
HT-178 User Manual

VER: 1.0

heights.telnet.com

Contents

1	Safety Precautions	1
2	Overview	2
2.1	Application	2
2.2	Features	2
2.3	Standards Compatibility and Compliance	3
3	Hardware Description and Installation	4
3.1	Hardware Description	4
3.1.1	Front Panel	4
3.1.2	Rear Panel and Side Panel	6
3.1.3	Connecting the Device	9
4	PC Network Configuration and Login	10
4.1	PC Network Configuration	10
4.2	Logging In to the Router	10
5	Web-Based Management	10
5.1	Device Information	11
5.1.1	Summary	11
5.1.2	WAN	12
5.1.3	Statistics	13
5.1.4	LAN	13
5.1.5	WAN Service	13
5.1.6	ARP	14
5.2	Advanced Setup	14
5.2.1	Layer2 Interface	15
5.2.2	WAN Service	17
5.2.3	IPV6	26
5.2.4	LAN Configuration	27
5.2.5	VPN	29
5.2.6	NAT	31
5.2.7	MAC Filtering	34
5.2.8	Firewall	36
5.2.9	Quality of Service	39
5.2.10	Routing	43

5.2.11	DNS	44
5.2.12	UPnP	46
5.2.13	Dnsmasq	47
5.2.14	Print Server	48
5.2.15	DLNA	48
5.2.16	Storage Service	49
5.2.17	IPSec	52
5.2.18	Multicast	54
5.3	Wireless	55
5.3.1	Radio	55
5.3.2	Media	58
5.3.3	SSID	60
5.3.4	Security	60
5.3.5	WPS	65
5.4	Diagnostics	66
5.4.1	Diagnostics	66
5.4.2	Ping	67
5.4.1	Traceroute	67
5.5	Management	68
5.5.1	Settings	69
5.5.2	System Log	70
5.5.3	Security Log	71
5.5.4	Voice	72
5.5.5	Sniffer	95
5.5.6	Internet Time	95
5.5.7	Access Control	97
5.5.8	Update Software	99
5.5.9	Reboot	100
6	Q&A	101

1 Safety Precautions

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exists or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

2 Overview

The Router is designed to provide a simple and cost-effective Internet connection for a private Ethernet. The Router combines high-speed Internet connection, IP routing for the LAN connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

The Router is easy to install and use. The Router connects to an Ethernet LAN or computers via standard Ethernet ports. The connection is made using ordinary telephone line with standard connectors. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

Network and Router management is done through the web-based management interface that can be accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

2.1 Application

- Home gateway
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

2.2 Features

- User-friendly GUI for web configuration
- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages

- Downloadable flash software updates
- Support for up to 8 PPPoE sessions
- Support RIP v1 & RIP v2
- IP routing and bridging
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Universal plug-and-play(UPnP)
- Web filtering
- Management and control
Web-based management (WBM)

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u

3 Hardware Description and Installation

Note:

The figures in this document are for reference only.

3.1 Hardware Description

3.1.1 Front Panel



Figure 1 Front panel

The following table describes the indicators on the front panel.

USB	Functions
Green	Device connected
Green blinking	DATA

User Manual

Lan ports	Functions
Green	link/act
Green blinking	Blinking speed will adapt According to transferring DATA

SFP	Functions
Green	link/act

Wan ethernet	Functions
Green	link/act
Green blinking	Blinking speed will adapt According to transferring DATA

Internet	Functions
Green	Connected
Red	authentication failed/no answer from DHCP(connection without dialer)

FXS	Functions
Green	Line is registered
Green Slow blinking	Calling, Talking, Ringing

POWER	Functions
Green	Start complete
Red	In CFE mode

2.4G WIRELESS	Functions
Green	Function open
Green off	Function close
Green blinking	DATA

5G WIRELESS	Functions
Green	Function open
Green off	Function close
Green blinking	DATA

3.1.2 Rear Panel and Side Panel



Figure 2 Rear Panel



Figure 3 Side panel

The following table describes the interfaces or the buttons.

Interface	Description
LAN	RJ-45 port, for connecting the router to a PC or another network device.
USB3.0	Connect the devices to router through USB port.
WAN	Device management port
Reset	Press the button for at least 1 second and then release it. System restores the factory default settings.
Power	Power interface, for connecting the power adapter.
On/Off	Power switch.

User Manual

Interface	Description
SFP	Insert SFP module to access network through fiber optic cable
WiFi	Wifi switch

Warning:

*Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the **Reset** button gently for 1 second with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.*

3.1.3 Connecting the Device

- Step 1** Connect the **WAN** port of the router with a telephone cable.
- Step 2** Connect the **LAN** port of the router to the network card of the PC through an Ethernet cable.
- Step 3** Plug the power adapter to the wall outlet and then connect the other end of it to the **Power** port of the router.

heights telecom

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address .

The IP address should be set 10.10.0.X.

4.2 Logging In to the Router

To log in to the Router, do as follows:

Open a Web browser on your computer.

Enter **https://100.100.100.100** (the default IP address of the Router) in the address bar. The login page appears.

Enter the the password. It should be the last six digits of SN



Figure 4 Login page

After logging in to the Router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

5 Web-Based Management

This chapter describes how to use Web-based management of the Router, which allows you to configure and control all of Router features and system parameters in a user-friendly GUI.

