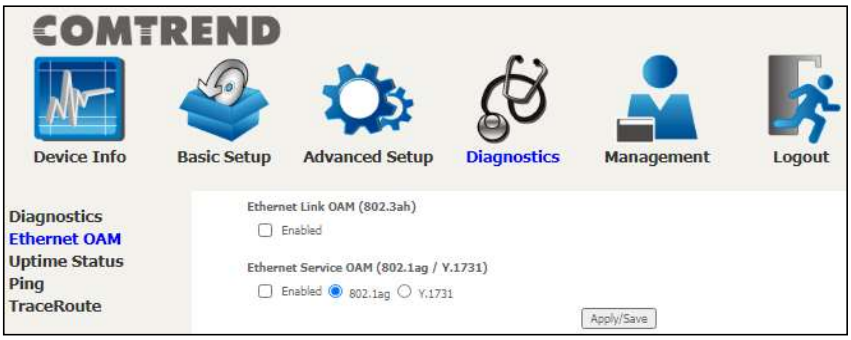
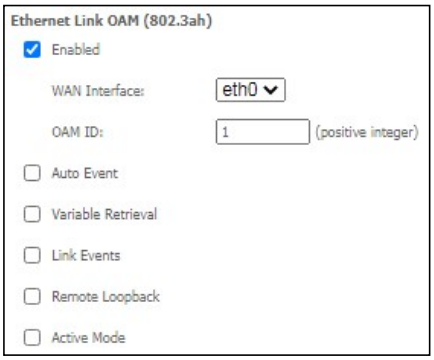
7.2 Ethernet OAM

The Ethernet OAM (Operations, Administration, Management) page provides settings to enable/disable 802.3ah, 802.1ag/Y1.731 OAM protocols.



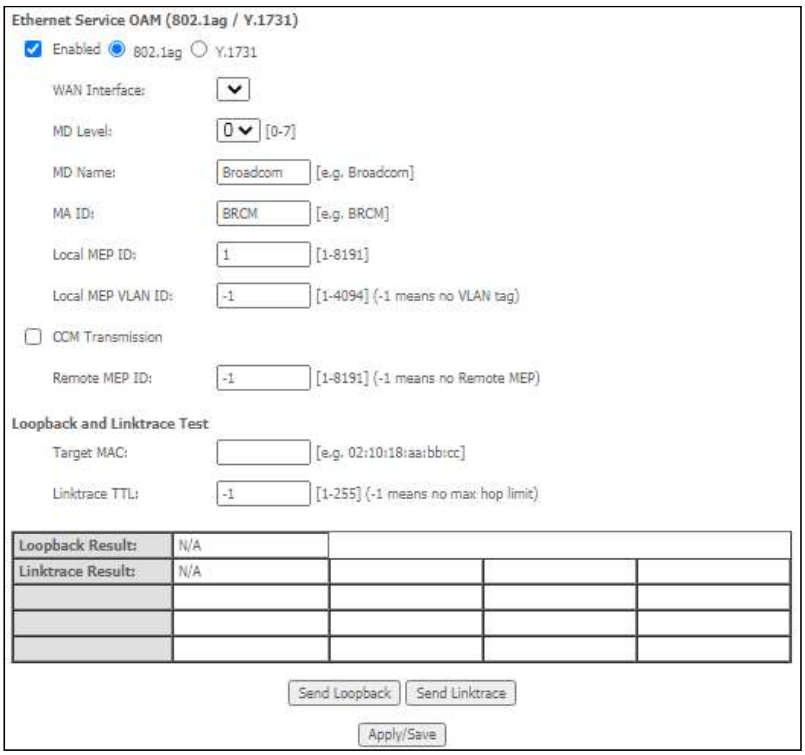
To enable Ethernet Link OAM (802.3 ah), click Enabled to display the full configuration list. At least one option must be enabled for 802.1ah.



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

Active mode	Supports OAM active mode

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



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

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

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

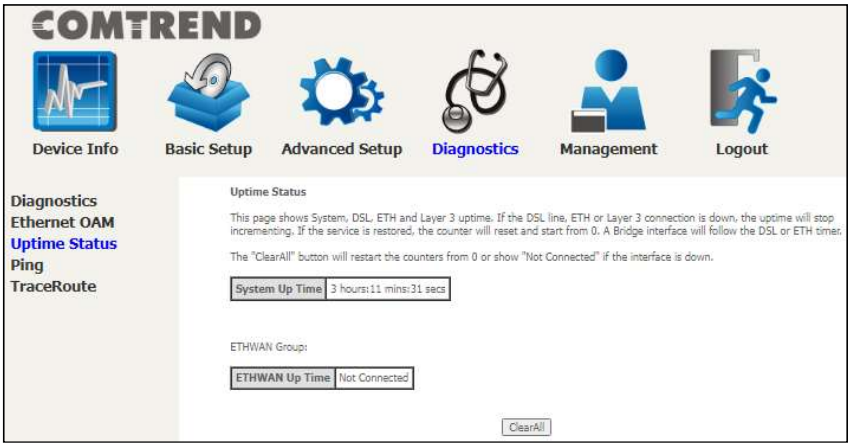
Remote MEP ID	Maintenance association End Point Identifier for the remote receiver

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

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

7.3 Uptime Status

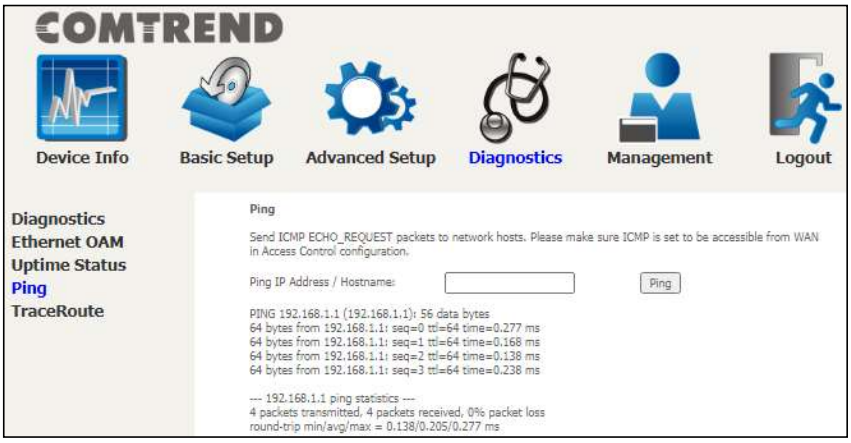
This page shows System, ETH and Layer 3 uptime. If the ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the ETH timer.



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

7.4 Ping

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



7.5 Trace Route

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

Chapter 8 Management

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

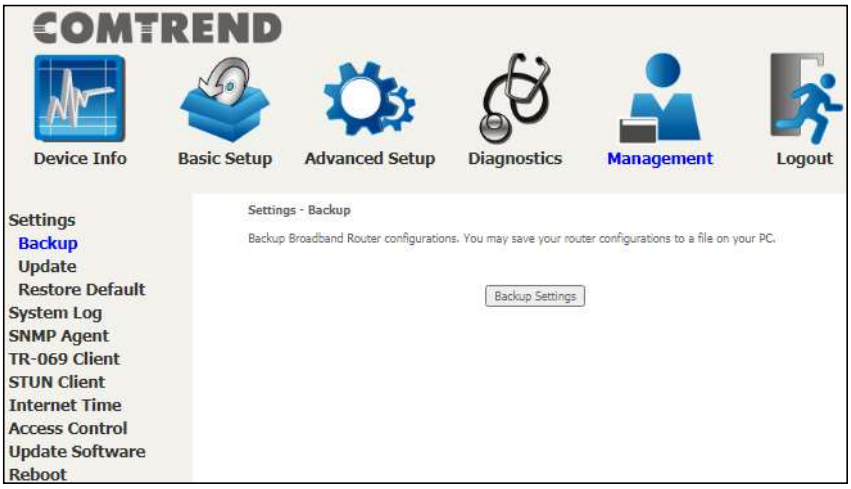
The Management menu has the following maintenance functions and processes:

8.1 Settings

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

8.1.1 Backup Settings

This option recovers configuration files previously saved using **Backup Settings**. Click the Choose File button to locate the backup file. Then click the **Update Settings** button to update your device settings.

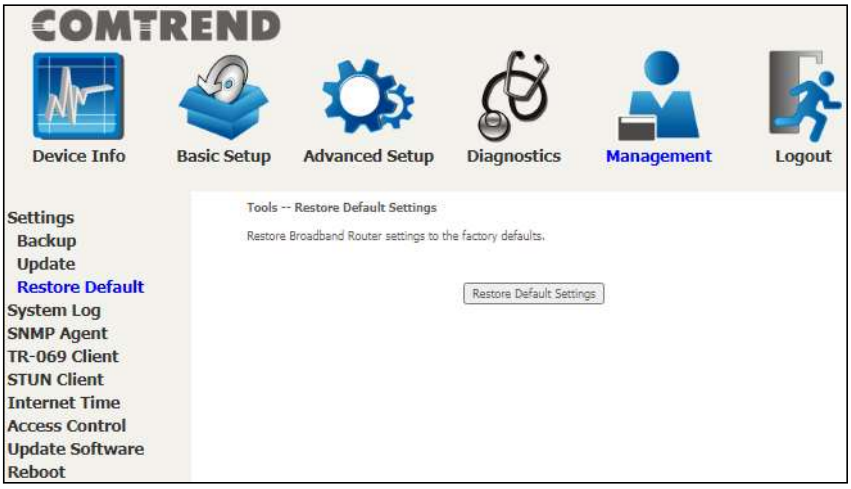


8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Click the **Choose File** button to search for the file, then click **Update Settings** to recover settings.

8.1.3 Restore Default

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



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

Broadband Router Restore

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

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

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

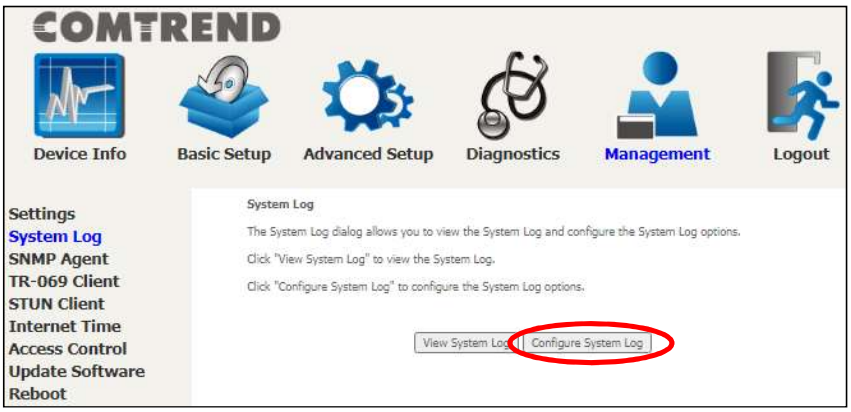
NOTE:	This entry has the same effect as the **Reset** button. The PRT-6351 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the current configuration data will be erased. If the **Reset** button is continuously pressed for more than 60 seconds, the boot loader will erase all configuration data saved in flash memory and enter bootloader mode.

