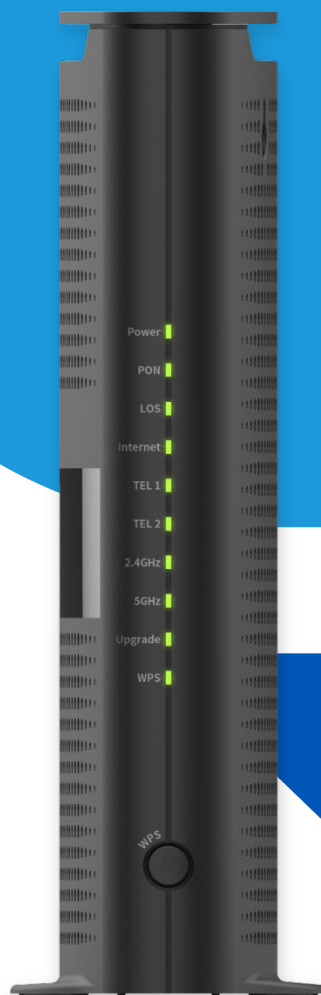


User Manual

HPF30E






Contents

Chapter 1. Introducing Your Router.....	1
1.1 Package contents.....	1
1.2 Product Overview	2
Chapter 2. Connecting Your Product.....	6
2.1 Position.....	6
2.2 Connection.....	7
Chapter 3. Logging into Your Product.....	10
3.1 Access to Web UI through Mobile/Web Browser.....	11
Chapter 4. Knowing Connection Status	13
4.1 Quick Menu.....	13
4.2 Home Menu	14
Chapter 5. Setting Internet Environment.....	15
5.1 Internet Setting.....	15
Chapter 6. Setting Wireless Network	16
6.1 Basic Wireless Setting.....	16
6.2 Primary Wireless Setting.....	21
6.3 Guest Wireless Setting	27
6.4 MAC Access Control.....	29
Chapter 7. Setting Local Setting.....	32
7.1 LAN Setting.....	32
7.2 Reserved IP Address.....	34
Chapter 8 Providing Network Service.....	36
8.1 Firewall.....	36
8.2 DDNS Setting	38
8.3 Port Forwarding Rule Setting.....	40

8.4 Port Triggering Rule Setting	42
8.5 DMZ Setting	43
8.6 Parental Control Rules	44
Chapter 9 Setting Advanced Options	46
9.1 Advanced Network Setting.....	46
9.2 Routing Rule Setting	48
9.3 UPnP Setting	51
9.4 Diagnosing.....	52
9.5 Statistics	56
Chapter 10. Managing the System.....	57
10.1 Log Analysis.....	57
10.2 Factory Reset/Restart	58
10.3 LED Mode.....	59
10.4 Change Password.....	60
10.5 Energy Saving Mode	61
10.6 Date/Time	61
10.7 Remote Access	62
Chapter 11. Voice	64
11.1 Status	64
11.2 Call History.....	64
Chapter 12. Troubleshooting.....	65
Chapter 13. Supplemental Information.....	67
13.1 Safety and Regulatory Information.....	67
13.2 Specification	69

Chapter 1. Introducing Your Router

Please read this user's manual carefully to safely install, use and maintain the product at maximum performance. The information in this user's manual is subject to change without notice. The detailed description may slightly differ depending on each product, and the images are merely for illustrational purposes and thus may differ from the screens you actually see. Throughout the whole manual, pay special attention to the following marks that indicate hazardous situations.

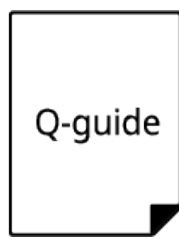
	Warning	Indicates a hazardous situation that could result in serious injury.
	Note	Indicates additional information to make the user aware of possible problems and information of any importance to help understand, use, and maintain the installation.
	Tips	Indicates information helpful to the user, like showing an easier way to do something.

1.1 Package contents

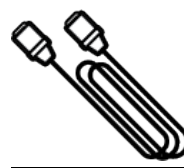
Your package contains the following items.



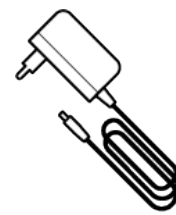
HPE30E
10G EPON Unit



Quick Installation
Guide



RJ-45
Ethernet Cable



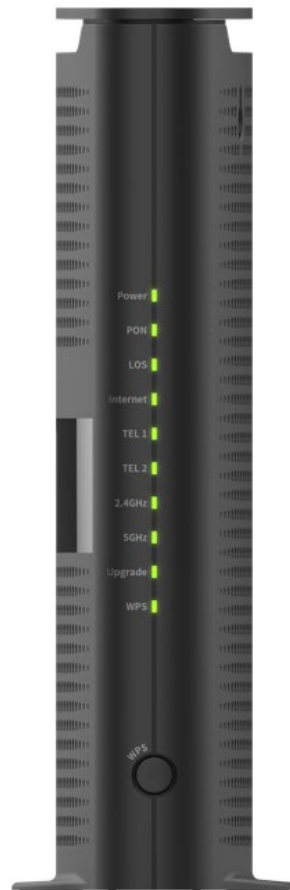
Power Adapter

Note: Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

1.2 Product Overview

1.2.1 Front Panel

The front panel provides 10 LEDs, and the WPS button showed the following figure.



You can use the LEDs to verify status and connections. The following table lists and describes each LED on the front panel of the product.

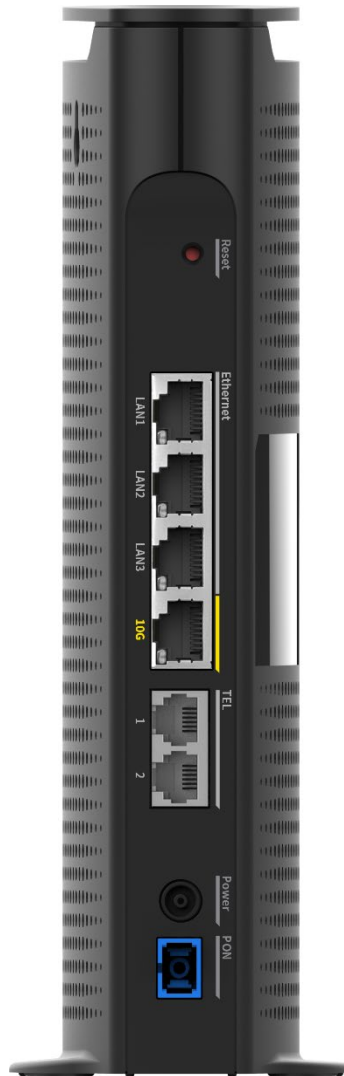
LED	Operation	
Power	Green On	Power is on.
	Green Blinking	Booting is in progress.
	Red On	Power failure.
	Red Blinking	POST (Power-ON-Self-Test) failure.
	Off	Power is off.
PON	Green On	Registration and provisioning are done.

	Green Blinking	ONT tries to create a connection to OLT (Registration is done but provisioning is in progress)
	Green Fast Blinking	ONT tries to create a connection to OLT. (Registration is in progress)
	Off	PON port is not connected.
LOS	Red On	There is no optical signal nor synced EPON signal.
	Off	There is a synced EPON signal.
Internet	Green On	Internet is connected.
	Green Blinking	Internet is connecting.
	Orange On	PPP authentication failed.
	Orange Blinking	Internet is not connected. (Not assigned IP address)
	Off	Internet is not connected.
TEL 1/2	Green On	Telephone is connected and on hook.
	Green Blinking	Telephone is off hook. (Making a call or having a conversation)
	Orange Blinking	Provisioning
	Red On	No Provisioned
	Off	Phone disabled
2.4GHz/5GHz	Green On	2.4GHz/5GHz radio is on.
	Off	2.4GHz/5GHz radio is off.
Upgrade	Green Blinking	Firmware is being upgraded.
WPS	Green Blinking	<ul style="list-style-type: none"> If WPS is running, it operates for 2 minutes at this time, and the LED operates at Blinking. If WPS succeeds within 2 minutes, the blinking stops and the LED turns off.
	Green Fast Blinking	If WPS fails after 2 minutes, it operates as Fast Blinking for 5 seconds, after which the LED turns off.
	Off	WPS is not running.

- **WPS Button:** The WPS button makes it easier to connect to devices you want to connect wirelessly. Press the WPS button and check the progress through the WPS LED. For more details, see [Connecting your router > Connection](#).

1.2.2 Back Panel

The back panel provides the connections and button shown in the following figure.



- **Reset** button: Press and hold the Reset button for 3 seconds to restore factory default settings.

Note: All user settings will be erased and this action cannot be undone.