5.1 Device Information

Choose **Device Info**, and the submenus of **Device Info** are shown as below:



5.1.1 Summary

Choose **Device Info > Summary**, and the following page appears.

Device Info

Board ID:	BCM963178DVT_Hs
Model Name:	HT-178AX-V2
MAC Address:	00:B8:C2:D6:DD:5D
Serial Number:	021018000001
Build Timestamp:	20230919_0744
Software Version:	2.0.0.3-HT-178AX-V2-OS-OPENINFRA-debug
Bootloader Version:	U-Boot 2019.07
DSL PHY and Driver Version:	A2pv6L047f1.d27n
Wireless Driver Version:	17.10.188.75
Voice Service Version:	Voice
Uptime:	0D 0H 35M 26S

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	10.10.0.138
Default Gateway:	Inactive
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
LAN IPv6 Global Address:	
Default IPv6 Gateway:	eth4.1
Date/Time:	Tue Sep 19 08:19:47 2023



This page displays the device information such as the board ID, software version, and the information of your WAN connection such as the upstream rate and the LAN address.

5.1.2 WAN

Choose **Device Info > WAN** and the following page appears.

User Manual

WAN Info															
Interface	Description	Type	Vlan/Port	IPv6	Ipmp Proxy	Ipmp Source	MLD Proxy	MLD Source	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address	Update
eth1 (Ethernet)	100_eth1_eth1	Port	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	ServiceDown		ServiceDown		00:00:00:00

This page displays the information of the WAN interface, such as the connection status, and the IP address.

5.1.3 Statistics

5.1.4 LAN

Choose **Device Info > Statistics > LAN** and the following page appears.

Statistics -- LAN&WLAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	5091	29	0	4256	25	0	4	8494	118	0	0	8430	117	0	1	
wl1.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

In this page, you can view the statistical information about the received and transmitted data packets of the Ethernet.

Click **Reset Statistics** to restore the values to zero and recount them.

5.1.5 WAN Service

Choose **Device Info > Statistics > WAN Service** and the following page appears.

Statistics -- WAN

Interface	Description	Received							Transmitted								
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth4.1	cpe-ipintf-4	346165	2807	0	0	15941	94	2658	55	322085	4616	0	0	648	8	4607	1

Reset Statistics

In this page, you can view the statistical information about the received and transmitted data packets of the WAN interface.

Click **Reset Statistics** to restore the values to zero and recount them. Route

Choose **Device Info > Route** and the following page appears.

Device Info -- Route

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

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
100.100.100.0	0.0.0.0	255.255.255.0	U	0	eth4.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0

In this page, you can view the route table information.

5.1.6 ARP

Choose **Device Info > ARP** and the following page appears.

Device Info -- ARP

IP address	Flags	HW Address	Device
100.100.100.106	Complete	48:02:2a:f0:92:a3	eth4.1

In this page, you can view the MAC address and IP address information of the device connected to the router.

5.2 Advanced Setup

Choose **Advanced Setup** and the submenus of **Advanced Setup** are shown as below:

Advanced Setup

Layer2 Interface

WAN Service

LAN

VPN

NAT

Security

Firewall

Quality of Service

Routing

DNS

DSL

UPnP

Dnsmasq

Print Server

DLNA

Storage Service

IP Tunnel

Certificate

Power Management

Multicast

5.2.1 Layer2 Interface

5.2.1.1 ETH Interface

Choose **Advanced Setup** > **Layer2 Interface** > **ETH Interface** . In this page, you can add or remove to configure DSL ETH Interfaces.

User Manual

Device Info
Advanced Setup
Layer2 Interface
ADH Interface
PTM Interface
ETH Interface
WAN
USB Modem Service
ZPW
LAN
VPI
NAT
NAC Filtering

ETH WAN Interface Configuration
Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove
eth4/eth4	VlanMuxMode	<input type="checkbox"/>
eth5/eth5	VlanMuxMode	<input type="checkbox"/>

Add Remove

Click **Add** to add ETH Interface and the following page appears.

ETH WAN Configuration

This screen allows you to configure a ETH port .

WAN Only Interfaces: eth4,eth5

Select a ETH port:

eth5/eth5 v

Back

Apply/Save

In this page, you can configuration the ETH interface Click Apply/Save.

Click **Apply/Save** to save the configuration, and return the following page:

ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove
eth4/eth4	VlanMuxMode	<input type="checkbox"/>
eth5/eth5	VlanMuxMode	<input type="checkbox"/>

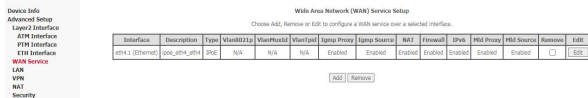
Add

Remove

If you want to remove this Interface, please select the **Remove** check box and click **Remove**.

5.2.2 WAN Service

Choose **Advanced Setup > WAN Service**, and the following page appears.



In this page, you are allowed to add, remove, or edit a WAN service.

5.2.2.1 Adding a PPPoE WAN Service by GUI

This section describes the steps for adding the PPPoE WAN service.

