorithm and adjust the queue weight/default precedence for the maximum QoS effect suitable for your environment.

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

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

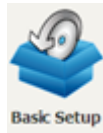
For example, a PTM interface in Default Mode is shown below.

DSL PTM Interface Configuration					
Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	<input type="button" value="Remove"/>

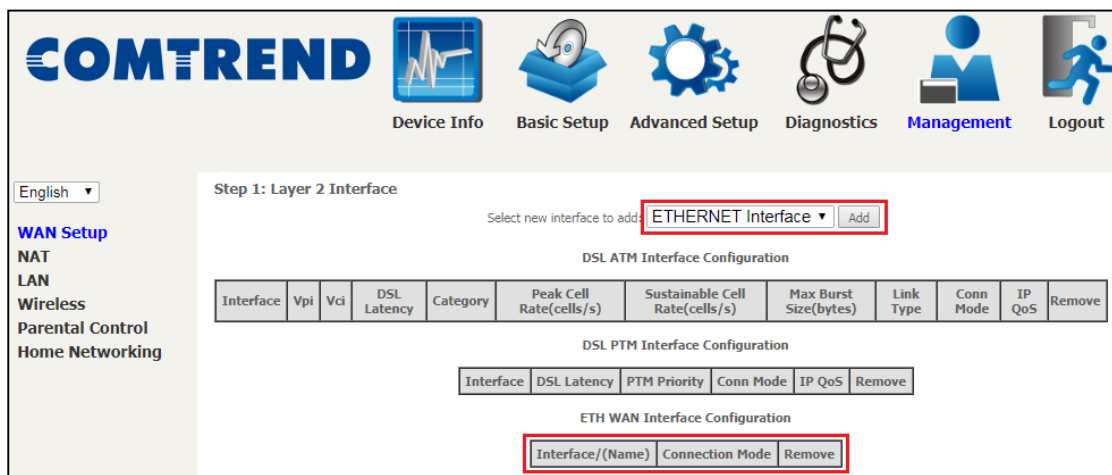
To add a WAN connection go to [Section F2 ~ WAN Connections](#).

F1.3 Ethernet WAN Interface

The VR-3063 supports a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet interface.



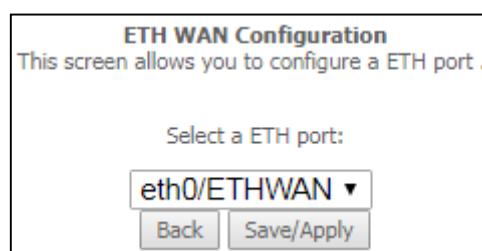
STEP 1: Go to Basic Setup → WAN Setup → Select ETHERNET Interface from the drop-down menu.



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.

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



STEP 3: Select an Ethernet port and Click **Save/Apply** to confirm your choices.

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

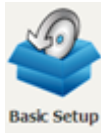
ETH WAN Interface Configuration		
Interface/(Name)	Connection Mode	Remove
eth0/ETHWAN	VlanMuxMode	<input type="button" value="Remove"/>

To add a WAN connection go to [Section F2 ~ WAN Connections](#).

F2 ~ WAN Connections

The VR-3063 supports one WAN connection for each interface, up to a maximum of 16 connections.

To setup a WAN connection follow these instructions.



STEP 1: Go to Basic Setup → WAN Setup.

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
<div style="display: flex; justify-content: center; gap: 10px;"> Add Remove </div>														

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
 high =1 --> High PTM Priority set

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:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.

802.1P Priority [0-7]:

802.1Q VLAN ID [0-4094]:

VLAN TPID:

Internet Protocol Selection:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Select a TPID if VLAN tag Q-in-Q is used.

STEP 5: 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) For [PPP over ETHERNET \(PPPoE\) – IPv4](#)
- (2) For [IP over ETHERNET \(IPoE\) – IPv4](#)
- (3) For [Bridging – IPv4](#)
- (4) For [PPP over ATM \(PPPoA\) – IPv4](#)
- (5) For [IP over ATM \(IPoA\) – IPv4](#)
- (6) For [PPP over ETHERNET \(PPPoE\) – IPv6](#)
- (7) For [IP over ETHERNET \(IPoE\) – IPv6](#)
- (8) Bridging – IPv6 (Not Supported)
- (9) For [PPP over ATM \(PPPoA\) – IPv6](#)
- (10) IPoA – IPv6 (Not Supported)

The subsections that follow continue the WAN service setup procedure.

F2.1 PPP over ETHERNET (PPPoE) – IPv4

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

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet (DHCP/ Static IP)
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.

802.1P Priority [0-7]:

802.1Q VLAN ID [0-4094]:

VLAN TPID:

Internet Protocol Selection:

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:

PPPoE Service Name:

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:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast Proxy

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

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 VR-3063 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

<input checked="" type="checkbox"/> Dial on demand (with idle timeout timer) Inactivity Timeout (minutes) [1-4320]: <input type="text" value="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 NAT

If the LAN is configured with a private IP address, the user should select this checkbox . 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 should not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox 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 . 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](#).