- **LAN 1~3:** Provides three 1Gbps LAN ports.
- **10G:** Provides one 10Gbps LAN port.
- **TEL 1/2:** Provides 2 telephone ports.

LED	Operation	
LAN 1~3	Green On	1G link up status

	Orange On	100M/10M link up status
	Off	The LAN is not connected.
10G	Green On	10G link up status
	Orange On	5G/2.5G/1G/100M link up status
	Off	The LAN is not connected.

- **Power:** Connect the power adapter provided in the package and plug it into an electrical outlet.
- **PON:** Connect the fiber optic cable.

1.2.3 Label

The label is on the side of the product. You can check the wireless and Web UI connection information.



To get help from your internet service provider, you may need to provide the model name, ONU, and MAC address listed on the label.

Chapter 2. Connecting Your Product

2.1 Position

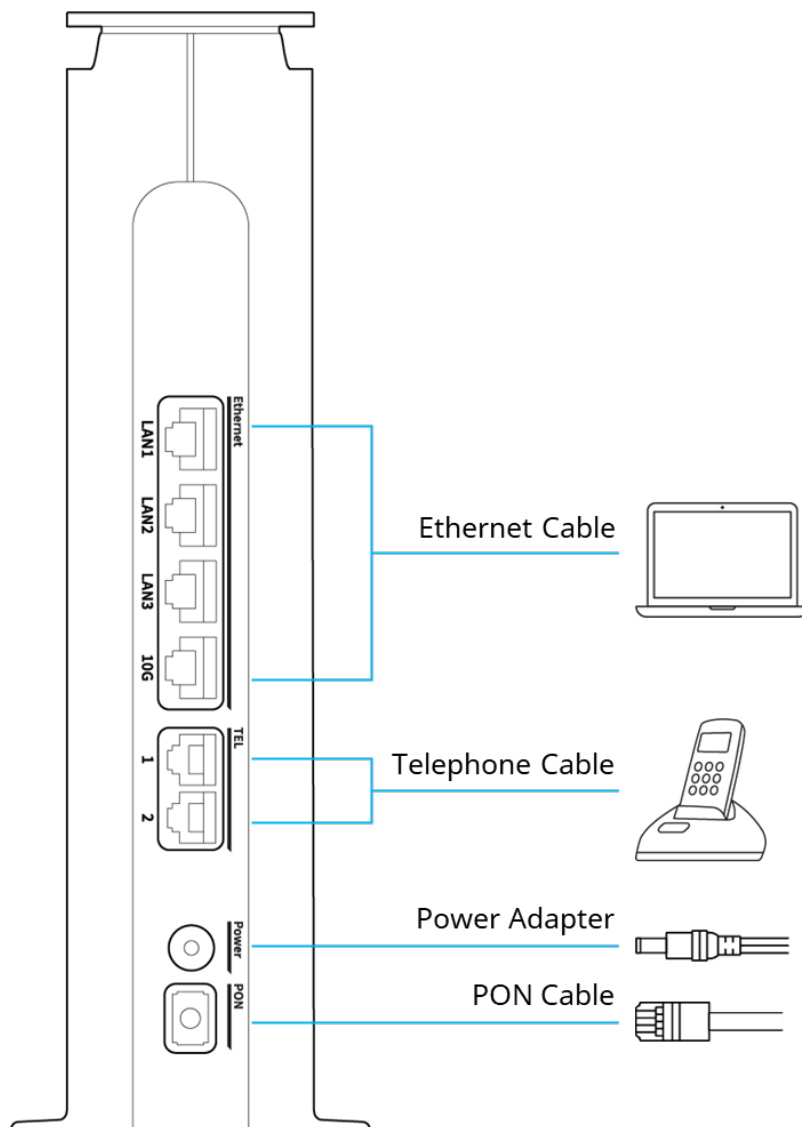
When you install your router, some tips make the Wi-Fi network more stable and robust at home.

- Locate your router near the center of the area where PC and other devices operate. The center will be the best place for optimum connection.
- Please install this product in a place where there are no objects such as PC or wall within 10cm from the front, rear, left, right, and top.
- Place your router in the location where it can be connected to various devices as well as to a power source.
- Safely place the cables and power cord out of the way so they do not create a tripping hazard.
- Place your router in an elevated location, minimizing the number walls and ceilings between the router and your other devices.
- Keep away from the intense electromagnetic radiation and the device of electromagnetic sensitive.
- Stand your router on a flat surface in an upright position not to tilt it.

2.2 Connection

Connect the DC power adaptor from the power connector to the electric outlet. If the power successfully turns on, a Power LED at the front panel turns on.

Note: Be sure to use the power adaptor provided.



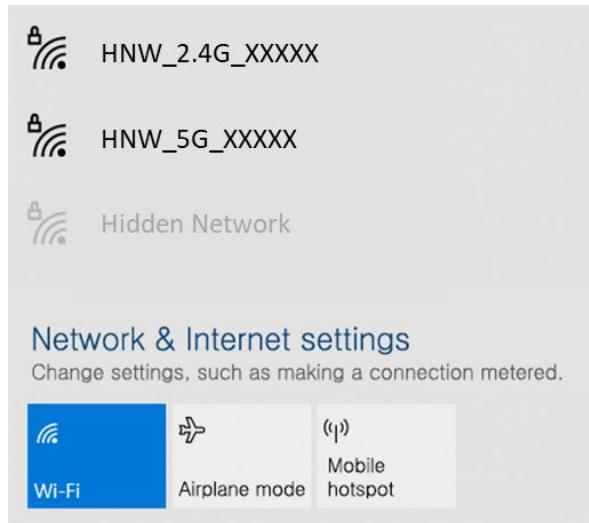
Connect the Devices (Telephone, PC, etc.)

Over wired Ethernet connection

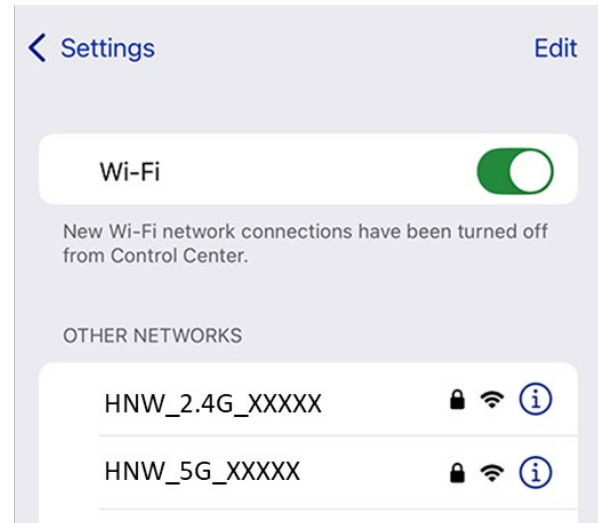
- ① Connect network devices such as PC, IPTV, OTT or game console using an Ethernet cable.

Wirelessly

① Go to the Wi-Fi setting menu on your network devices.



PC



Mobile

② Select the network name (SSID) of your product from the Wi-Fi list and enter the password. If the network name is not shown, you need to enter it manually. The default network name (SSID) and password are printed on the left side of the product.

If there is no Network Name (SSID) you are looking for, you can also connect by manually entering the Network Name (SSID).

Using WPS button

If your network device supports WPS, you can connect it to the router by simply pressing the WPS button.

① Tap the WPS icon or press the WPS button on your network device.

② Press the WPS button on your product within 2 minutes.

Note:

- Place your network device close to the product during WPS configuration.
- If security is set to WPA3-SAE, the WPS function is disabled and does not work.
- If Hide SSID is set to On, connection through the WPS button is not possible.

Wi-Fi access through QR Code

QR Code through Wi-Fi connection is provided on the label on the left side of the product.

- ① Open the camera app on your mobile and scan the QR Code.
- ② When the connection confirmation pop-up appears, press OK and it will automatically connect to Wi-Fi.



※ This function may not be supported depending on mobile specifications.

Chapter 3. Logging into Your Product

This product can be used to check the product status and set various settings using a **Web or mobile browser**.

The screen resolution may vary depending on the device you are accessing.

Mobile Browser

Mobile browsers are suitable for checking product status and basic configuration settings.

Pre-connection Check

Your mobile device must be connected to the product's Wi-Fi network. Connection status can be verified in your mobile device's Wi-Fi settings.

Recommended Environment

- iOS Safari browser
- Android Chrome browser
- Other default mobile browsers

Web Browser

Web browsers are recommended for advanced settings and detailed environment configuration.