8.2 System Log

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

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

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



STEP 2: Select desired options and click **Apply/Save**.

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

Item	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the **Enable** radio button and then

	click **Apply/Save**.
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the PRT-6351 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

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

System Log

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

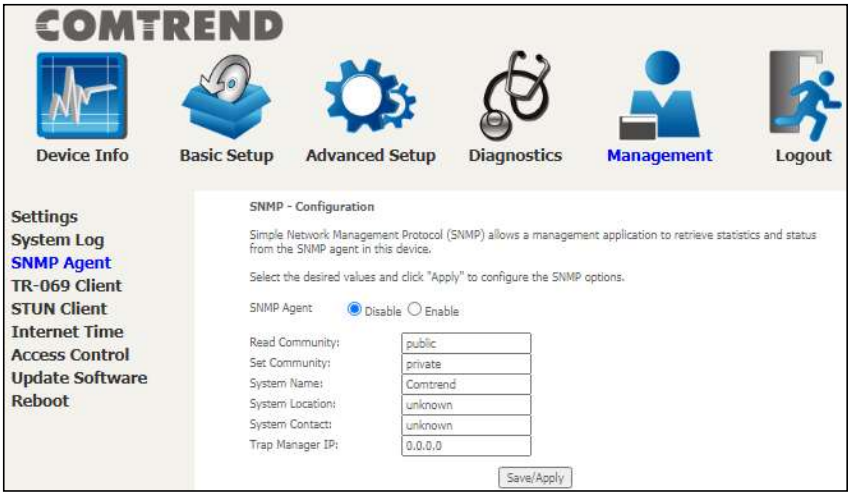
Refresh Close

Click the **Refresh** button to update the system log and click the **Close** button to

remove the current log from the screen.

8.3 SNMP Agent

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

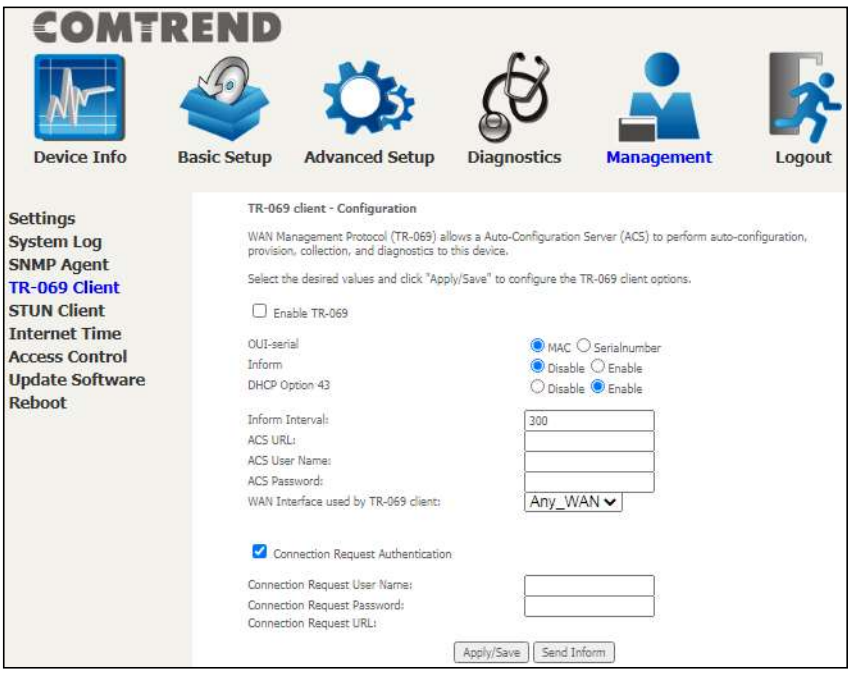


The settings shown above are described below.

Item	Description
SNMP Agent	Enable or Disable the SNMP Agent
Read Community	Default is "public"
Set Community	Default is "private"
System Name	Default is "Comtrend"
System Location	Describes the location of the system (user defined)
System Contact	Describes who should be contacted about the host the agent is running on (user defined)
Trap Manager IP	Trap request supports to monitor and alarm via port 162 from Agent

8.4 TR-069 Client

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



The table below is provided for ease of reference.

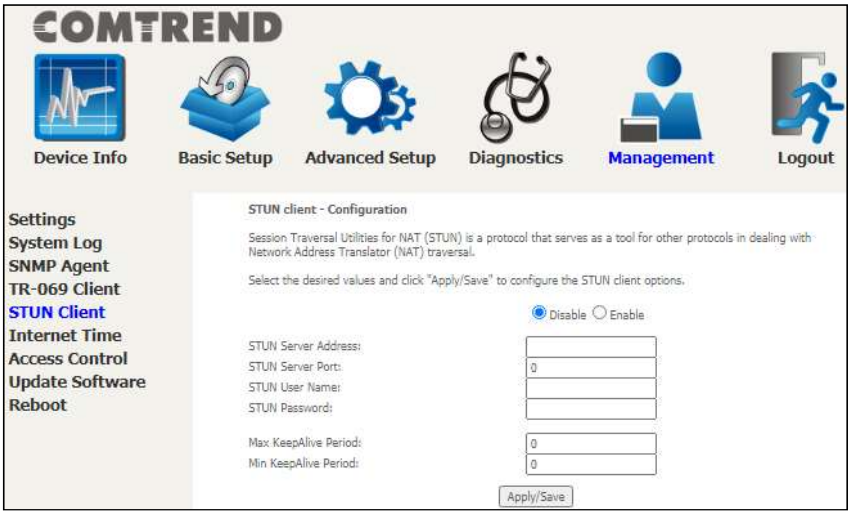
Item	Description
Enable TR-069	Tick the checkbox ☑ to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with the ACS or select serial number to use the router's serial number.
Inform	Disable/Enable TR-069 client on the CPE.
DHCP Option 43	Enable/Disable using DHCP option 43 received from WAN server to configure ACS URL.

Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Connection Request	
Authentication	Tick the checkbox ☑ to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to the router.

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

8.5 STUN Client

Session Traversal Utilities for NAT (STUN) is a protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal.



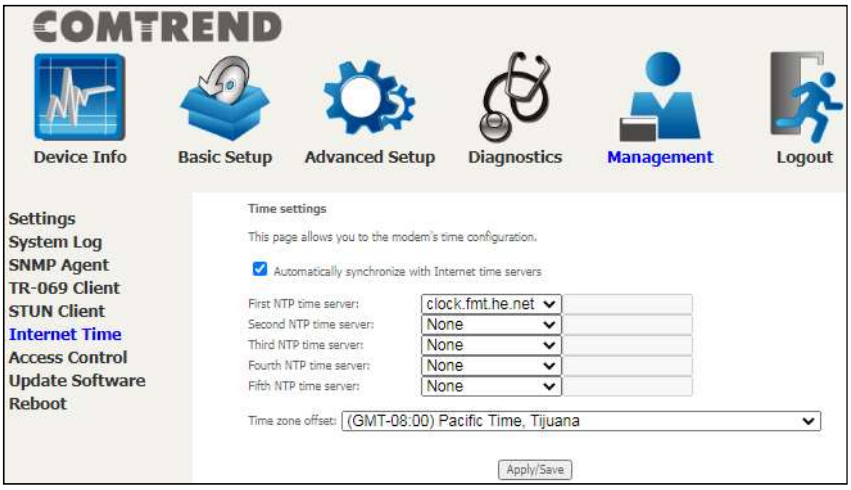
Select the desired values and click the **Apply/Save** button to configure the STUN client options.

The settings shown above are described below.

Item	Description
Disable/Enable	Disable/Enable STUN client.
STUN Server Address	IP address of the STUN server.
STUN Server Port	Service port of the STUN server.
STUN User Name	Account to link to the STUN server.
STUN Password	Password of said account to link to the STUN server.
Max KeepAlive Period	Maximum period to wait for a packet to be received from the STUN server to keep the link alive.
Min KeepAlive Period	Minimum period to send a packet to the STUN server to keep the link alive.

8.6 Internet Time

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



NOTE: Internet Time must be activated to use. See 5.5 Parental Control.
The internet time feature will not operate when the router is in bridged mode, since the router would not be able to connect to the NTP timeserver.

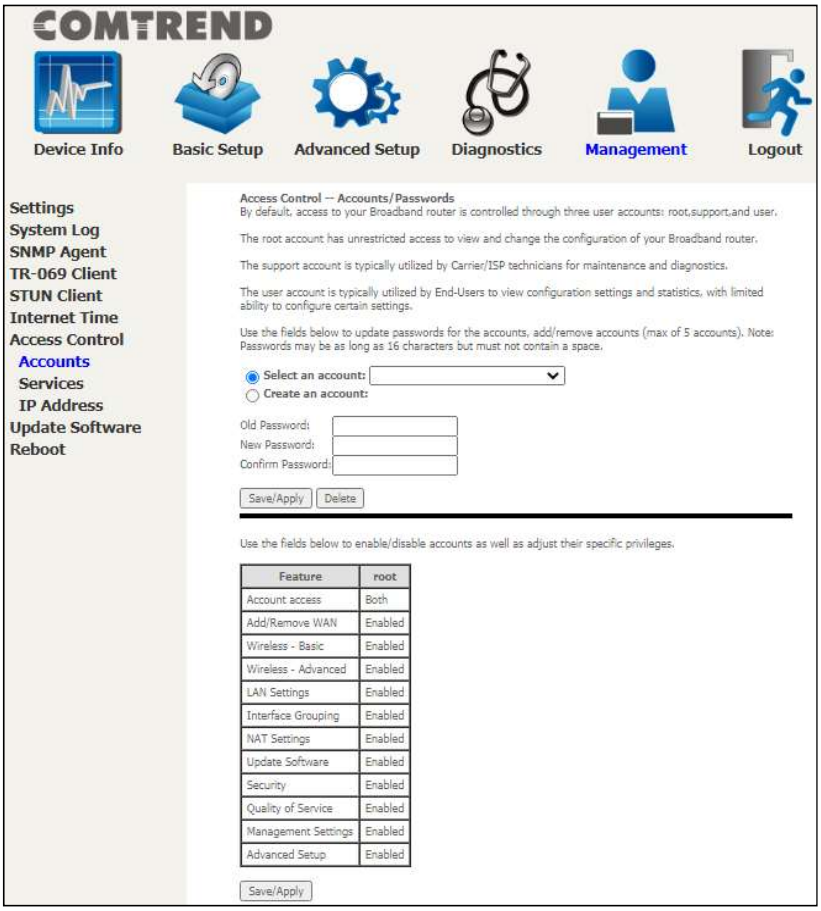
8.7 Access Control

8.7.1 Accounts

This screen is used to configure the user account access passwords for the device. Access to the PRT-6351 is controlled through the following user accounts:

- The root account has unrestricted access to view and change the configuration of your Broadband router.