- Step1** In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM interface for this WAN service.)

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

eth4/eth4 ▼

Back

Next

Step2 In this page, you can select a ETH Interface for the WAN service. After selecting the ATM interface, click **Next** to display the following page.

User Manual

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

Enter interface name:

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

Enter 802.1P Priority [0-7]:

(-1 means no VLAN)

Enter 802.1Q VLAN ID [0-4094]:

(-1 means no VLAN)

Select VLAN TPID:

Internet Protocol Selection:

Step3 In this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. Click **Next** to display the following page.

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:
MTU[576-1492]:

- Enable NAT
- Enable Fulkone NAT
- Enable Firewall
- Enable Default Gateway
- Use Static IPv4 Address
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

- Enable IGMP Multicast Proxy
- Enable IGMP Multicast Source

Step4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.

- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable NAT:** NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port.
- **Enable Fullcone NAT:** NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Enable Firewall :** Used to control whether remote access is allowed
- **Enable Default Gateway :** Set that wan connection as the default gateway
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Enable PPP Debug Mode:** Enable or disable this function.
- **Bridge PPPoE Frames Between WAN and Local Ports:** Enable or disable this function.
- **Enable IGMP Multicast Proxy:** If you want PPPoE mode to support IPTV, enable it.
- **Enable IGMP Multicast Source:** if enable it, allow this interface accept the Multicast Source.

Step5 After setting the parameters, click **Next** to display the following page.

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
DHCP Snooping:	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.

User Manual

- Step6** In this page, it displays the information about the PPPoE settings. Click **Apply/Save** to save and apply the settings.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Name	Interface	Description	Type	Vlan802Ip	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mid Proxy	Mid Source	Remove	Edit
InterfaceStaticMgmt	eth4.1	cpe-ipref-4	IPvE	N/A	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
Internet	ppp0-2	cpe-ipref-5	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

Adding a MER (IPoE) WAN service by GUI

This section describes the steps for adding the MER WAN service.

- Step1** In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM interface for this WAN service.)

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

eth4/eth4 ▼

Back

Next

Step2 Select an ETH Interface, and then click **Next** to display the following page.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

Enter interface name:

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

Enter 802.1P Priority [0-7]:

(-1 means no VLAN)

Enter 802.1Q VLAN ID [0-4094]:

(-1 means no VLAN)

Select VLAN TPID:

Select a TPID ▾

Internet Protocol Selection:

Step3 In this page, select the WAN service type to be IP over Ethernet, enter the service description for this service. After finishing setting, click **Next** to display the following page.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IADID: (8 hexadecimal digits)

Option 61 DUVID: (16 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:

Primary DNS server:

Secondary DNS server:

User Manual

Step4 In this page, you may modify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP. Click **Next** and the following page appears.

Note:

*If selecting **Obtain an IP address automatically**, DHCP will be enabled for PVC in MER mode.*

*If selecting **Use the following Static IP address**, please enter the WAN IP address, subnet mask and gateway IP address.*

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
- Enable Default Gateway
- Enable DHCP Snooping

MTU SETTING

MTU[576-1500]:

IGMP Multicast

- Enable IGMP Multicast Proxy
- Enable IGMP Multicast Source

[Back](#) [Next](#)

Step5 In this page, click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	IPvE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
DHCP Snooping:	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](#)

User Manual

Step6 In this page, it displays the information about the IPOE settings. Click **Apply/Save** to save and apply the setting.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Name	Interface	Description	Type	Vlan8021p	VlanMaxId	VlanType	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mid Proxy	Mid Source	Remove	Edit
InterfaceStaticMgmt	eth4.1	cpe-ipint-4	IPOE	N/A	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
Internet	atm0.2	cpe-ipint-5	IPOE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

Add Remove

5.2.2.2 Adding a Bridge WAN service by GUI

This section describes the steps for adding the Bridge WAN service.

Step1 In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM interface for this WAN service.) Click the **Add** button to display the following page.

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

eth4/eth4 ▼

Back

Next

Step2 Select the proper ETH Interface and then click **Next** to display the following page.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging
 Allow as IGMP Multicast Source
 Allow as MLD Multicast Source

Enter Service Description:

Enter interface name:

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

Enter 802.1P Priority [0-7]:

(-1 means no VLAN)

Enter 802.1Q VLAN ID [0-4094]:

(-1 means no VLAN)

Select VLAN TPID:

Select a TPID ▾

[Back](#) [Next](#)

Step3 In this page, you can select the WAN service type, and modify the service description for this service. After finishing setting, click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	Bridge
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
DHCP Snooping:	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.

[Back](#) [Apply/Save](#)

Step4 In this page, it displays the information about the bridge settings. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

User Manual

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Name	Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mid Proxy	Mid Source	Remove	Edit
InterfaceStaticMgmt	eth4.1	cpe-serial-4	IPoE	N/A	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit
Internet	atrn0.1	cpe-serial-5	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

5.2.3 IPV6

Choose **Advanced Setup > IPV6**, and the following page appears.

Device Info
Advanced Setup
Layer2 Interface
WAN
USB Modem Service
IPV6
LAN
VPN
NAT
MAC Filtering

IPV6 enable or disable control setting
This page allows you to enable / disable IPV6 support.