Recommended Environment

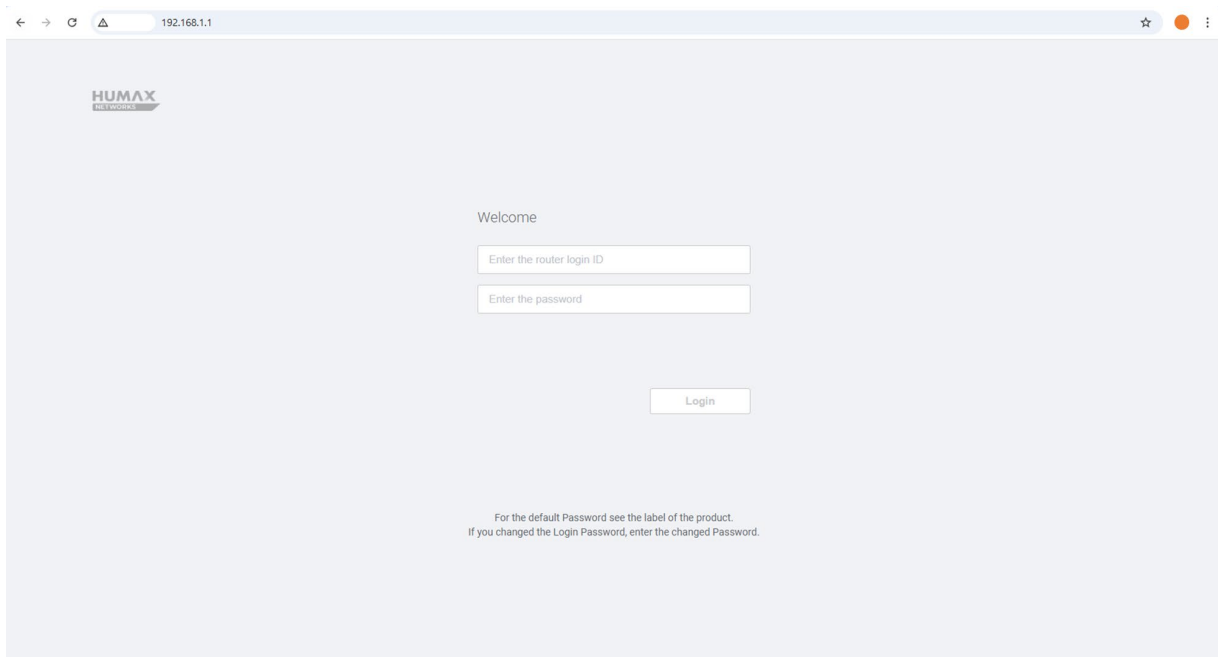
<ul style="list-style-type: none"> * Microsoft Windows 7 or later - Microsoft Edge 80 or later - Internet Explorer 10 or later - Google Chrome 23 or later - Firefox Mozilla 21 or later - Opera 15 or later 	<ul style="list-style-type: none"> * MAC OS 10.7 or later - Safari 6 or later
<ul style="list-style-type: none"> * iOS 10.3 or later - Safari 6 or later 	<ul style="list-style-type: none"> * Android 6.0 or later - Google Chrome 23 or later

3.1 Access to Web UI through Mobile/Web Browser

When you access the Web UI, you need to set up the login ID and password.

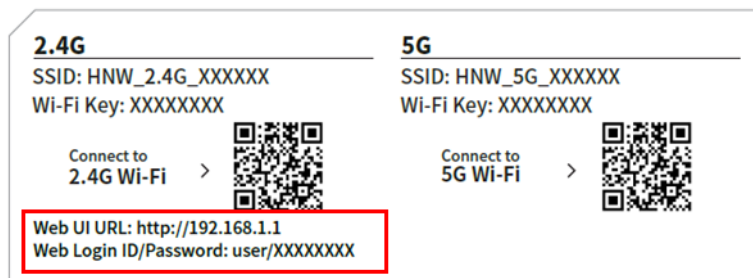
① Open the mobile/web browser.

② Enter **http://192.168.1.1** to the address bar, and then press the Enter key.



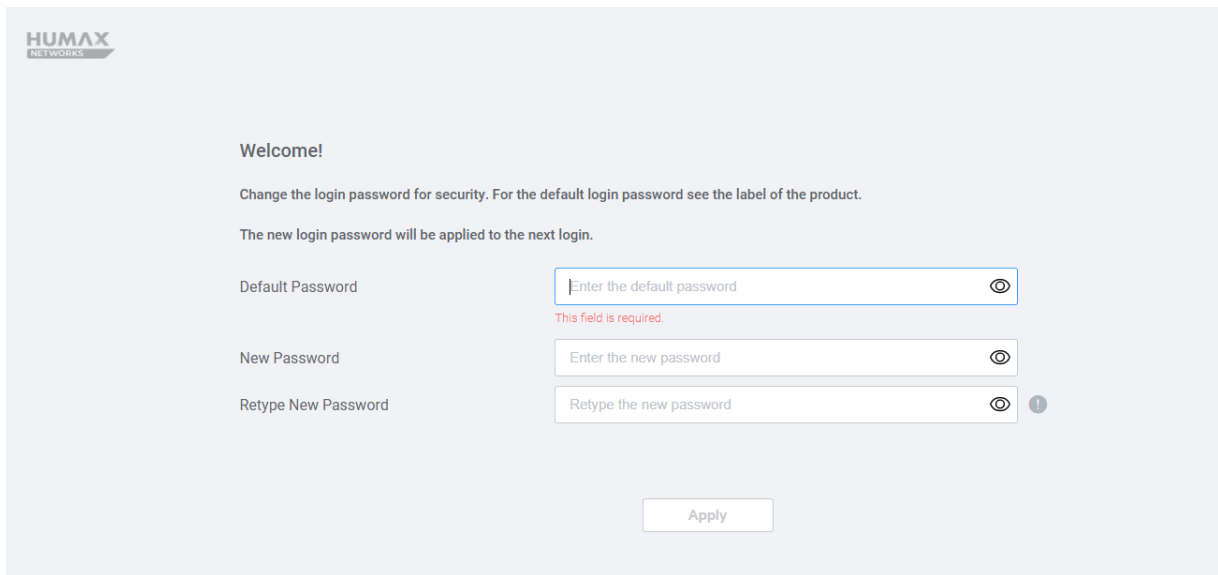
③ Enter the **default ID and password** to login to the user interface.

The default ID and password is printed on the product label.



※ 'XXXXXXXX' is a combination of 8 letters, numbers, and uppercase and lowercase letters that are different for each product, so you should check the label of the actual product.

④ When you first enter the Web UI, you can change your password.




HUMAX NETWORKS


Welcome!



Change the login password for security. For the default login password see the label of the product.

The new login password will be applied to the next login.

Default Password 

This field is required.

New Password 

Retype New Password  

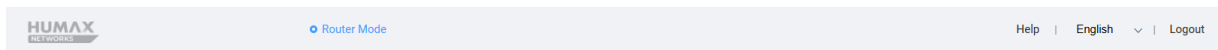
Note:

- The new password can be from 6 to 64 characters A-Z, a-z, 0-9, and all characters. A combination of letters and numbers is recommended.
- If you lose your password, you must perform a factory reset, which will erase all custom settings.

Chapter 4. Knowing Connection Status

4.1 Quick Menu

You can see the quick menu at the top right. Using the quick menu, you can check the operation mode and custom ID and simply change the system environment.



- **HUMANETWORKS Logo**
- **Operation Mode:** Means the current operation mode of the product
- **Help:** If you click this hyperlink, display the help message popup
- **Language:** Set the language to display the WEB UI
- **Logout:** Press this button to logout of WEB UI

4.2 Home Menu

You can see the information on the Internet, LAN, Wireless, Interface Link Status, PON Status, Voice Status and Connected Devices In the HOME menu.

The screenshot displays the HUMAX router's Home menu interface. The top navigation bar includes 'Home', 'Internet', 'Wireless', 'LAN', 'Service', 'Advanced', 'Management', and 'Voice'. The main content area is divided into several panels:

- Information:** Displays router details such as Model Name (HPF30E), Serial Number (19171587400019), Firmware Version (01.05.07.XEE0), Time (1970.01.01 02:35:55), Operation Mode (10G-EPON), Operation Time (0 days 02:35:52), and MAC Address (BC:9A:8E:69:86:E8).
- Internet:** Shows WAN Type (Disconnected), WAN IP Address, Subnet Mask, Gateway, DNS Server 1 / DNS Server 2, and MAC Address (BC:9A:8E:69:86:E8). A 'Connect' button is visible.
- LAN:** Displays LAN IP Address (192.168.1.1), DHCP Server (On), IP Address Assignment (Auto), Client Account (100), and MAC Address (BC:9A:8E:69:86:EF).
- Wireless:** Shows Network Name (SSID) (HNW_2.4G_6986E8), Security (WPA2/WPA-PSK), Password (masked), and MAC Address (BC:9A:8E:69:86:F8).
- Connected Devices:** A table listing connected devices:

Device Name	Interface	MAC Address	IP Address
shyoonn1	LAN 4	AC:1A:3D:8E:42:A5	192.168.1.2
- Interface Link Status:** Lists WAN (PON), LAN Port 1, LAN Port 2, LAN Port 3, and LAN Port 4 (1G Full).
- Voice:** Shows Tel 1 and Tel 2, Registration (Unregistered), Line Status (On-Hook), Telephone Number, Extension Number (#1), and Description.
- PON Status:** Displays Input(Rx) Power (-40.000000 dBm), Output(Tx) Power (-40.000000 dBm), Supply Voltage (3359 mV), Transmitter bias current (0 uA), and Operating Temperature (37 °C).