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

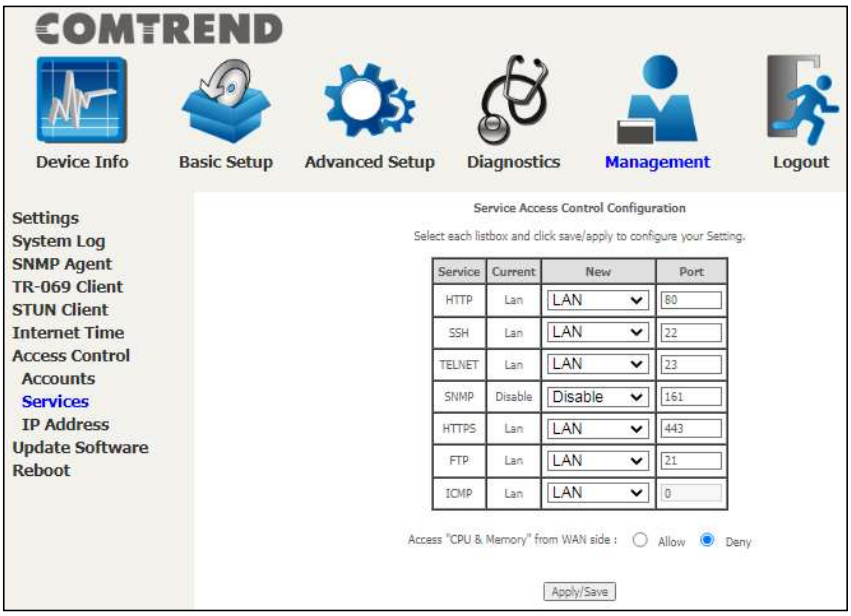


Note: Passwords may be as long as 16 characters but must not contain a space. Click **Save/Apply** to continue.

8.7.2 Services

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

Access "CPU & Memory" from WAN side:This allows the WAN side to access the Device Info CPU & Memory page.

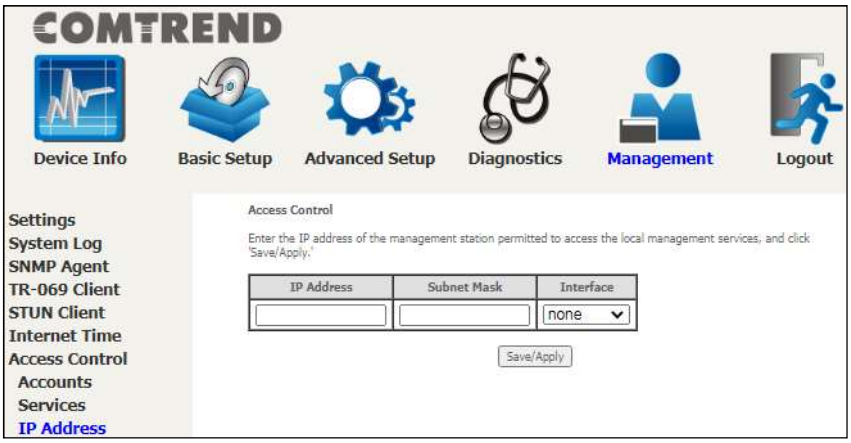


Please note that any Comtrend firmware upgrade will not modify any WiFi parameters (including the WiFi power setting). Comtrend's products follow the market's standard requirements.

8.7.3 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.

8.8 Update Software

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

Please note that any Comtrend firmware upgrade will not modify any WiFi parameters (including the Wi-Fi power setting). Comtrend's products follow the market's standard requirements.

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

STEP 2: Enter the path to the image file location in the box below or click the **Choose File** button to locate the image file.

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.

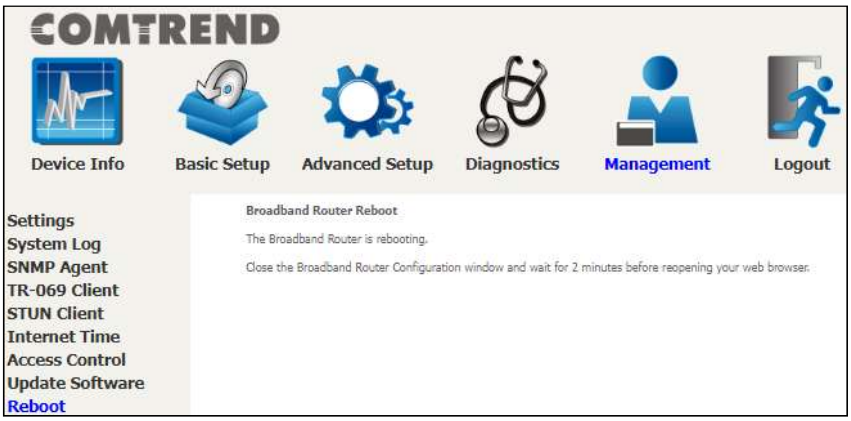
STEP 3: Click the **Update Software** button once to upload and install the file.

NOTE1:	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.
NOTE2:	The Power LED indicates the status of firmware update progress. Please **DO NOT** power off the device when Power LED is flashing or the device will be damaged.

8.9 Reboot

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

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

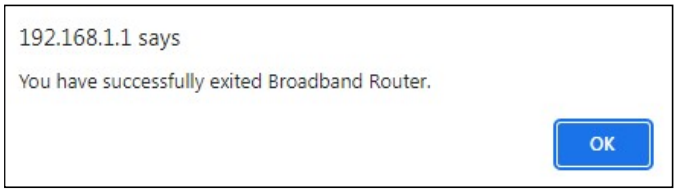


Chapter 9 Logout

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 PRT-6351, 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-45 X 4 for GELAN

· RJ-45 X 1 for 2.5GEWAN

· USB 2.0 X 1

· Reset button X 1

· WiFi on/off X 1

· WPS button X 1

· Internal Antenna X 6 (2.4GHz *2 / 5GHz * 4 / 6GHz * 2)

· Power switch X 1

2.5Gigabit Ethernet

· IEEE 802.3bz

· 2.5G BASE-T, auto-sense

· Support MDI/MDX

Gigabit Ethernet

· IEEE 802.3, IEEE 802.3u IEEE 802.3ab

· 10/100 /1000 BASE-T, auto-sense

· Support MDI/MDX

Software Features

· WAN Type: Dynamic IP/Static IP/PPPoE

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

· Quality of Service: WMM, Bandwidth Control

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

· VPN: PPTP, L2TP, IPSec

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

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

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

· Management: Access Control, Local Management, Remote Management
Internet Protocol: IPv4, IPv6

Management

· TR-069/TR-104/TR-111/TR-181, SNMP, Telnet, Web- Based Management,

Configuration Backup and Restoration

· Software Upgrade via HTTP, TFTP Server, or FTP Server

Wireless

· IEEE 802.11ax, 2.4GHz, 2T2R

Backward compatible with 802.11n/g/b

2412～2462 MHz

· IEEE 802.11ax, 5GHz, 4T4R

Backward compatible with 802.11ac/n/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)

· IEEE 802.11ax, 6GHz, 2T2R

U-NII-5 (5925～6425 MHz)

U-NII-6 (6425～6525 MHz)

U-NII-7 (6525～6875 MHz)

U-NII-8 (6875～7125 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

· Output : USB3.0, ⎓ 900mA

Environment

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

· Operating Humidity: 10%~90% non-condensing

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

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

已註解 **[Trevor1]:** Or this?

· Storage Temperature: -25°C ~65°C (-23°F ~149°F)

Kit Weight

(1* PRT-6351, 1*RJ45 cable, 1*power adapter) = 0.8 kg

NOTE: Specifications are subject to change without notice.

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*

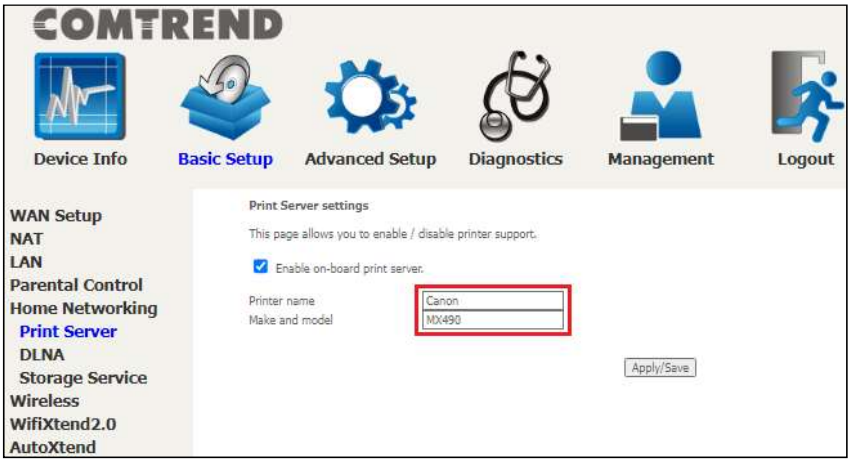
NOTE: The *WAN IP address* can be found on the Device Info → WAN screen

Appendix E - Printer Server

These steps explain the procedure for enabling the Printer Server.

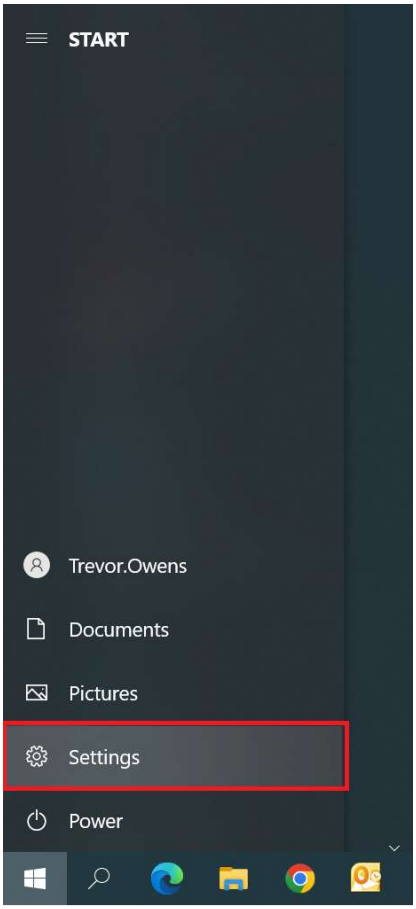
NOTE:	This function only applies to models with an USB host port.