Enable IPV6 working.

In the **IPV6 enable or disable control setting** page, Click **Apply/Save** to save and apply the settings.

5.2.4 LAN Configuration

5.2.4.1 IPv4 Autoconfiguration

Choose **Advanced Setup > IPv4 Autoconfig**, and the following page appears.

Local Area Network (LAN)

LAN IP:	10.10.0.138
LAN mask:	255.255.255.0
Start IP Address:	10.10.0.1
End IP Address:	10.10.0.64
Primary DNS server:	10.10.0.138
Secondary DNS server:	0.0.0.0
Leased Time (seconds):	86400

In this page, only show the settings. User can't config it.

5.2.4.2 IPv6 Autoconfiguration

Click **Advanced Setup > LAN > IPv6 Autoconfig**, and the following page appears.

IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64.

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required): fe80::2221:12ff:fe25:18

IPv6 LAN Applications

Enable DHCPv6 Server

Stateless

Stateful

Start interface ID: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour): 24

Enable RADVD

Enable ULA Prefix Advertisement

Randomly Generate

Statically Configure

Prefix:

Preferred Life Time (hour): 0

Valid Life Time (hour): 0

Enable MLD Snooping

Save/Apply

In this page, you can set an IP address for the DSL IPv6 router, enable the DHCPv6 server, enable RADVD and enable the MLD snooping function.

- **Enable DHCPv6 Server:** WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.
- **Enable RADVD:** The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
- **Enable MLD Snooping:** Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

After finishing setting, click the **Save/Apply** button to apply the settings.

5.2.5 VPN

5.2.5.1 L2TP Client

Choose **Advanced Setup > VPN > L2TP Client** the following page appears.



Step1 In the **L2TP Client Side PPP Connection** page. Click the **Add** button to display the following page.

Add a L2TP Client Side PPP Connection (PPPoE/L2TP WAN Service)

Tunnel Name:

L2TP Server Ip Address:

Wan Interface:

Next

Step2 In this page, you can modify the **Tunnel Name**, **L2TP Server Ip Address**, **Wan Interface**.

- **Tunnel Name:** The name of the Tunnel
- **L2TP Server Ip Address:** Set the address of the L2TP server.
- **Wan Interface:** Select an existing wan connection, and then build an L2TP channel on this wan connection.

Step3 After setting the parameters, click **Next** to display the following page.

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:

- Enable Firewall
- Enable Default Gateway

Back Next

Step4 In this page, you can modify the **PPP Username, PPP Password, Enable Firewall, Enable Default Gateway.**

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **Enable Firewall :** Used to control whether remote access is allowed
- **Enable Default Gateway :** Set that wan connection as the default gateway

Step5 After setting the parameters, click **Next** to display the following page.

WAN Setup - Summary

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

Connection Type:	L2TP
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
DHCP Snooping:	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.

Step6 In this page, it displays the information about the PPPoE settings. Click **Apply/Save** to save and apply the settings.

5.2.6 NAT

5.2.6.1 Port Forwarding

Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The Port Forwarding can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

Choose **Advanced Setup > NAT > Port Forwarding**, and the following page appears.

NAT - Port Forwarding Setup
 Port Forwarding allows you to direct incoming traffic from the WAN interface (identified by its Protocol and External Port) to the Internal server with a private IP address on the LAN interface. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.
 Note: An IPv6 address is not editable if the IPv6 NAT function is turned off.
 Note: An IPv6 address is not editable if the IPv6 function of the interface is turned off.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IPv4 Address	Server IPv6 Address	WAN Interface	Resource

In this page, you are allowed to add or remove a Port Forwarding entry.

To add a Port Forwarding, do as follows:

Step 1 Click the **Add** button to display the following page.

NAT - Port Forwarding
 Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for the service to the specified server (NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start").
 Note: IPv6 address will prohibit edit if the NAT function of IPv6 is turned off.
 Note: IPv6 address will prohibit edit if the IPv6 function of interface is turned off.
 Remaining number of entries that can be configured: 32

Use Interface:

Service Name:

Select a Service

Custom Service:

Server IPv4 Address:

Server IPv6 Address:

External Port Start	External Port End	Protocol	Internal Port Start	External Port End
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		
		TCP v		

- **Use interface:** Select an interface that you want to configure.
- **Select a Service:** Select a proper service in the drop-down list.
- **Custom Server:** Enter a new service name to establish a user service type.
- **Server IPv4 Address:** Assign an IP address to virtual server.
- **Server IPv6 Address:** Assign an IP address to virtual server.

- **External Port Start:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **External Port End:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Protocol:** You may select TCP/UDP, TCP, or UDP in the drop-down list.
- **Internal Port Start:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Internal Port End:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

Step 2 After finishing setting, click **Save/Apply** to save and apply the settings.

5.2.6.2 Port Triggering

Some applications need some ports to be opened in the firewall for the remote access. When an application initializes a TCP/UDP to connect to a remote user, port triggering dynamically opens the open ports of the firewall.

Choose **Advanced Settings > NAT > Port Triggering**, and the following page appears.

NAT -- Port Triggering Setup

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

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

In this page, you may add or remove an entry of port triggering. Click the **Add** button to display the following page.