Chapter 5. Setting Internet Environment

5.1 Internet Setting

① Enter the **Internet > Internet Setting**

You can set the Manual DNS and IPv6.

Internet Setting

Manual DNS

DNS Server 1 . . .

DNS Server 2 . . .

IPv6

② Enter the options:

Display	Description
Manual DNS	Set whether to use Manual DNS. If set to 'On', DNS server address 1/2 can be entered directly.
DNS Server 1	Sets the primary DNS server.
DNS Server 2	Sets the secondary DNS server.
IPv6	Toggle to use IPv6 WAN side network or not.

Note:

- The provider assigns the DNSv4 server address for the DNS setup, so a manual DNS setup is usually not required.
- In the case of IPv6, it is available only if you have subscribed to the service.

③ Click **Apply** to save the changes.

Chapter 6. Setting Wireless Network

6.1 Basic Wireless Setting

This page configures each frequency used in your wireless.

This model is a dual-band model, providing a total of three frequencies (2.4GHz, 5GHz). Each frequency has different characteristics in terms of range, speed, interference, and supported devices. Understanding the differences between these bands can help you optimize wireless network performance for your specific environment and requirements.

Feature	2.4 GHz	5 GHz
Range	Long range	Shorter range than 2.4 GHz
Speed	Up to 600 Mbps (theoretical)	Up to 3.5 Gbps or more
Interference	High interference (crowded)	Less interference
Number of Channels	Fewer channels (3 non-overlapping)	More channels (19 non-overlapping)
Device Compatibility	Supported by most devices	Supported by modern devices
Use Cases	General browsing, IoT, long range	Streaming, gaming Fast data

Using the Band Steering function, you can divide the wireless by frequency or use it as one SSID. Please refer to section *6.2 Primary Wireless Setting* for details.

6.1.1 2.4GHz

Settings for the 2.4GHz frequency.

(*Do not change default settings unless it is necessary.)

① Enter the **Wireless > Basic Setting**.

Basic Setting

2.4GHz 5GHz

Radio

Channel Q APs

802.11 Mode

Bandwidth

Sideband

TWT

Output Power

② Enter the option values:

Display	Description
Radio	<p>Enable or disable the 2.4GHz wireless network.</p> <ul style="list-style-type: none"> • If you turn it off, all the options below will disappear, and you cannot use 2.4GHz wireless network. The default value is On. • Radio cannot be turned off if Mesh Setting is set.
Channel	<p>Select an operating channel for the 2.4GHz wireless network.</p> <ul style="list-style-type: none"> • The default value is 'Auto' that enables selecting an optimal channel for the current network environment. You can also set it to a manual channel (1-13). • If you press the APs button, you can check the surrounding 2.4GHz frequency usage.
802.11 Mode	<p>Select 802.11 mode according to your wireless client devices to allow 802.11 supported devices on your wireless network.</p> <ul style="list-style-type: none"> - Available: 802.11b, 802.11b+g, 802.11b+g+n, 802.11 b+g+n+ax - It is recommended to select the highest level of 802.11 mixed mode to ensure compatibility with previous versions.
Bandwidth	<p>Select a bandwidth for the 2.4GHz wireless network.</p> <ul style="list-style-type: none"> - The default setting is '20MHz'.
Sideband	<p>Set the sideband.</p> <ul style="list-style-type: none"> • When using channels 5-9, you can select either the upper channel or lower channel when the bandwidth is set to 40MHz.

Display	Description
TWT	<p>Enable or disable the TWT((Target Wake Time).</p> <ul style="list-style-type: none"> TWT (Target Wake Time) is a Wi-Fi 6 (802.11ax) power-saving feature that extends battery life by scheduling when devices wake up to send or receive data. This feature reduces network congestion and improves efficiency, particularly in environments with multiple IoT devices.
Output Power	<p>Set the radio signal strength.</p> <ul style="list-style-type: none"> You can select one from "High," "Medium," and "Low." > High: (Default): Outputs the maximum wireless signal strength. > Medium: 25% reduction in 'High' output. > Low: 50% reduction in 'High' output If you lower the signal strength, your wireless range may be reduced.

6.1.1 5GHz

Settings for the 5GHz frequency.

(*Do not change default settings unless it is necessary.)

Basic Setting

2.4GHz
5GHz

Radio	<input checked="" type="checkbox"/>
Channel	Auto ⓘ Q.APs
802.11 Mode	802.11a+n+ac+ax
Bandwidth	80 MHz
TWT	<input type="checkbox"/>
Output Power	High

5GHz

Display	Description
Radio	<p>Enable or disable the 5GHz wireless network.</p> <ul style="list-style-type: none"> • If you turn it off, all the options below will disappear, and you cannot use 5GHz wireless network. The default value is On. • Radio cannot be turned off if Mesh Setting is set.
Channel	<p>Select an operating channel for the wireless network.</p> <ul style="list-style-type: none"> • The default value is 'Auto' that enables selecting an optimal channel for the current network environment. You can also set it to a manual channel (36~140, 19 Channels). • If you press the APs button, you can check the surrounding 5GHz frequency usage.
802.11 Mode	<p>Select 802.11 mode according to your wireless client devices to allow 802.11 supported devices on your wireless network.</p> <ul style="list-style-type: none"> • Available: 802.11a, 802.11a+n, 802.11a+n+ac, 802.11a+n+ac+ax • It is recommended to select the highest level of 802.11 mixed mode to ensure compatibility with previous versions.
Bandwidth	<p>The available bandwidth values vary depending on the selected Channel and 802.11 Mode.</p>
TWT	<p>Enable or disable the TWT((Target Wake Time).</p> <ul style="list-style-type: none"> • TWT (Target Wake Time) is a Wi-Fi 6 (802.11ax) power-saving feature that extends battery life by scheduling when devices wake up to send or receive data. This feature reduces network congestion and improves efficiency, particularly in environments with multiple IoT devices.
Output Power	<p>Set the radio signal strength.</p> <ul style="list-style-type: none"> • You can select one from "High," "Medium," and "Low." > High: (Default): Outputs the maximum wireless signal strength. > Medium: 25% reduction in 'High' output. > Low: 50% reduction in 'High' output • If you lower the signal strength, your wireless range may be reduced.

Note:

- If a radar signal is detected during communication, the communication may be temporarily interrupted because the DFS function automatically changes the channel.

- Depending on the environment, it may be connected with a lower bandwidth than the actual setting.

6.2 Primary Wireless Setting

Set up the main wireless network.

The configuration on both 2.4GHz and 5GHz network is identical to each other. Therefore, how to configure the 2.4GHz wireless network will be described and the description for the 5GHz wireless network will be omitted.

① Enter the **Wireless > Primary Wireless**.

Primary Wireless

Band Steering (2.4GHz + 5GHz)

2.4GHz 5GHz

2.4GHz Primary Wireless

Network Name(SSID)

Security

Encryption

MFP

Password

Hide SSID

Internet Only

Wi-Fi Client

AP Isolation

WMF

QR Code Generation

※ QR Code is provided for easy Wi-Fi connection. Press the [QR Code Generation] button to generate a QR code, scan it through the mobile's camera, you can directly access the Wi-Fi.

6.2.1 2.4GHz+5GHz

When Band Steering is enabled, 2.4GHz and 5GHz bands operate under a single SSID, providing optimal wireless connection and simplified network management across both frequency bands.

Primary Wireless

Band Steering (2.4GHz + 5GHz)



2.4GHz + 5GHz

Network Name(SSID)

Security


Encryption

MFP

Password  

Hide SSID

Internet Only

Wi-Fi Client 

AP Isolation

WMF

[QR Code Generation](#)

※ QR Code is provided for easy Wi-Fi connection. Press the [QR Code Generation] button to generate a QR code, scan it through the mobile's camera, you can directly access the Wi-Fi.