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

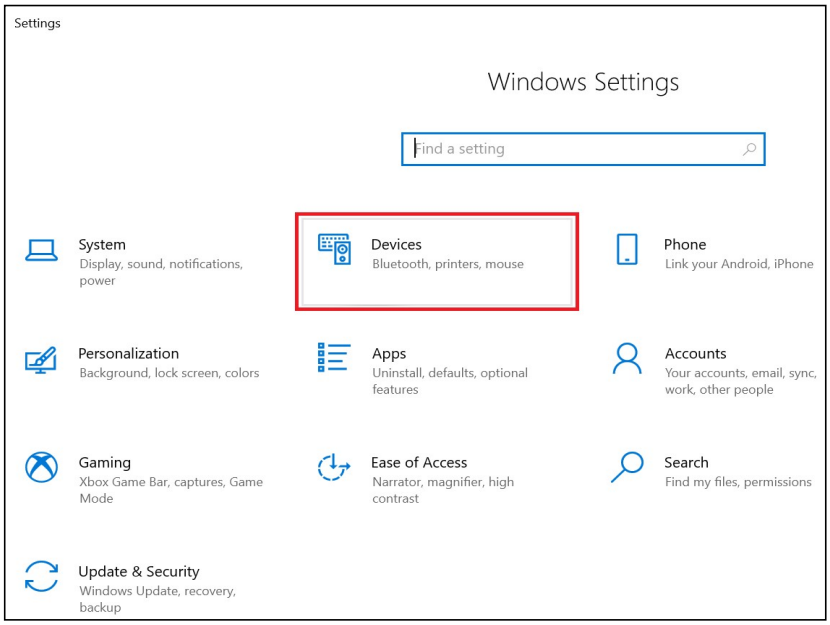


NOTE:	The **Printer name** can be any text string up to 40 characters. The **Make and model** can be any text string up to 128 characters.

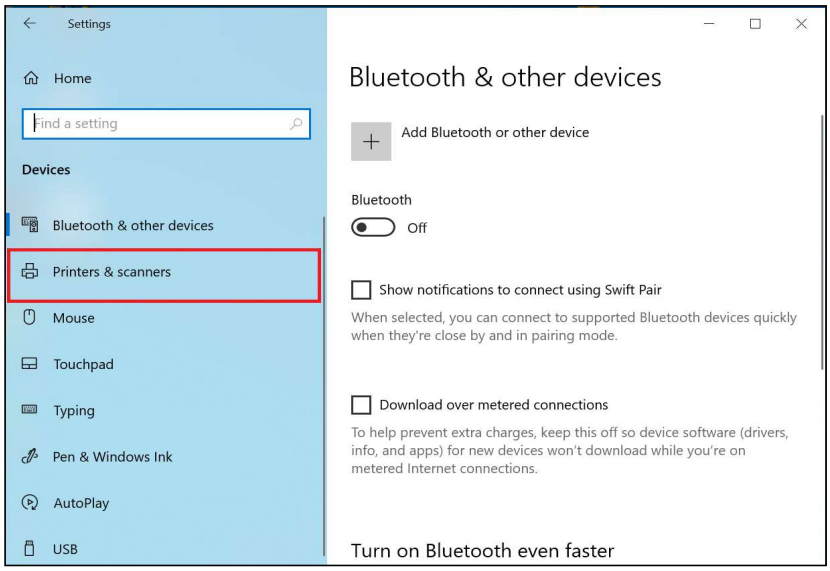
STEP 2: Click the Windows start button. → Then select **Settings**.



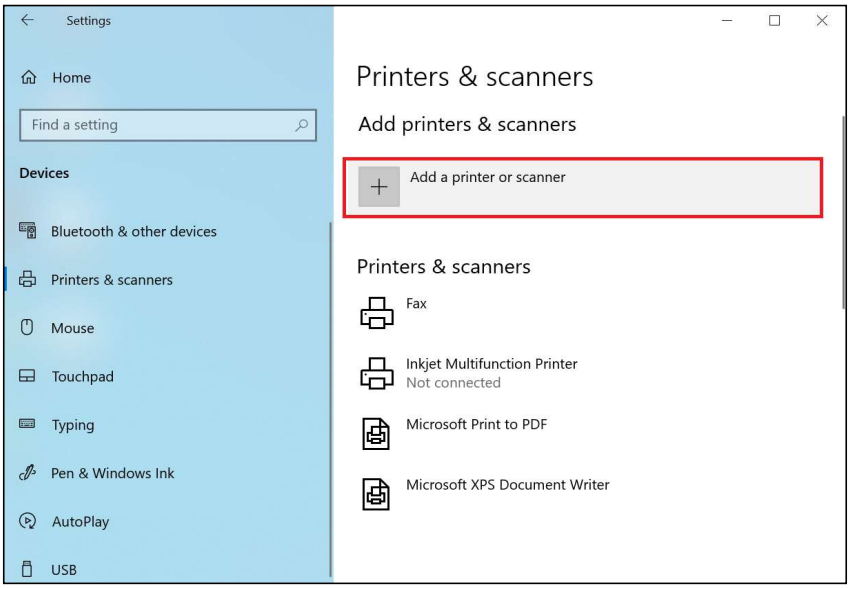
STEP 3: Select **Devices**.



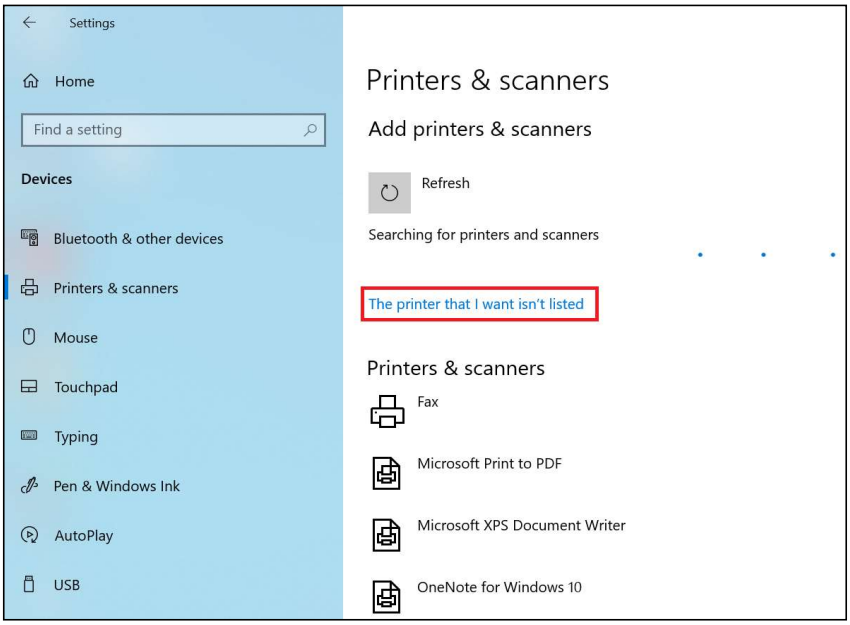
STEP 4: Select **Printers & scanners**.



STEP 5: Select **Add a printer or scanner**.



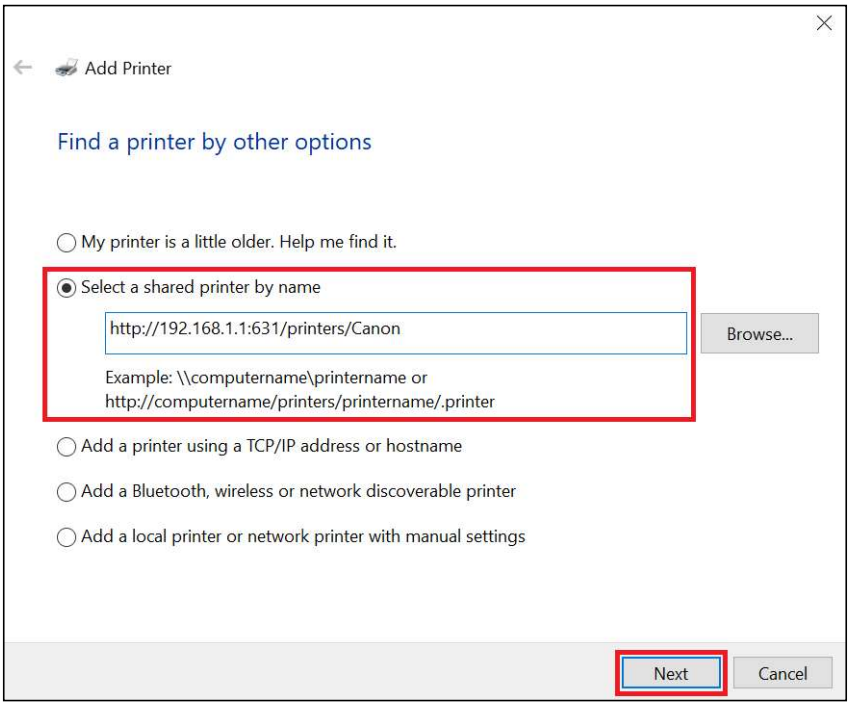
STEP 6: → Select **The printer that I want isn't listed**.



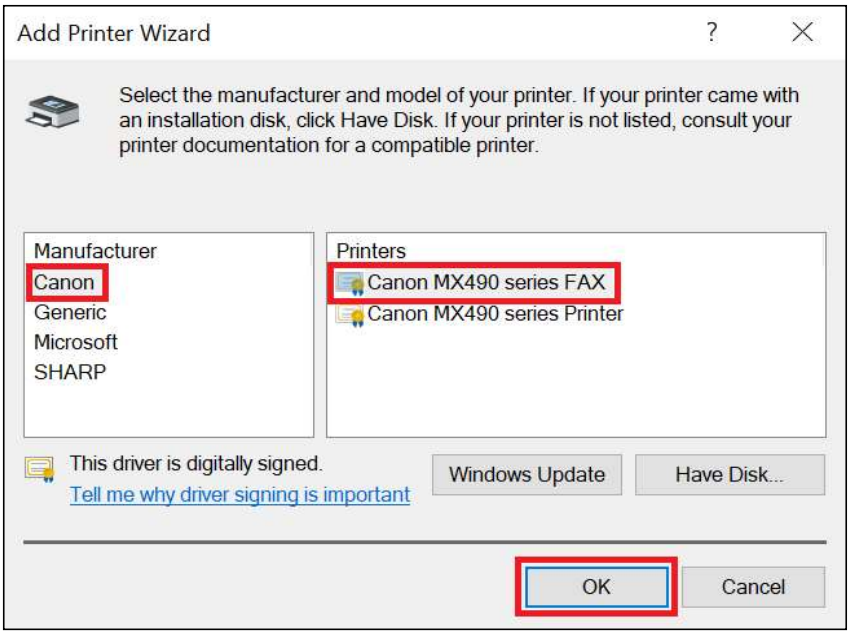
STEP 7: Choose **Select a shared printer by name**. Then input the printer link and click **Next**.