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 VR-3063 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE IGMP MULTICAST PROXY

Tick the checkbox 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 highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	<input type="button" value="->"/> <input type="button" value="<-"/>	
<input type="button" value="Back"/> <input type="button" value="Next"/>		

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
ppp0.1	<input type="button" value="->"/> <input type="button" value="<-"/>	

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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 **Save/Apply** 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:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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

F2.2 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)
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.

802.1P Priority [0-7]:
802.1Q VLAN ID [0-4094]:
VLAN TPID:

Internet Protocol Selection:

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.

WAN Service Interface Configuration

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 automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digits)

Option 77 User ID:

Option 125: Disable Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

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 Next

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox . 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 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 is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox 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. 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 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 highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
atm0.1	<input type="button" value="->"/>	
	<input type="button" value="<-"/>	

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
<div style="border: 1px solid gray; padding: 5px; min-height: 150px;">atm0.1</div>	<div style="border: 1px solid gray; width: 30px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;">-></div> <div style="border: 1px solid gray; width: 30px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;"><-</div>	<div style="border: 1px solid gray; min-height: 150px;"></div>

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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 **Save/Apply** 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:	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:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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

F2.3 Bridging – IPv4

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:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.

802.1P Priority [0-7]:

802.1Q VLAN ID [0-4094]:

VLAN TPID:

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.

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

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

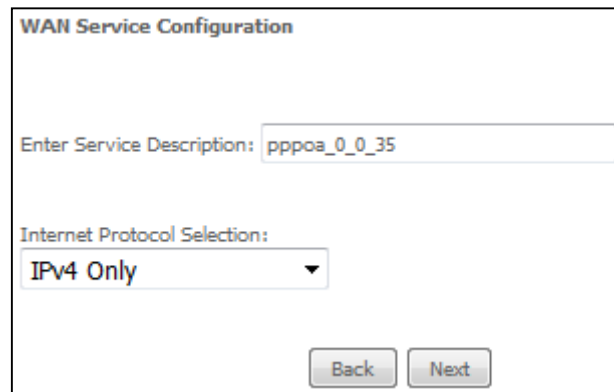
Connection Type:	Bridge
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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

NOTE: If this bridge connection is your only WAN service, the VR-3063 will be inaccessible for remote management or technical support from the WAN.

F2.4 PPP over ATM (PPPoA) – IPv4



The image shows a 'WAN Service Configuration' dialog box. It contains a text input field for 'Enter Service Description' with the value 'pppoa_0_0_35'. Below it is a dropdown menu for 'Internet Protocol Selection' currently set to 'IPv4 Only'. At the bottom right are 'Back' and 'Next' buttons.

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:

Enable PPP Debug Mode

IGMP Multicast Proxy

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

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 VR-3063 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . 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 . 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 should not be selected to free up system resources for better performance.

ENABLE FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox 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 . 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](#).

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 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 highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0a0	

->
<-

Back Next

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
pppoa0	<input type="button" value="->"/> <input type="button" value="<-"/>	

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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 **Save/Apply** 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:	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:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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

F2.5 IP over ATM (IPoA) – IPv4

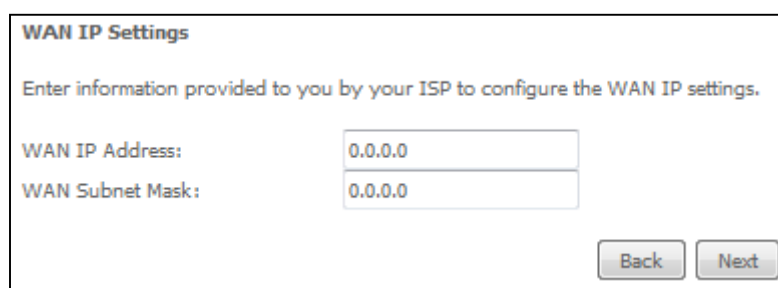


WAN Service Configuration

Enter Service Description:

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

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



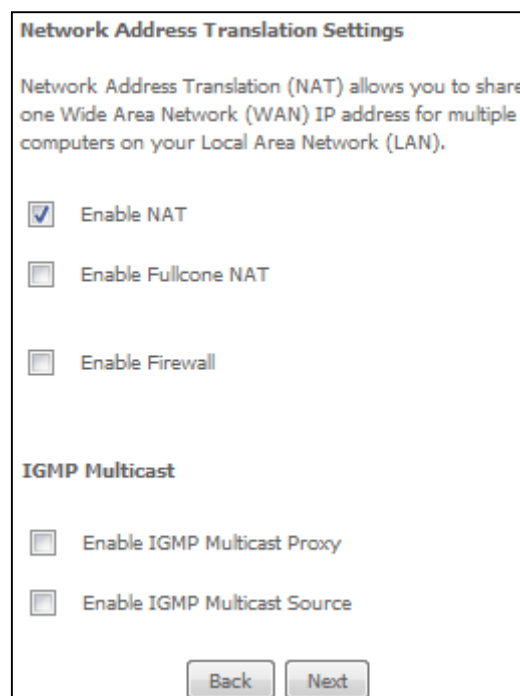
WAN IP Settings

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

WAN IP Address:

WAN Subnet Mask:

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

ENABLE NAT

If the LAN is configured with a private IP address, the user should select this checkbox . 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 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 is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox 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. 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 4: Choose an interface to be the default gateway.