Display	Description
Network Name (SSID)	Enter a network name of your product if you want to change it. <ul style="list-style-type: none"> You can enter up to 32 characters a-z, A-Z, 0-9, and special characters, and they are case sensitive. The default Network Name(SSID) is printed on the label of your product.

Display	Description													
Security	<p>Select a security type for your product.</p> <ul style="list-style-type: none"> Your product provides None, WPA2-PSK, WPA2/WPA-PSK, WPA3-SAE and WPA2-PSK/WPA3-SAE Mixed. The lower you go, the stronger the security. <p>> None does not provide any security. Any devices have access to the Wi-Fi network.</p> <p>> WPA2-PSK is a security method using PSK(Pre-Sharing of Keys).</p> <p>> WPA2/WPA-PSK Mixed automatically uses WPA2 or WPA security method depending on the wireless device to be connected.</p> <p>> WPA3-SAE is a security method using SAE(Simultaneous Authentication of Equals).</p> <p>> WPA2-PSK/WPA3-SAE Mixed provides a secure and fast connection from the latest specification client devices.</p> <ul style="list-style-type: none"> If your Wi-Fi client supports it, you should consider setting the security mode accordingly. If you are unsure, we recommend choosing WPA3-SAE/WPA2-PSK or WPA2-PSK. 													
Encryption	<p>Select an encryption type to protect the data of the users who have connected to the wireless network.</p> <p>> AES provides the most robust encryption.</p> <p>> AES/TKIP offers strong encryption with improved backward compatibility.</p> <ul style="list-style-type: none"> The default value of AES/TKIP is recommended. 													
MFP	<p>Enable or disable the MFP(Management Frame Protection)</p> <ul style="list-style-type: none"> Sets client devices that support the MFP(Management Frame Protection) function to communicate with enhanced security. 													
Password	<p>Enter the password of the Wi-Fi network.</p> <ul style="list-style-type: none"> You can enter the only a~z, A~Z, 0~9, and special characters <table border="1" data-bbox="528 1592 1134 1644"> <tr> <td>!</td><td>)</td><td>+</td><td>.</td><td>:</td><td>?</td><td>~</td><td>\$</td><td>'</td><td>"</td><td><</td><td>,</td><td>/</td> </tr> </table>, and they are case-sensitive. The default password is printed on the label of your product. This will be required when you connect a mobile device wirelessly to your wireless network. 	!)	+	.	:	?	~	\$	'	"	<	,	/
!)	+	.	:	?	~	\$	'	"	<	,	/		
Hide SSID	<p>Enable or disable the Hide SSID.</p> <ul style="list-style-type: none"> You can prevent other users from detecting your network when they scan for the available wireless network. 													

Display	Description
Internet Only	Enables or disables the feature that allows only Internet access. <ul style="list-style-type: none"> • Users connected to that Wi-Fi cannot communicate with each other over the internal network and cannot enter the Web UI.
Wi-Fi Client	Set the maximum number of allowed wireless clients. <ul style="list-style-type: none"> • The value can be set between 1 and 75.
AP Isolation	Enable or disable AP Isolation. <ul style="list-style-type: none"> • AP Isolation prevents wireless clients connected to the same access point from communicating with each other, enhancing network security.
WMF	Enable or disable the WMF.(Wireless Multicast Forwarding) <ul style="list-style-type: none"> • WMF optimizes network traffic by forwarding multicast data only to intended wireless clients, improving overall network performance.

- **QR Code Generation** Button: Click the QR Code Generation button to generate a QR Code on the right side. Users can scan the QR Code on their mobile devices to instantly connect to the wireless network. This feature may not be available depending on the user's mobile device model.

Note:

- The default network name(SSID) and password is printed on the label of your product.
- If the SSID is hidden, some devices may not detect the Wi-Fi network of your router. You need to search the SSID to connect to the Wi-Fi network manually. Connection through the WPS button is not possible.
- The WPS feature is available when the security level has been set to "None," "WPA2-PSK," "WPA2/WPA-PSK," or "WPA3-SAE/WPA2-PSK." The WPS feature will not be available when the security level has been set to "WPA3-SAE.")
- When the security is set to WPA3-SAE, only clients that support WPA3-SAE can access it.

6.2.1 2.4GHz, 5GHz

When Band Steering is disabled, 2.4GHz and 5GHz bands operate independently with separate SSIDs, allowing manual selection of frequency bands.

> 2.4GHz

Primary Wireless

Band Steering (2.4GHz + 5GHz)



2.4GHz 5GHz

2.4GHz Primary Wireless



Network Name(SSID)

HNW_2.4G_6986E8

Security

WPA2/WPA-PSK

Encryption

AES/TKIP

MFP



Password

.....



Hide SSID



Internet Only



Wi-Fi Client

75



AP Isolation



WMF



[QR Code Generation](#)

※ QR Code is provided for easy Wi-Fi connection. Press the [QR Code Generation] button to generate a QR code, scan it through the mobile's camera, you can directly access the Wi-Fi.

> 5GHz

Primary Wireless

Band Steering (2.4GHz + 5GHz)

2.4GHz **5GHz**

5GHz Primary Wireless

Network Name(SSID)

Security

Encryption

MFP

Password

Hide SSID

Internet Only

Wi-Fi Client

AP Isolation

WMF

[QR Code Generation](#)

※ QR Code is provided for easy Wi-Fi connection. Press the [QR Code Generation] button to generate a QR code, scan it through the mobile's camera, you can directly access the Wi-Fi.

- The description for each item is the same as 6.2.1 2.4GHz+5GHz, so it is omitted.

③ Click **Apply** to save the changes.



Tips: Scanning the QR Code makes it easier to access Primary Wireless.

If you press [Generate the QR Code], a QR Code with Primary Wireless information on the right is created. Scan the QR Code on your mobile, and you will be connected directly to the Wireless.

6.3 Guest Wireless Setting

You can configure the secondary wireless network.

- ① Enter the **Wireless > Guest Wireless**

Guest Network

2.4GHz 5GHz

2.4GHz Guest Network

2.4GHz

- ② Turn **On** the 2.4GHz of Guest Wireless.

Guest Network

2.4GHz 5GHz

2.4GHz Guest Network

Network Name(SSID)

Security v

Encryption v

MFP

Password 👁 !

Hide SSID

Internet Only

Wi-Fi Client !

AP Isolation

WMF

5GHz

Guest Network

2.4GHz **5GHz**



5GHz Guest Network

Network Name(SSID)

Security


Encryption

MFP

Password  

Hide SSID

Internet Only

Wi-Fi Client 

AP Isolation

WMF

- The description for each item is the same as 6.2.1 2.4GHz+5GHz, so it is omitted.

6.4 MAC Access Control

Manage the MAC address you want to allow/reject connections. You can set whether to connect for each Wireless (Primary Wireless, Secondary Wireless).

- 1 Enter the **Wireless > MAC Access Control**.

MAC Access Control

Primary Wireless Guest Wireless

2.4GHz Access Control

5GHz Access Control

- 2 Turn **On** the wireless type you wish to allow/reject access to.

MAC Access Control

Primary Wireless Guest Wireless

2.4GHz Access Control

MAC Access Control Type Black Mode White Mode
Only devices with MAC addresses registered in the white list can connect to this device via WiFi.

MAC Access Control List (White Mode)

No.	MAC Address	Device Name	Delete
No Data			

5GHz Access Control

MAC Access Control Type Black Mode White Mode
Devices with MAC addresses registered in the black list can't connect to this device via WiFi.

MAC Access Control List (Black Mode)


No.	MAC Address	Device Name	Delete
No Data			

You can set Primary Wireless 2.4GHz and 5GHz to Black Mode or White Mode respectively.

- **Black Mode:** Register/manage MAC addresses that do not allow access.
- **White Mode:** Register/manage MAC addresses that allow access. Unregistered devices cannot connect to the wireless.

Note:

When setting White Mode, if there are no registered devices, no device will be connected wirelessly. If there are no registered devices, all existing devices will be disconnected. In this case, you can connect to another available wireless or wired connection and then connect to the Web UI. Be careful when setting. (* When you select White Mode and press the [OK] button in the pop-up that appears, it will be applied immediately, so be careful.)

MAC Access Control List (White Mode)			
No.	MAC Address	Device Name	Delete
1	AA:BB:CC:DD:EE:FF	shyoon-n1	

MAC Access Control List

It shows the rules set by the user. You can delete them individually by pressing the **Delete** button.

To add an item

To add a new entry, click the **Add** button at the bottom. You can add up to 32 rules.

- ① Click **Add** to add a rule.