http://LAN IP:631/printers/Canon

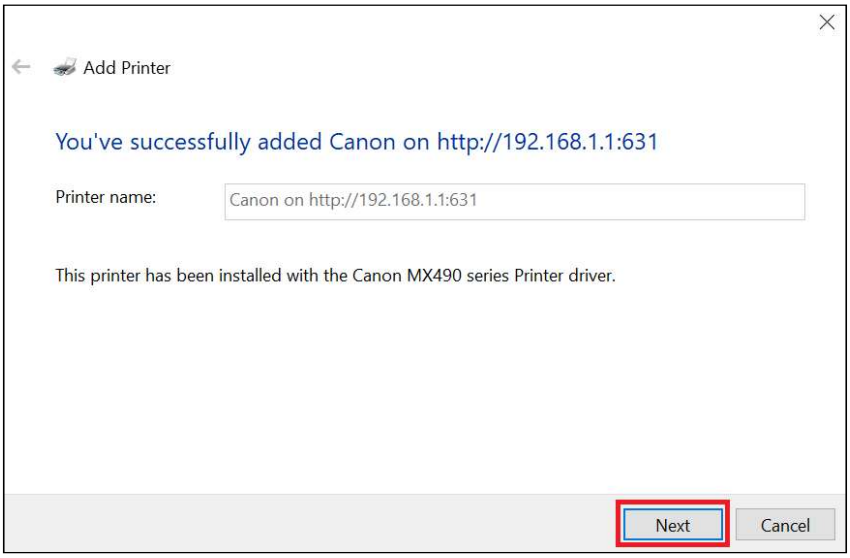
NOTE:	The printer name must be the same name inputted in the WEB UI "Print Server settings" as in step 1.



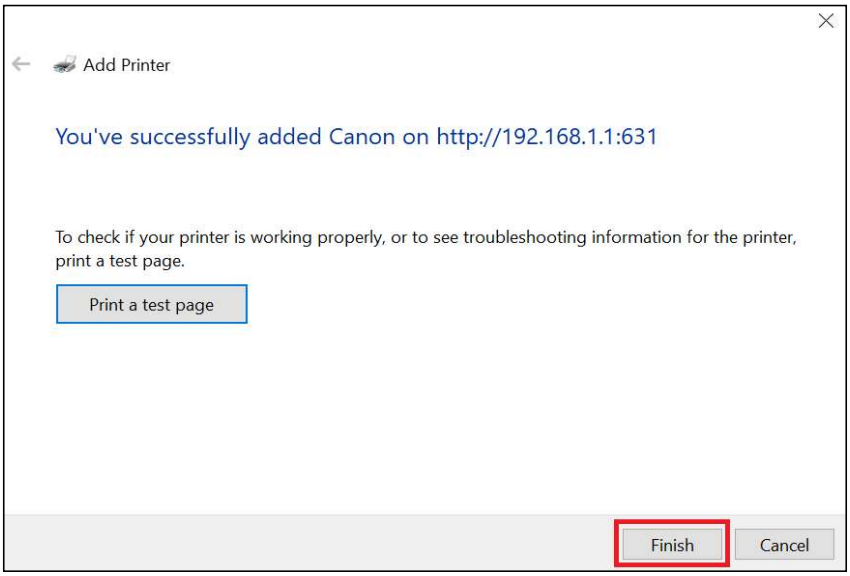
STEP 8: Select the manufacturer → and model of your printer → then, click **OK**.



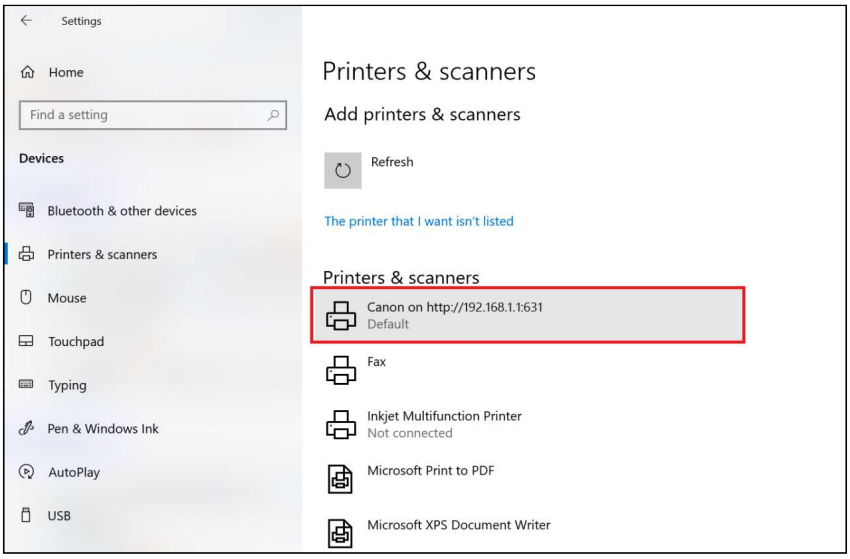
STEP 9: The printer has been successfully installed. Click the **Next** button.



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



STEP 11: Go to → **Settings** → **Devices** → **Printers & scanners** 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

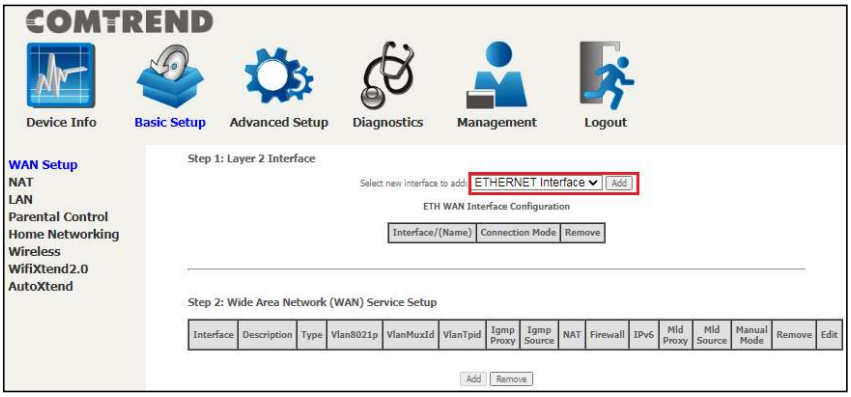
Every layer2 interface operates in Multi-Service Connection (VLAN MUX) mode, which supports multiple connections over a single interface. Note that PPPoA and IPoA connection types are not supported for Ethernet WAN interfaces. After adding WAN connections to an interface, you must also create an Interface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

F1.1 Ethernet WAN Interface

The PRT-6351 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.



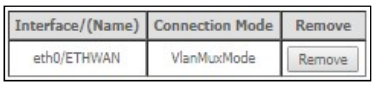
STEP 2: Click **Add** to proceed to the next screen.

This table is provided here for ease of reference.

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

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



Interface/(Name)	Connection Mode	Remove
eth0/ETHWAN	VlanMuxMode	Remove

To add a WAN connection go to Section F2 ~ WAN Connections.

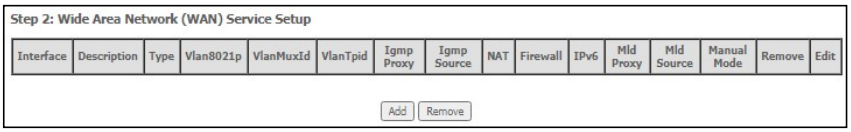
F2 ~ WAN Connections

The PRT-6351 supports one WAN connection for each interface, up to a maximum of 16 connections.

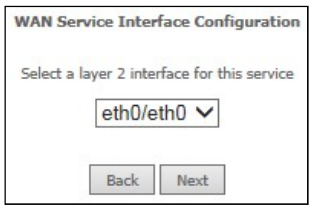
To setup a WAN connection follow these instructions.

STEP 1: Go to Basic Setup

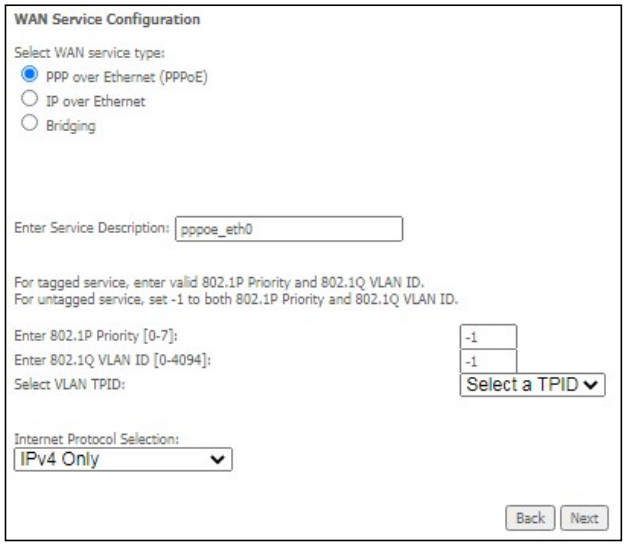
→ WAN Setup.



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



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.



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.

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

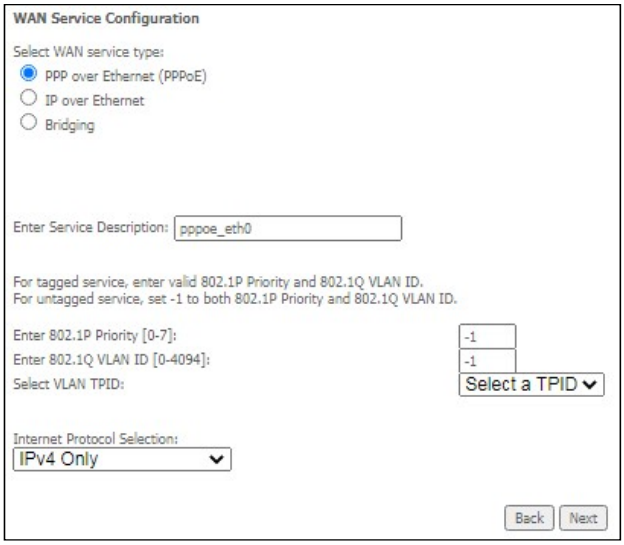
STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(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 (Not Supported)
(5) For IP over ATM (IPoA) – IPv4 (Not Supported)
(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 (Not Supported)
(10) IPoA – IPv6 (Not Supported)