User Manual

NAT -- Port Triggering

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

Remaining number of entries that can be configured:32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

- **Use interface:** Select an interface that you want to configure.
- **Select an application:** Select a proper application in the drop-down list.
- **Custom application:** Manually define an application.
- **Trigger port Start:** The start port number that LAN uses to trigger the open port.
- **Trigger port End:** The end port number that LAN uses to trigger the open port.
- **Trigger Protocol:** Select the application protocol. You may select TCP/UDP, TCP, or UDP.
- **Open Port Start:** The start port number that is opened to WAN.
- **Open Port End:** The end port number that is opened to WAN.
- **Open Protocol:** Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

After finishing setting, click **Save/Apply** to apply the settings.

Note:

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

5.2.6.3 DMZ Host

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. Set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by firewall.

Choose **Advanced Setup > NAT > DMZ host** to display the following page.

NAT -- DMZ Host

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

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

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

DMZ Host IPv4 Address:

DMZ Host IPv6 Address:

In this page, enter the IP address of the DMZ host.

After finishing the settings, click the **Apply/Save** button to apply the settings.

If you want to clear the DMZ function of the host, please delete the IP address of the host in the field of **DMZ Host IP Address**, and then click the **Apply/Save** button.

5.2.7 MAC Filtering

In some cases, you may want to manage Layer2 MAC address to block or permit a computer within the home network. When you enable MAC filter rules, the Router serves as a firewall that works at layer 2.

Note:

MAC filtering is only effective on ATM PVCs configured in bridge mode.

Choose **Advanced Setup > MAC Filtering** and the following page appears.

User Manual

MAC Filtering Setup

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

MAC Filtering Policy For Each Interface:

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

Interface	Policy	Change
atm0.1	FORWARD	<input type="checkbox"/>

Change Policy

Choose Add or Remove to configure MAC filtering rules.

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

Add Remove

In this page, you can add or remove the MAC filtering rule. You may change the MAC filtering policy from **FORWARDED** to **BLOCKED** by clicking the **Change Policy** button.

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

Add MAC Filter

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

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Save/Apply

- **Protocol Type:** Select the proper protocol type.
- **Destination MAC Address:** Enter the destination MAC address.
- **Source MAC Address:** Enter the source MAC address.
- **Frame Direction:** The direction of transmission frame.

User Manual

- **WAN Interface (Configured in bridge mode only):** Select the proper WAN interface in the drop-down list.

After finishing setting, click **Apply/Save** to save and apply the filtering rule.

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

URL List Type: Exclude Include

Address	Port	Weekdays	Start	Stop	Remove
www.google.com	80	Mon,Tue,Wed,Thu	00:00	23:59	<input type="checkbox"/>

5.2.8 Firewall

Choose **Advanced Setup > Firewall**, and the following page appears.

Device Info
Advanced Setup
Layer2 Interface
WAN
USB Modem Service
IPv6
LAN
VPI
NAT
MAC Filtering
Parental Control
Firewall
Quality of Service
Routing
DNS
DSL
IPoP
DNS Proxy
Print Server
DLNA
Storage Service

Firewall – This function only processes forwarded packets, and does not process packets sent to the device itself.
Note: Only one level rule can take effect at a time
Note: If you need to create a level instance, you must first create a chain

Enabled

Level

Name	Chain Name	DefaultPolicy	Enable	Remove
------	------------	---------------	--------	--------

Chain - Rule

Chain Name	Source Interface	Dest Interface	Ip Version	SourceIP	DestIP	SourceIP(v6)	DestIP(v6)	Protocol	Source Port	Source Port Range Max	Dest Port	Dest Port Range Max	Action	Enable	Remove
------------	------------------	----------------	------------	----------	--------	--------------	------------	----------	-------------	-----------------------	-----------	---------------------	--------	--------	--------

In this page, you are allowed to add, remove, or edit a level and Chain rule.

Note: If you need to create a level instance, you must first create a chain

5.2.8.1 Adding a Chain Rule

This section describes the steps for adding the chain rule.

- Step1** In the **Chain - Rule** page, click the **Add** button to display the following page.

Firewall -- Add

Note: An IPv4 address is uneditable if the NAT function of IPv4 is turned off.

Note: An IPv6 address is uneditable if the IPv6 function of the interface is turned off.

Enabled

Chain Name:

Source Interface:

Dest Interface:

Action:

IP Version:

Dest IPv4 Address:

Source IPv4 Address:

Dest IPv6 Address:

Source IPv6 Address:

Protocol:

Source Port:

Source Port Range Max:

Dest Port:

Dest Port Range Max:

Step2 In this page, you can modify follow parameters.

- **Chain Name:** The name of the chain.
- **Source Interface:** Select an interface which the packet receive.
- **Dest Interface:** Select the interface from which the packet is sent.
- **Action:** Set the processing action for the packets matching the rule..Accept or Drop.
- **IP Version:** IP Version.
- **Dest IPv4 Address:** Dest IPv4 Addresss of packet.
- **Source IPv4 Address :** Source IPv4 Address of packet.
- **Dest IPv6 Address:** Dest IPv6 Addresss of packet.
- **Source IPv6 Address :** Source IPv6 Address of packet.
- **Protocol:** TCP or UDP
- **Source Port:** Source Port
- **Source Port Range Max:** Source Port Range Max
- **Dest Port:** Dest Port
- **Dest Port Range Max:** Dest Port Range Max
-

Step3 After setting the parameters, Click **Apply/Save** to save and apply the settings.