MAC Access Control Rule ×

Choose the SSID 2.4GHz ▾

MAC Address / Device Name Select or enter the device

Cancel
Apply

- ② Select the wireless type (SSID) you want to set up.

- ③ Select a device from the list of connected devices. You can enter the MAC address if there is no device name in the list. In this case, you do not need to enter the Device Name.

- ④ Click **Apply** to save the changes.

Chapter 7. Setting Local Setting

7.1 LAN Setting

You can set LAN IP address, subnet mask, and DHCP server and allocate specific IP addresses to MAC address.

① Enter the **LAN > LAN Setting**.

LAN Setting

IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Server	<input checked="" type="checkbox"/>
IP Address Assignment	<input type="text" value="Auto"/>
Client Account	<input type="text" value="100"/> Up to 253 clients available
Lease Time	<input type="text" value="24"/> <input type="button" value="hour"/> !
WINS Server	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

② Enter the options.

Display	Description
IP Address	Enter the IP address of your router. <ul style="list-style-type: none"> You can access the web UI page via the IP address. The default value is 192.168.1.1.
Subnet Mask	Set the subnet mask type.
DHCP Server	Enables or disables the use of a DHCP server to assign IP addresses to devices connected to the local network.

Display	Description
IP Address Assignment	<p>Set the IP address allocation type via the DHCP server.</p> <ul style="list-style-type: none"> • If set to "Automatic", IP addresses will be automatically allocated as many as the number of allocatable IP addresses (Client Account). • If set to "Manual", IP addresses will be allocated within the given range as many as the number of allocatable IP addresses starting from the start IP address.
Start IP Address	<p>Set the starting address for the DHCP server to begin assigning IP addresses. (*Only if IP Address Assignment is set to "Manual")</p>
Client Account	<p>Set the maximum number of devices that will be connected.</p> <ul style="list-style-type: none"> • The maximum number of devices that can be connected is provided below the settings field.
Lease Time	<p>Set the time duration for the connected device to stay connected using the assigned IP.</p> <ul style="list-style-type: none"> • The default setting is 24 hours.
WINS Server	<p>Enter the address for the WINS server to notify the DHCPv4 client.</p>

③ Click **Apply** to save the changes.

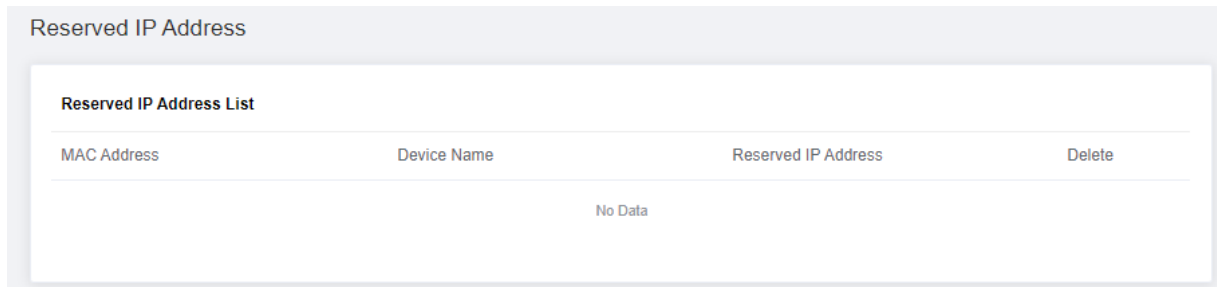
Note:

- If DHCP server is turned off, connected clients cannot automatically obtain addresses within the local network range. In this case, addresses must be manually configured on client devices.
- Incorrect settings can cause connection problems. It is recommended to use the default value.
- If the IP address has changed, you will need to restart the system. The phone cannot be used during reboot, and after reboot, you need to access the web page with the new address.

7.2 Reserved IP Address

You can allocate IP addresses to MAC address. Your device is allocated for the same IP address whenever accessing the DHCP server. Allocating IP address is similar to configuring static IP address.

- 1 Enter the **LAN > Reserved IP Address**.



MAC Address	Device Name	Reserved IP Address	Delete
No Data			

Reserved IP Address List

It shows the rules set by the user. You can delete them individually by pressing the **Delete** button. please delete them and edit them again.

To add an item

Click **Add** to add a rule. You can add up to 32 rules.

- 2 Click **Add** to add a rule.



- 3 Select a device from the list of connected devices. You can enter the MAC address if there is no device name in the list.

- 4 Enter the last digit of IP address to allocate to the selected device.

⑤ Click **Apply** to save the changes. You can see the list of reserved IP address. To edit or delete the reserved IP address from the list, click the pencil or trash icon. Click **Add** to add a rule. You can add up to 32 rules.

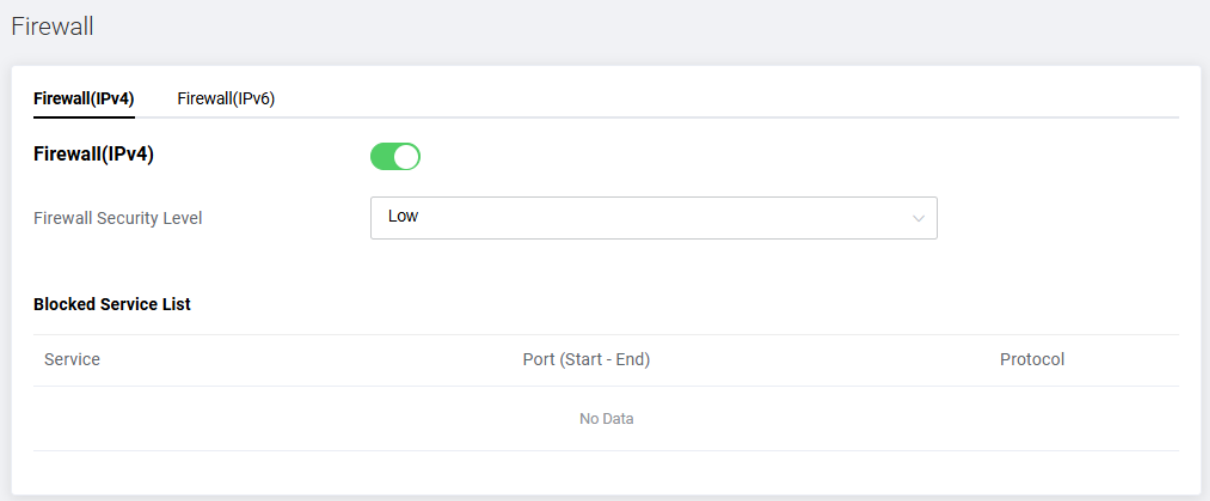
Chapter 8 Providing Network Service

8.1 Firewall

You can configure the filtering rules to prevent network devices from sending outgoing TCP/UDP traffic to the Internet to the Internet via their MAC addresses or your router. It can be useful to prevent unauthorized devices from connecting to your network.

8.1 IPv4

① Enter the **Service > Firewall(IPv4)**.



Firewall

Firewall(IPv4) Firewall(IPv6)

Firewall(IPv4)

Firewall Security Level:

Blocked Service List

Service	Port (Start - End)	Protocol
No Data		

② Select the firewall security level: High, Medium, Low, or Custom. The list of allowed services is shown below based on the selected security level.

- When IPv4 Security Level is set to **High or Medium**: Shows a list of allowed services.
- When Security Level is set to **Low**: no services are blocked.

Firewall

Firewall(IPv4) Firewall(IPv6)

Firewall(IPv4)

Firewall Security Level:

Blocked Service List

Service	Port (Start - End)	Protocol
No Data		

- When Security Level is set to **Custom**:

Firewall

Firewall(IPv4) Firewall(IPv6)

Firewall(IPv4)

Firewall Security Level:

Block HTTP/HTTPS

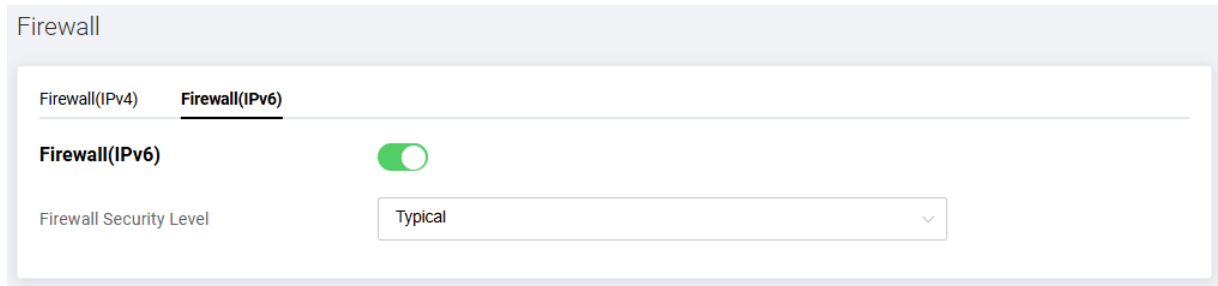
Block ICMP

Block P2P Applications

Block IDENT

Display	Description
Block HTTP/HTTPS	Set whether to block HTTP/HTTPS. Enabling HTTP/HTTPS blocking will restrict web browsing and may affect cloud services, web applications, and other internet-based services.
Block ICMP	Set whether to block ICMP. Enabling ICMP Blocking will disable ping requests and may limit network diagnostics capabilities.
Block P2P Applications	Set whether to block P2P Applications. Enabling P2P applications Blocking will restrict file sharing and may affect video conferencing, online gaming, and other peer-to-peer services.
Block IDENT	Set Whether to block IDENT. Enabling IDENT blocking will block port 113 requests, which may cause delays in email server connections and affect some legacy applications.