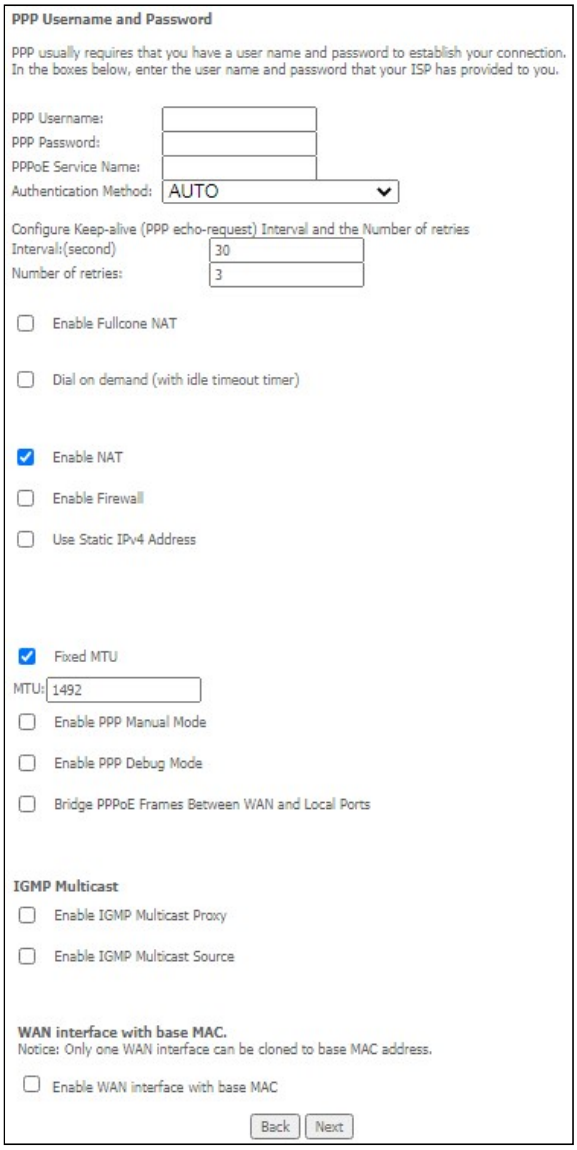
The subsections that follow continue the WAN service setup procedure.

F2.1 PPP over ETHERNET (PPPoE) – IPv4

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



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.



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

The settings shown above are described below.

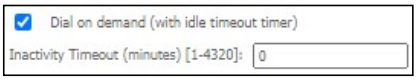
PPP SETTINGS

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.

CONFIGURE KEEP-ALIVE
Configures the interval and number of keep alive packets (PPP echo-request) sent by the device for the PPP connection.
Interval (second): Time between sending out each PPP echo-request packet.
Number of retries: Number of retries before PPP connection is dropped.

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 PRT-6351 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.



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 MANUAL MODE
Use this button to manually connect/disconnect PPP sessions.

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.

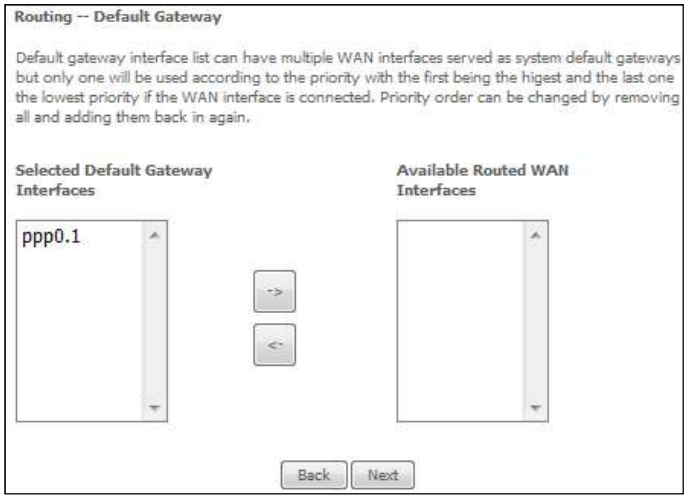
BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(This option is hidden when PPP IP Extension is enabled)
When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The PRT-6351 supports pass-through 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.

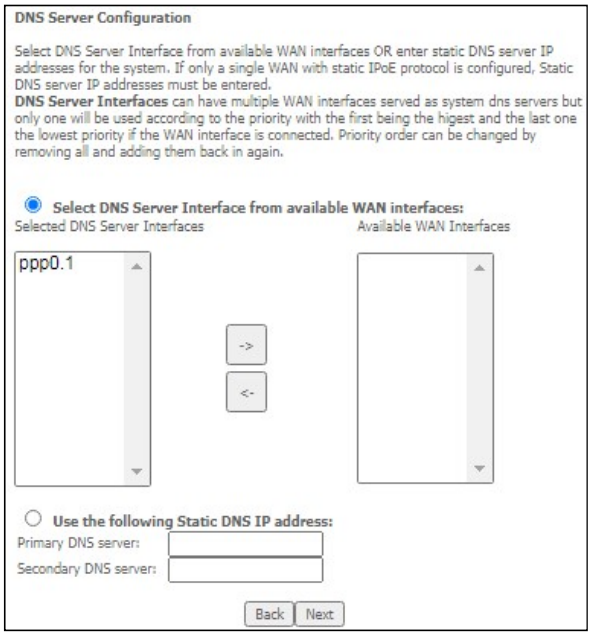
Enable WAN interface with base MAC
Tick the checkbox ☑ to enable this function which will hook up the br0 MAC address to this very WAN service.

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



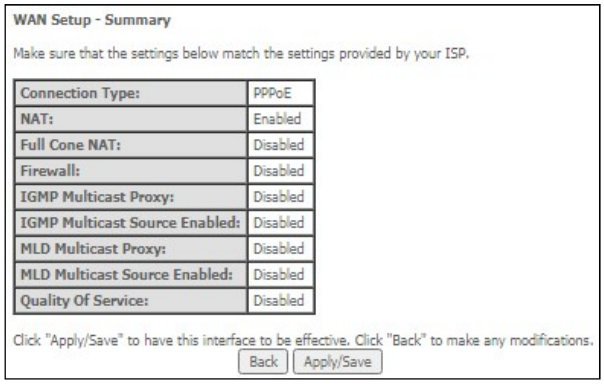
Click **Next** to continue or click **Back** to return to the previous step.

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.



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

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



WAN Setup - Summary

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

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

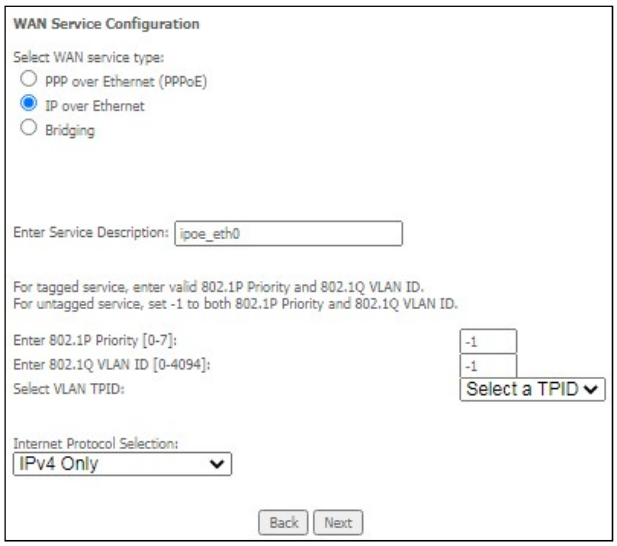
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

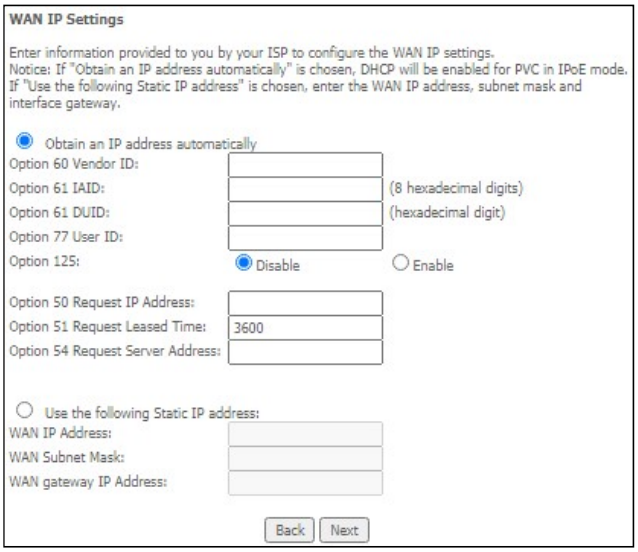
After clicking **Apply/Save**, the new service should appear on the main screen.

F2.2 IP over ETHERNET (IPoE) – IPv4

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



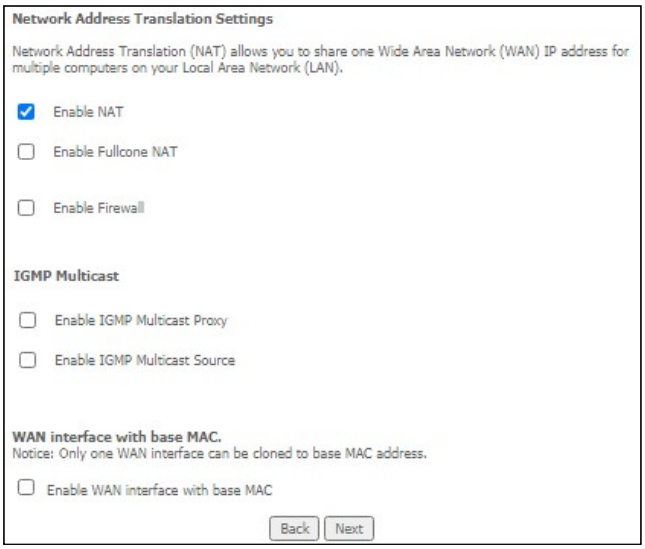
STEP 2: The WAN IP settings screen provides access to the DHCP server settings.
You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can use the **Static IP address** method instead to assign WAN IP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



With reference to different options, please contact your ISP (Internet Service Provider) for more details.

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.



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.

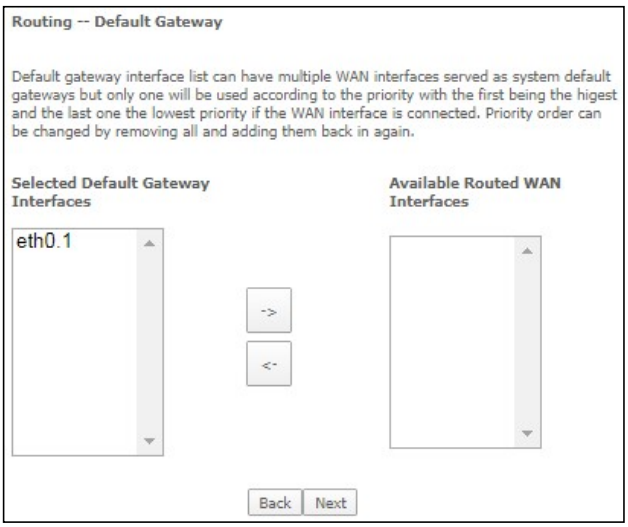
ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

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.