Chain	Rule	Chain Name	Source Interface	Dest Interface	In Version	SourceIP	DestIP	SourceIPv6	DestIPv6	Protocol	Source Port	Source Port Range Max	Dest Port	Dest Port Range Max	Action	Enable	Remove
test		test	eth0	eth0.2	IPv4	192.168.1.11	192.168.1.12			TCP	20	30	20	30	Accept	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Apply](#) [Add](#) [Remove](#)

5.2.8.2 Adding a Level Rule

This section describes the steps for adding the Level rule.

Step1 In the **Level** page, click the **Add** button to display the following page.

Firewall Level -- Add

Enable:

Level name:

Select Chain:

DefaultPolicy:

Step2 In this page, you can modify follow parameters.

- **Enable** : enable this level.
- **Level name**:The name the level.
- **Select Chain**: Select a chain to associate this level.
- **DefaultPolicy**: Default Policy.

Step4 After setting the parameters, Click **Apply/Save** to save and apply the settings.

Name	Chain Name	DefaultPolicy	Enable	Remove
<input type="text" value="testlevel"/>	<input type="text" value="test"/> ▾	<input type="text" value="Drop"/> ▾	<input checked="" type="radio"/>	<input type="checkbox"/>

5.2.9 Quality of Service

Enabling QoS

Choose **Advance Setup > Quality of Service** and the following page appears.

QoS -- Queue Management Configuration

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

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

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

Enable QoS

Select **Enable QoS** to enable QoS and configure the default DSCP mark.

User Manual

QoS -- Queue Management Configuration

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

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

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

Enable QoS

Select Default DSCP Mark

Apply/Save

In this page, enable the QoS function and select the default DSCP mark. After finishing setting, click **Apply/Save** to save and apply the settings.

Note:

If the **Enable QoS** checkbox is not selected, all QoS will be disabled for all interfaces. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Queue Configuration

Choose **Advanced Setup > Quality of Service > QoS Queue**, and the following page appears.

User Manual

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.

In PTM mode, maximum 8 queues can be configured.

For each Ethernet interface, maximum 8 queues can be configured.

For each Ethernet WAN interface, maximum 8 queues can be configured.

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

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

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

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

Note: Ethernet LAN queue configuration only takes effect when all the queues of the interface have been configured.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate (bps)	Min Bit Rate(bps)	Burst Size (bytes)	Enable	Remove
LAN Q8	1	eth1	8	1/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q7	2	eth1	7	2/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q6	3	eth1	6	3/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q5	4	eth1	5	4/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q4	5	eth1	4	5/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q3	6	eth1	3	6/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q2	7	eth1	2	7/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN Q1	8	eth1	1	8/SP						<input checked="" type="checkbox"/>	<input type="checkbox"/>

In this page, you can enable, add or remove a QoS rule.

Note:

The lower integer value for precedence indicates the higher priority.

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

QoS Queue Configuration

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

Name:

Enable:

Interface:

- **Name:** Enter the name of QoS queue.
- **Enable:** Enable or disable the QoS queue.
- **Interface:** Select the proper interface for the QoS queue.

User Manual

After finishing setting, click **Apply/Save** to save and apply the settings.

QoS Classification

Choose **Advanced Setup > Quality of Service > QoS Classification** and the following page appears.

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

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

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

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

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

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

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

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

In this page, you can enable, add or remove a QoS classification rule.

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

Add Network Traffic Class Rule

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

Traffic Class Name:

Rule Order:

Rule Status:

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

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

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

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue

is not specified to exist, will instead egress to the default queue on the interface.

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.

- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.

- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.

- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [kbits/s]

QoS Port Shaping

Choose **Advanced Setup** > **Quality of Service** > **QoS Port Shaping** and the following page appears.

QoS Port Shaping Setup

QoS port shaping supports traffic shaping of Ethernet interface.

If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	Shaping Rate (Kbps)	Burst Size (bytes)
eth1	LAN	<input type="text" value="-1"/>	<input type="text" value="0"/>

5.2.10 Routing

5.2.10.1 Adding a Route by GUI

Choose **Advanced Setup** > **Routing** > **Route**, and the following page appears.

Routing -- Default Gateway

The default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used accord being the lowest priority, if the WAN interface is connected. The priority can be changed by removing all and adding them back in again

Selected Default IPv4 Gateway Interfaces

->

<-

Available IPv4 Routed WAN Interfaces

Selected Default IPv6 Gateway Interface:

Step1 After setting the parameters, click **Apply/Save** to save and apply the settings.

RIP

Choose **Advanced Setup > Routing > RIP** and the following page appears.

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm2	2	Passive	<input type="checkbox"/>
ipoa0	2	Passive	<input type="checkbox"/>
atm4	2	Passive	<input type="checkbox"/>

Apply/Save

In this page, if you want to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.11 DNS

5.2.11.1 Adding a DNS Server by GUI

Choose **Advanced Setup > DNS > DNS Server** and the following page appears.