- IPv6 is the same as IPv4, so the explanation is omitted.



8.2 DDNS Setting

When DDNS is set, the specified domain name and the changed IP address are linked in real time, so that regardless of whether the IP address is changed or not, the corresponding IP address can be accessed through the domain name.

The DNS service supports Noip.com and dyn.com providers, and to the user, you need to subscribe to the service of the site.

Note:

DNS services require prior registration with Noip.com or dyn.com. you must enter the registered username and password.

- DynDNS : account.dyn.com
- NoIP : <https://www.noip.com/>

① Enter the **Service > DDNS**.

DDNS

DDNS

Service Provider

User Name

Password

Domain Name

Connection Status **Internet disconnected**

IP Address -

② Toggle 'On' to use a DDNS service.

DDNS

DDNS

Service Provider

User Name

Password

Domain Name

Connection Status **Internet disconnected**

IP Address -

③ Enter the option values:

Display	Description
Service Provider	Select a service provider. Select either NoIP or DynDNS.
User Name	Enter the user name or account name provided by the selected service.
Password	Enter the password provided by the selected service.
Domain Name	Enter the domain name to be used. A DDNS address will be generated with the name you have entered.

Display	Description
Connection Status	<p>Displays the connection status to the DDNS server. You can check whether the actual DDNS service is available through the DDNS status message.</p> <ul style="list-style-type: none"> - DDNS Update Successful: The generated DDNS is available for use. - DDNS Update Failed: The generated DDNS is not available for use. - Duplicated Hostname: The host name is already in use. Enter another host name. - Contact Service Provider: An error related to the service occurred. Contact your service provider for troubleshooting.
IP Address	Display the IP address for the DDNS.

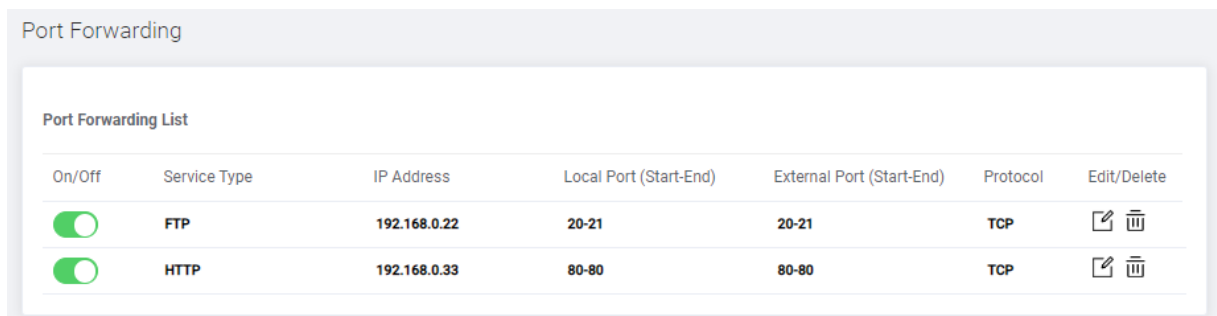
④ Click **Apply** to save the changes.

You can check whether the actual DDNS service is available through the DDNS status message.





8.3 Port Forwarding Rule Setting

Port Forwarding is a Network Address Translation (NAT) application technique that allows direct transmission of data from an external network to a specific device within an internal network. This feature enables access to specific services or applications in the internal network from the outside.

① Enter the **Service > Port Forwarding**.



The screenshot shows the 'Port Forwarding' configuration page. At the top, there is a 'Port Forwarding List' table with the following columns: On/Off, Service Type, IP Address, Local Port (Start-End), External Port (Start-End), Protocol, and Edit/Delete. Two rules are listed:

On/Off	Service Type	IP Address	Local Port (Start-End)	External Port (Start-End)	Protocol	Edit/Delete
<input checked="" type="checkbox"/>	FTP	192.168.0.22	20-21	20-21	TCP	 
<input checked="" type="checkbox"/>	HTTP	192.168.0.33	80-80	80-80	TCP	 

Shows the rules set by the user. Each item can be turned **On** or **Off**, and can be individually edited or deleted by pressing the **Edit** or **Delete** button.

To add an item

Click **Add** below to register a new rule. You can add up to 32 rules.

① Click **Add** to add a rule.

Port Forwarding Rule ×

Service Type

IP Address . . .

Local Port (Start-End) -

External Port (Start-End) -

Protocol

② Enter the option values:

Display	Description
Service Type	Enter the service type or click the input box to select from predefined services. <ul style="list-style-type: none"> When you select a predefined service, the local port, external port, and protocol will be automatically filled with the corresponding values. You can modify these values manually. For manual entry, you can enter up to 16 characters.
IP Address	Enter the IP address of the internal client device running the application.
Local Port (Start-End)	Enter the service port number for the internal client device. <ul style="list-style-type: none"> For a single port, enter the same value in both Start and End fields. For a port range, enter different Start and End port values Enter a number between 1 to 65535.
External Port (Start-End)	Enter the service port of the running application.
Protocol	Select the protocol to be used by the service program. <ul style="list-style-type: none"> Available options: TCP, UDP, or TCP/UDP

Note:

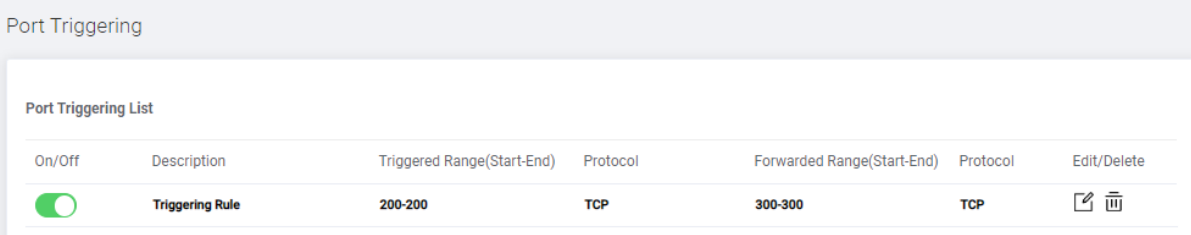
- Multiple service applications can be run on a single device. In such cases, configure different port numbers for the same IP address. Note that the same port cannot be used on two different PCs.
- Since dynamically assigned IP addresses to vary, we recommend you allocate a static IP address.

③ Click **Apply** to save the changes.



8.4 Port Triggering Rule Setting

You can configure a port triggering rule to control communication between internal and external host devices in an IP network. By setting up port triggering, your network devices will have access to the Internet without any interruption.

① Enter the **Service > Port Triggering**.



Port Triggering

Port Triggering List						
On/Off	Description	Triggered Range(Start-End)	Protocol	Forwarded Range(Start-End)	Protocol	Edit/Delete
<input checked="" type="checkbox"/>	Triggering Rule	200-200	TCP	300-300	TCP	 

Shows the rules set by the user. Each item can be turned **On** or **Off**, and can be individually edited or deleted by pressing the **Edit** or **Delete** button.

To add an item

Click **Add** below to register a new rule. You can add up to 10 rules.

① Click **Add** to add a rule.

Port Triggering Rule ✕

Description

Triggered Range(Start-End) -

Protocol

Forwarded Range(Start-End) -

Protocol

② Enter the option values:

Display	Description
Description	Enter a name to identify this rule.
Triggered Range (Start-End)	Enter a triggering range. <ul style="list-style-type: none"> • Enter a number between 1 to 65535.
Protocol	Select the protocol to apply to the triggered ports. <ul style="list-style-type: none"> • Available options: TCP, UDP, or TCP/UDP
Forwarded Range (Start-End)	Enter a forwarding range. <ul style="list-style-type: none"> • Enter a number between 1 to 65535.
Protocol	Select the protocol to be used by the service program. <ul style="list-style-type: none"> • Available options: TCP, UDP, or TCP/UDP

③ Click **Apply** to save the changes.