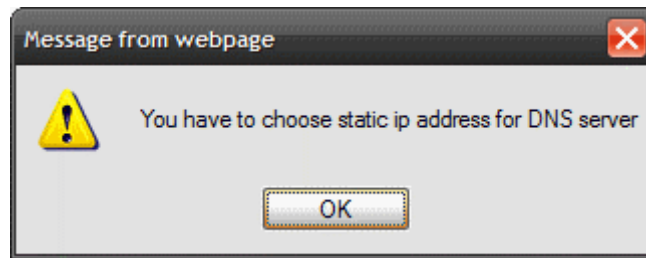
Routing -- Default Gateway

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 highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ipoa0	<input type="button" value="->"/> <input type="button" value="<-"/>	
<input type="button" value="Back"/>		<input type="button" value="Next"/>

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

NOTE: If the DHCP server is not enabled on another WAN interface then the following notification will be shown before the next screen.



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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
	<input type="button" value="->"/> <input type="button" value="<-"/>	

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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 **Save/Apply** 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:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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

F2.6 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:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.

802.1P Priority [0-7]:

802.1Q VLAN ID [0-4094]:

VLAN TPID:

Internet Protocol Selection:

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:

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Enable MLD Multicast Proxy

Enable MLD Multicast Source

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 VR-3063 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.

<input checked="" type="checkbox"/> Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]: <input type="text" value="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 is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox 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 . 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 . 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 VR-3063 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 highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0.1	

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

Selected WAN Interface:

Back Next

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.

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

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:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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 **Save/Apply** 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:	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:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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

F2.7 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:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.

802.1P Priority [0-7]:
802.1Q VLAN ID [0-4094]:
VLAN TPID:

Internet Protocol Selection:

STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IPv6 address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can use the **Static IPv6 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 Service Interface Configuration

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 automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digits)

Option 77 User ID:

Option 125: Disable Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

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 automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

Use the following Static IPv6 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:

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 .

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

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 . 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 should not be selected, so as to free up system resources for improved performance.

ENABLE FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox 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

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

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
atm0.1	<input type="button" value="->"/> <input type="button" value="<-"/>	

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

Selected WAN Interface

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.

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

atm0.1

->

<-

Available WAN Interfaces

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:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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 **Save/Apply** 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.

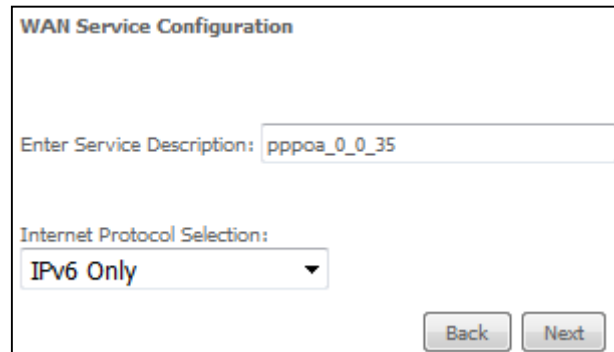
Connection Type:	IPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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

F2.8 PPP over ATM (PPPoA) – IPv6

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



The screenshot shows a configuration window titled "WAN Service Configuration". It contains the following elements:

- A text input field labeled "Enter Service Description:" with the value "pppoa_0_0_35".
- A dropdown menu labeled "Internet Protocol Selection:" with "IPv6 Only" selected.
- Two buttons at the bottom right: "Back" and "Next".

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:

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:

Enable PPP Debug Mode

Enable MLD Multicast Proxy

Enable MLD Multicast Source

PPP SETTINGS

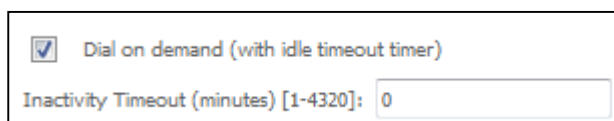
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

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 VR-3063 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox . 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 FIREWALL

If this checkbox is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox 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 . 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 . 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 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.

<p>Selected Default Gateway Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;">pppoa0</div>	<div style="border: 1px solid gray; width: 30px; height: 30px; margin: 5px auto; display: flex; align-items: center; justify-content: center;">-></div> <div style="border: 1px solid gray; width: 30px; height: 30px; margin: 5px auto; display: flex; align-items: center; justify-content: center;"><-</div>	<p>Available Routed WAN Interfaces</p> <div style="border: 1px solid gray; padding: 5px; min-height: 100px;"></div>
--	---	--

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

Selected WAN Interface pppoa_0_0_35/pppoa0

Back
Next

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.

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces		Available WAN Interfaces
pppoa0	<input type="button" value="->"/> <input type="button" value="<-"/>	

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:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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 **Save/Apply** 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

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