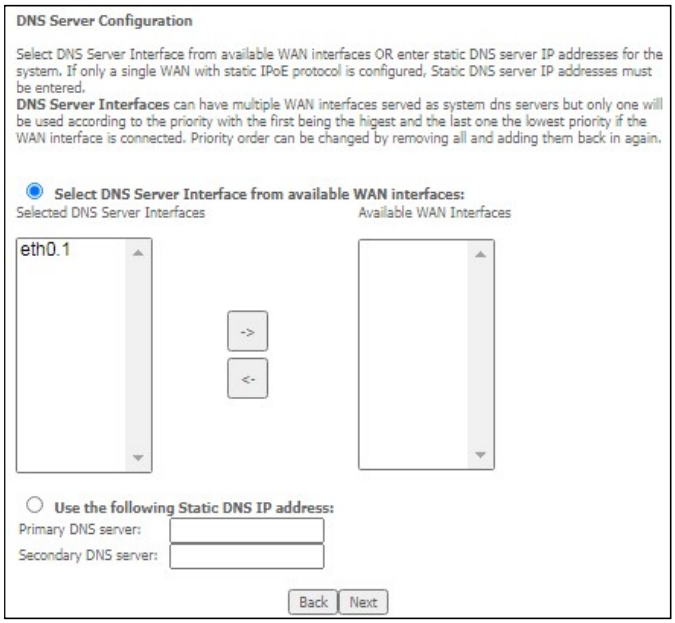
Enable WAN interface with base MAC
Tick the checkbox ☑ to enable this function which will hook up the br0 MAC address to this very WAN service.

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



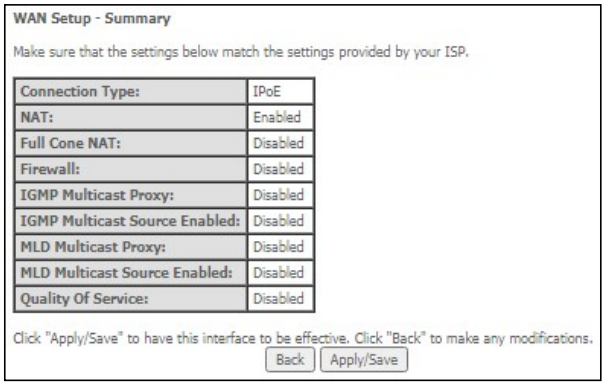
Click **Next** to continue or click **Back** to return to the previous step.

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.



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

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



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

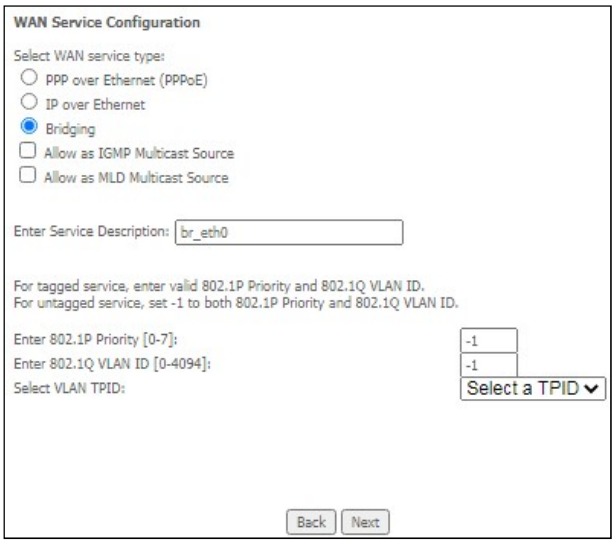
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

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

F2.3 Bridging – IPv4

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



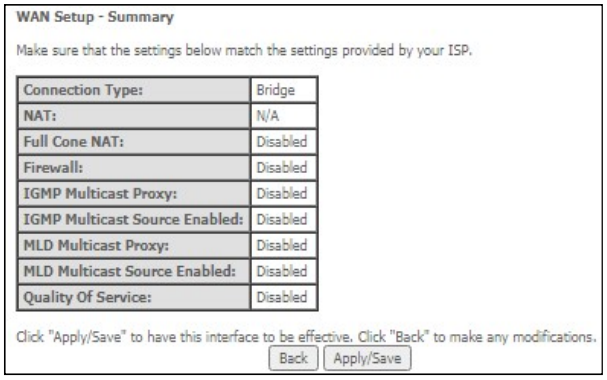
Allow as IGMP Multicast Source

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

Allow as MLD Multicast Source

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

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



WAN Setup - Summary

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

Connection Type:	Bridge
NAT:	N/A
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.

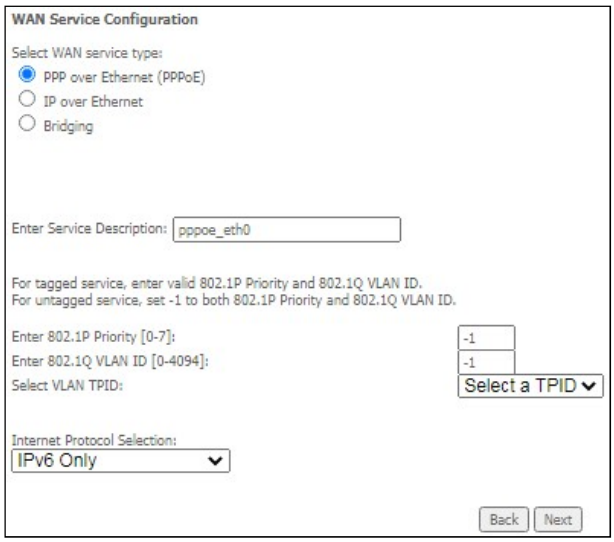
Back Apply/Save

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

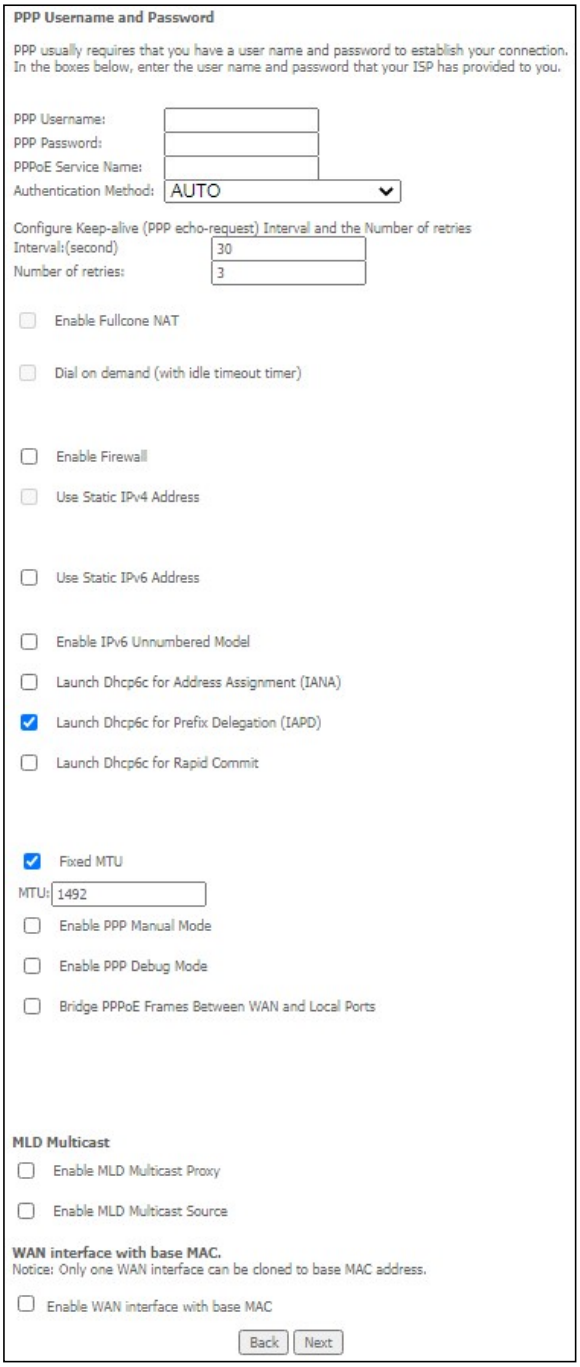
NOTE:	If this bridge connection is your only WAN service, the PRT-6351 will be inaccessible for remote management or technical support from the WAN.

F2.4 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**.



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.

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.

CONFIGURE KEEP-ALIVE
Configures the interval and number of keep alive packets (PPP echo-request) sent by the device for the PPP connection.
Interval (second): Time between sending out each PPP echo-request packet.
Number of retries: Number of retries before PPP connection is dropped.

ENABLE FULLCONE NAT
Not available for IPv6.

DIAL ON DEMAND
Not available for IPv6.

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
Not available for IPv6.

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 MANUAL MODE
Use this button to manually connect/disconnect PPP sessions.

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.

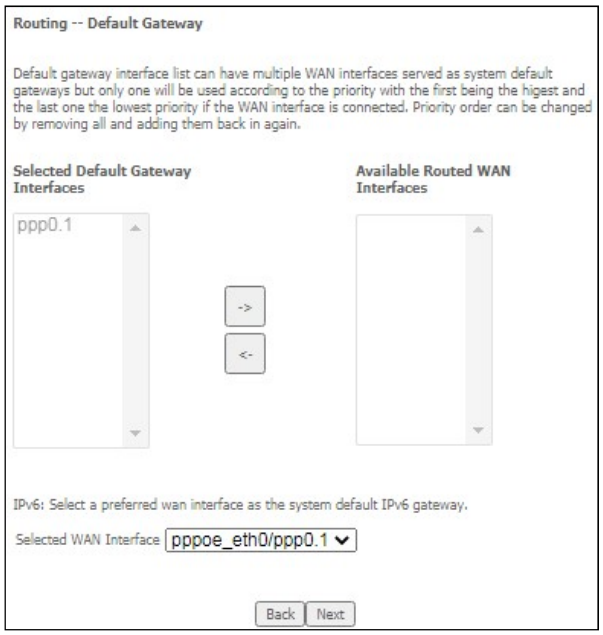
BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(This option is hidden when PPP IP Extension is enabled)
When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The PRT-6351 supports pass-through 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.

Enable WAN interface with base MAC
Tick the checkbox ☑ to enable this function which will hook up the br0 MAC address to this very WAN service.