User Manual

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. If only a single WAN interface is used, the IP address 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 order 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

eth4.1	->	
	<-	

Use the following Static DNS IP address:

Primary DNS server:
Secondary DNS server:

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

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Step1 After setting the parameters, click **Apply/Save** to save and apply the settings.

Dynamic DNS

Choose **Advanced Setup > DNS > Dynamic DNS** and the following page appears.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

In this page, you are allowed to modify the DDNS settings.
Click the **Add** button to display the following page.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

DynDNS.org ▼

Hostname

Interface

pppoe_0_1_1/ppp0.1 ▼

DynDNS Settings

Username

Password

Apply/Save

- **D-DNS provider:** Select a proper DDNS server in the drop-down list.
- **Hostname:** It is the domain name and it can be modified.
- **Interface:** The interface that the packets pass through on the Router.
- **Username:** Enter the username for accessing the DDNS management interface.
- **Password:** Enter the password for accessing the DDNS management interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.12 UPnP

Choose **Advanced Setup > UPnP** and the following page appears.

UPnP Configuration

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

Enable UPnP:
UPnP version: 2.0 ▾

Apply/Save

In this page, you can enable or disable the UPnP function.
After finishing setting, click **Apply/Save** to save and apply the settings.

Following is the cli command to enable or disable the upnp:

```
upnp
  enable
exit
```

5.2.13 Dnsmasq

Choose **Advanced Setup > Dnsmasq** and the following page appears.

Dnsmasq Configuration

Host name of the Broadband Router: Heights
Domain name of the LAN network: local

Apply/Save

In this page, you can enable or disable the DNS function.

After enabling the DNS function, enter the host name of the broadband router and the domain name of the LAN network, and then click **Apply/Save** to save and apply the settings.

5.2.14 Print Server

Choose **Advanced Setup > Print Server** and the following page appears.

The screenshot shows a web interface for configuring the Print Server. On the left is a navigation menu with the following items: Device Info, Advanced Setup (highlighted), Layer2 Interface, WAN, USB Modem Service, IPV6, LAN, VPN, NAT, MAC Filtering, Parental Control, Firewall, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, and Print Server (highlighted in red). The main content area is titled 'Print Server settings' and contains the following text: 'This page allows you to enable / disable printer support.' Below this is a checked checkbox labeled 'Enable on-board print server.' There are three input fields: 'Printer name' with the value 'Print', 'Make and model' with the value 'DSL', and a URL field with the value 'http://192.168.1.1:631/printers/Print'. At the bottom right of the settings area is an 'Apply/Save' button.

In this page, you can enable or disable the **Print Server** function.

After enabling the **Print Server** function, enter the Printer name, Make and model, and then click **Apply/Save** to save and apply the settings.

5.2.15 DLNA

Choose **Advanced Setup > DLNA** and the following page appears.

Device Info

Advanced Setup

Layer2 Interface

WAN

USB Modem Service

IPV6

LAN

VPN

NAT

MAC Filtering

Parental Control

Firewall

Quality of Service

Routing

DNS

DSL

UPnP

DNS Proxy

Print Server

DLNA

Digital Media Server settings

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

Enable on-board digital media server.

Apply/Save

In this page, you can enable or disable the **DLNA** function.

After enabling the **DLNA** function, and then click **Apply/Save** to save and apply the settings.

5.2.16 Storage Service

5.2.16.1 Storage Device Info

Choose **Advanced Setup > Storage Service > Storage Device Info** and the following page appears.

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	FileSystem	Total Space	Used Space
------------	------------	-------------	------------

In this page, you can see the detail info about the USB device what plug to the Router.

5.2.16.2 Adding a User Account

Choose **Advanced Setup > Storage Service > User Accounts** and the following page appears.

Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.

UserName	Remove
----------	--------

Step2 In the **Storage UserAccount Configuration** page, click the **Add** button to display the following page.

height

Storage User Account Setup

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

Username:

Password:

Confirm Password:

Apply/Save

Step3 In this page, you can modify the Username, Password.

- **Username:** Set the Username to access the USB device.
- **Password:** Set the Password to access the USB device.

Step4 After setting the parameters, click **Apply/Save** to save and apply the settings.

Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.

UserName	Remove
bezeqnet	<input type="checkbox"/>

5.2.17 IPSec

Choose **Advanced Setup > IPSec** and the following page appears.

IPSec Tunnel Mode Connections

Add or remove IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
<input type="button" value="Add New Connection"/> <input type="button" value="Remove"/>				

In this page, you can add or remove the IPSec tunnel connections.
Click the **Add New Connection** button to display the following page.

IPSec Settings

IPSec Connection Name	<input type="text" value="new connection"/>
IP Version:	<input type="button" value="IPv4"/>
Tunnel Mode	<input type="button" value="ESP"/>
Local Gateway Interface:	<input type="button" value="Select interface"/>
Remote IPSec Gateway Address (IP or Domain)	<input type="text" value="0.0.0.0"/>
Tunnel access from local IP addresses	<input type="button" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
Mask or Prefix Length	<input type="text" value="255.255.255.0"/>
Tunnel access from remote IP addresses	<input type="button" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
Mask or Prefix Length	<input type="text" value="255.255.255.0"/>
Key Exchange Method	<input type="button" value="Auto(IKE)"/>
Authentication Method	<input type="button" value="Pre-Shared Key"/>
Pre-Shared Key	<input type="text" value="key"/>
Perfect Forward Secrecy	<input type="button" value="Disable"/>
Advanced IKE Settings	<input type="button" value="Show Advanced Settings"/>

In this page, set the parameters such as the IPSec connection name, tunnel mode, and remote IPSec gateway address.