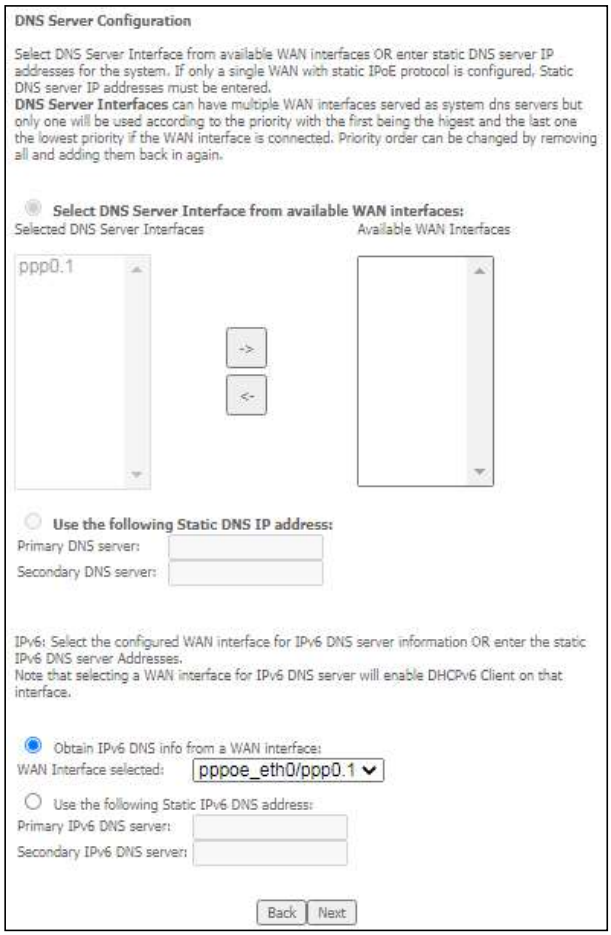
STEP 3: Choose an interface to be the default gateway. Also, select a preferred WAN interface as the system default IPv6 gateway (from the drop-down box).



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

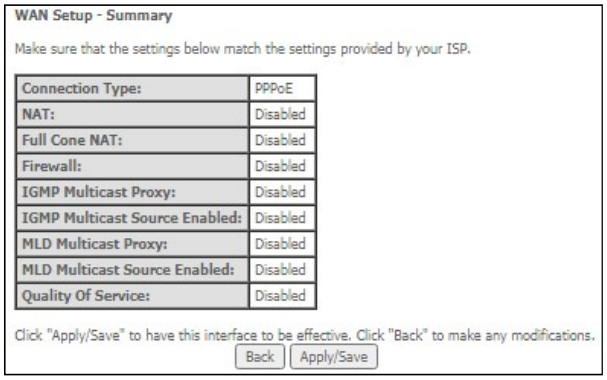
STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

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.



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

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



WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	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

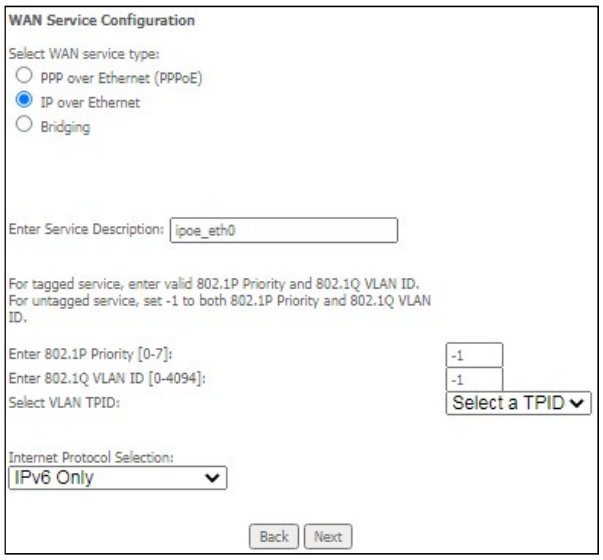
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

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

F2.5 IP over ETHERNET (IPoE) – IPv6

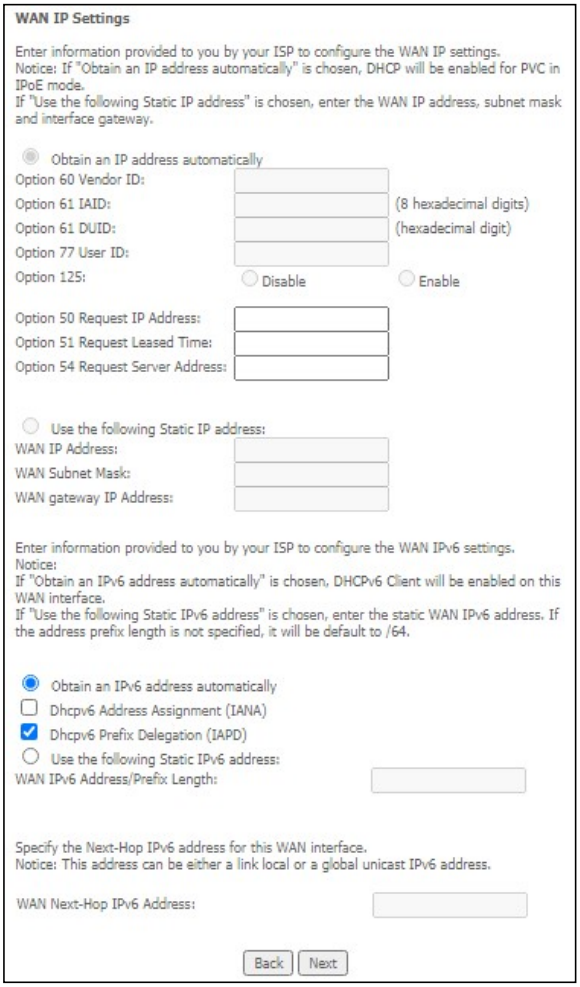
STEP 1: Select the IP over Ethernet radio button and click **Next.** Then select IPv6 only from the drop-down box at the bottom off the screen and click **Next**.



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.



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

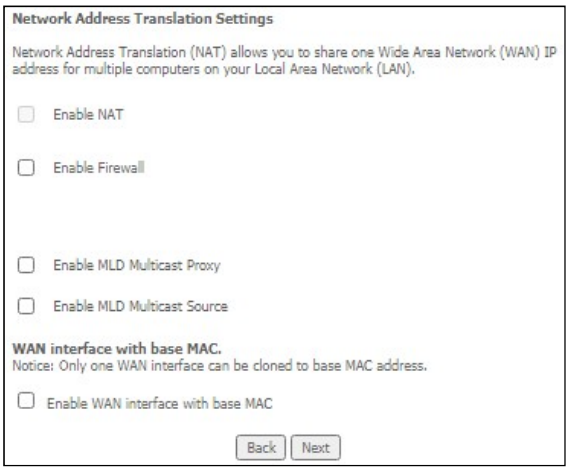
DHCP6C FOR ADDRESS ASSIGNMENT (IANA)
The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there 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.

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 ☑.



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

ENABLE NAT
Not available for IPv6.

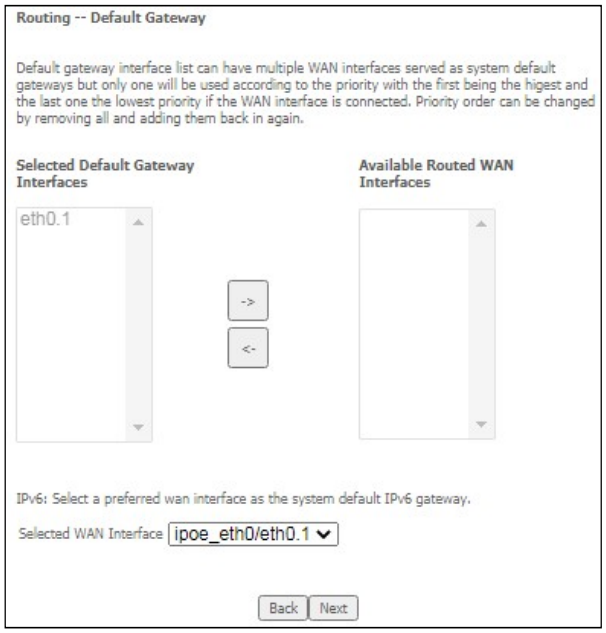
ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

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.

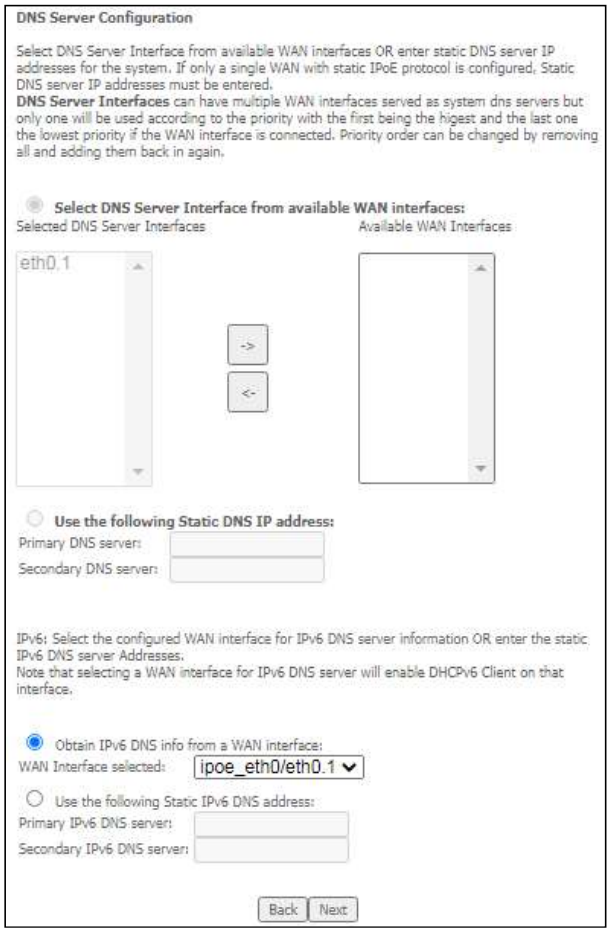
Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

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).



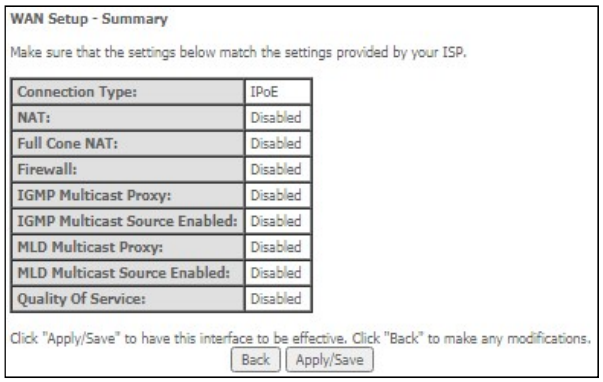
Click **Next** to continue or click **Back** to return to the previous step.

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.



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

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



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.

Back Apply/Save

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