If you need to configure the advanced settings of this IPSec tunnel connection, please click the **Show Advanced Settings** button to display the other parameters. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.18 Multicast

Choose **Advanced Setup > Multicast** and the following page appears.

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="3"/>
Query Interval:	<input type="text" value="125"/>
Query Response Interval:	<input type="text" value="10"/>
Last Member Query Interval:	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="25"/>
Maximum Multicast Data Sources (for IGMPv3):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="25"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>

IGMP Group Exception List

Group Address	Mask/Mask bits	Remove
224.0.0.0	255.255.255.0	
239.255.255.250	255.255.255.255	<input type="checkbox"/>
224.0.255.135	255.255.255.255	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="2"/>
Query Interval:	<input type="text" value="125"/>
Query Response Interval:	<input type="text" value="10"/>
Last Member Query Interval:	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="10"/>
Maximum Multicast Data Sources (for mldv2):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="10"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>

MLD Group Exception List

Group Address	Mask/Mask bits	Remove
ff01::0000	ffff::0000	
ff02::0000	ffff::0000	
ff05::0001:0003	ffff:ffff:ffff:ffff:ffff:ffff:ffff	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

In this page, you can configure the multicast parameters.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.3 Wireless

Choose **Wireless** and the submenus of **Wireless** are shown as below:



5.3.1 Radio

Choose **Wireless > Radio** to display the following page. This page allows you to configure the advanced features of the wireless LAN interface. Usually, you do not need to change the settings in this page.

User Manual

Radio

This page allows you to configure the Physical Wireless interfaces.

Wireless Interface: 178-Business-2.4(20:21:12:25:18:0C) ▼

Country: ISRAEL ▼ Current: IL

Regulatory Revision: 0 ▼ Current: 0

Interface: Disabled ▼

802.11 Band: 2.4 GHz ▼ Current: 2.4 GHz

Channel Specification: Auto ▼

802.11 n-mode: Auto ▼

Bandwidth: 40 MHz ▼ Current: 20MHz

NPHY Rate: Auto ▼

NPHY TxChains: 2 ▼

NPHY RxChains: 2 ▼

54g™ Mode: 54g Auto ▼

802.11n Protection: Auto ▼

VLAN Priority Support: Off ▼

Rate: 1 Mbps ▼

Basic Rate Set: Default ▼

Multicast Rate: Auto ▼

Regulatory Mode: 802.11H Loose ▼

DFS Preferred Channel List: ▼ ▼ ▼ ▼ ▼ ▼

TPC Mitigation (db): 0 (Off) ▼

OBSS Coexistence: On ▼

Fragmentation Threshold: 2346

RTS Threshold: 2347

DTIM Interval: 1

Beacon Interval: 100

Beacon Rotation: Disabled ▼

Preamble Type: Long ▼

Max Associations Limit: 128

XPress™ Technology: On ▼

SW Probe Response: On ▼

Beamforming transmission (BFR): VHT MU + HE MU+CQI BFR ▼

Beamforming reception (BFE): VHT MU + HE MU BFE ▼

MU-MIMO TX: Enabled ▼

WiFi 6 (11ax): Auto ▼

RIFS Mode Advertisement: Auto ▼

WMM Support: On ▼

No-Acknowledgement: Off ▼

APSD Support: On ▼

EDCA AP Parameters:

	CWmin	CWmax	AIFS	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	AdmissionControl	Discard Control	Oldest First
AC_BE	15	63	3	0	0	Off ▼	Off ▼	
AC_BK	15	1023	7	0	0	Off ▼	Off ▼	
AC_VI	7	15	1	6016	3008	Off ▼	Off ▼	
AC_VO	3	7	1	3264	1504	Off ▼	Off ▼	

EDCA STA Parameters:

AC_BE	15	1023	3	0	0
AC_BK	15	1023	7	0	0
AC_VI	7	15	2	6016	3008
AC_VO	3	7	2	3264	1504

Mode: Access Point ▼

Network: BSS ▼

URE Mode: Off ▼

STA Retry Time(sec): 5

DWDS: Disabled ▼

Apply Cancel

- **Channel Specification:** Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the

same channel in order to work correctly. This router supports auto channeling functionality.

- **802.11 n-mode::** Select **off** 802.11n or **Auto**.
- **Bandwidth:** Select the bandwidth for the network. You can select **20MHz in Both Bands, 20MHz in 2.4G Band and 40MHz in 5G Band**, or **40MHz in Both Bands, 80MHz in 5G Band, 160MHz in 5G Band**
- **802.11n Protection:** The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without “speaking” at the same time.
- **Basic Rate Set:** Select the basic transmission rate ability for the AP.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **XPress Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The default is Disabled.