8.5 DMZ Setting

You can configure the DMZ to make applications free from port restrictions.

When a PC is set to be a DMZ host in the local network, it is totally exposed to the Internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts.

The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host. But, in this case, all ports open, and it may cause security vulnerabilities.

- ① Enter the **Service > DMZ**.

The screenshot shows the 'DMZ' configuration interface. At the top, the label 'DMZ' is followed by a toggle switch that is currently turned off (grey). Below this, the 'Destination' field is populated with the IP address '192.168.1.2', with each octet in its own input box.

- ② Toggle 'On' to enable DMZ host configuration.

The screenshot shows the 'DMZ' configuration interface. At the top, the label 'DMZ' is followed by a toggle switch that is now turned on (green). Below this, the 'Destination' field remains populated with the IP address '192.168.1.2'.

- ③ Enter the Destination (Host IP Address).

- ④ Click **Apply** to save the changes.

8.6 Parental Control Rules

- ① Enter the **Service > Parental Control**.

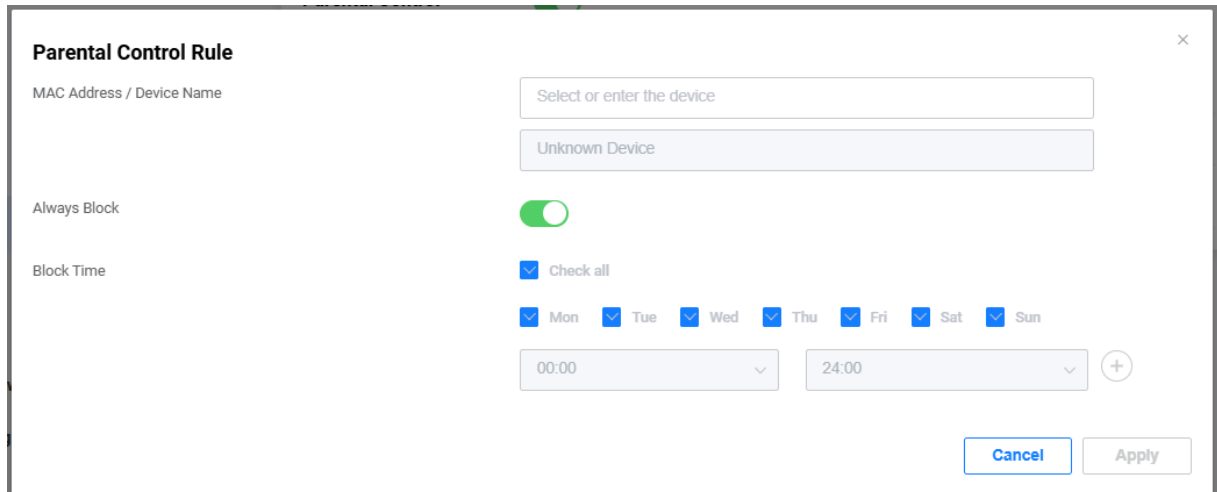
The screenshot shows the 'Parental Control' configuration interface. At the top, the label 'Parental Control' is followed by a toggle switch that is turned on (green). Below this, there is a section titled 'Control Rule List'. Underneath, there is a table with the following headers: 'On/Off', 'MAC Address', 'Device Name', 'Block Schedule', and 'Edit/Delete'. The table body is currently empty, displaying 'No Data' in the center.

On/Off	MAC Address	Device Name	Block Schedule	Edit/Delete
No Data				

To add an item

Click **Add** below to register a new rule. You can add up to 6 rules.

① Click **Add** to add a rule.



② Enter the option values:

Display	Description
MAC Address/Device Name	Set the devices to which you want to restrict access. <ul style="list-style-type: none"> • Select a device from the list of connected devices. • You can enter the MAC address if there is no device name in the list. In this case, you do not need to enter the Device Name.
Always Block	Set whether to Always Block. <ul style="list-style-type: none"> • Enabling Always Block blocks Internet access for registered MAC addresses at all times.
Block Time	Set the blocking time and days. <ul style="list-style-type: none"> • Disabling Always Block allows you to configure dates and times for access control.

③ Click **Apply** to save the changes.

Chapter 9 Setting Advanced Options

You can set the advanced network options. If you are not familiar with network settings, we recommend not to change the settings in the advanced menus. Most users do not need to change these settings.

9.1 Advanced Network Setting

You can block network traffic from any source in several ways.

- 1 Enter the **Advanced > Network**.

Network

Options

WAN ICMPv4 Blocking	<input checked="" type="checkbox"/>
WAN ICMPv6 Blocking	<input checked="" type="checkbox"/>
IP Spoofing Blocking	<input type="checkbox"/>
IPSec Passthrough	<input checked="" type="checkbox"/>
PPTP Passthrough	<input checked="" type="checkbox"/>
L2TP Passthrough	<input checked="" type="checkbox"/>
NAPT/SPI Setting	
TCP Timer	<input style="width: 150px;" type="text" value="3600"/> Seconds !
UDP Timer	<input style="width: 150px;" type="text" value="300"/> Seconds !

- 2 Enter the option values:

Display	Description
WAN ICMPv4 Blocking	Set whether to block WAN ICMPv4. <ul style="list-style-type: none"> • Enabling WAN ICMPv4 Blocking blocks incoming ICMP packets from external networks, preventing ping requests and similar network diagnostics from outside sources.
WAN ICMPv6 Blocking	Set whether to block WAN ICMPv6. <ul style="list-style-type: none"> • Enabling WAN ICMPv6 Blocking blocks incoming ICMP packets from external networks, preventing ping requests and similar network diagnostics from outside sources.
IP Spoofing Blocking	Set whether to block IP Spoofing. <ul style="list-style-type: none"> • Enabling IP Spoofing Blocking prevents unauthorized access by blocking packets with forged (spoofed) source IP addresses.
IPSec Passthrough	Set whether to enable IPSec Passthrough. <ul style="list-style-type: none"> • Enabling IPSec Passthrough allows IPSec tunneled packets to pass through the router, enabling VPN connections that use IPSec protocol.
PPTP Passthrough	Set whether to enable PPTP Passthrough. <ul style="list-style-type: none"> • Enabling PPTP Passthrough allows PPTP tunneled packets to pass through the router, enabling VPN connections that use PPTP protocol.
L2TP Passthrough	Set whether to enable L2TP Passthrough. <ul style="list-style-type: none"> • Enabling L2TP Passthrough allows L2TP tunneled packets to pass through the router, enabling VPN connections that use L2TP protocol.
FTP ALG	Set whether to enable FTP ALG. <ul style="list-style-type: none"> • Enabling FTP ALG allows the router to recognize FTP traffic and handle port connections automatically for FTP transfers.
TFTP ALG	Set whether to enable TFTP ALG. <ul style="list-style-type: none"> • Enabling TFTP ALG allows the router to recognize TFTP traffic and handle port connections automatically for TFTP transfers.
SIP ALG	Set whether to enable SIP ALG. <ul style="list-style-type: none"> • Modern VoIP systems and devices often have built-in mechanisms to handle NAT and routing without the need for SIP ALG. In such cases, it is recommended to disable SIP ALG for professional VoIP setups, as it may conflict with the built-in NAT handling mechanisms.
TCP Timer	Set the TCP timer value between 30 and 432000 (seconds). The default value is 3600 (seconds).

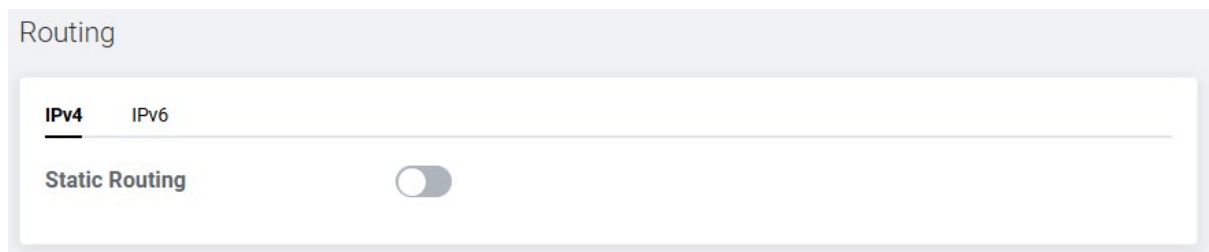
Display	Description
UDP Timer	Set the UDP timer value between 30 and 36000 (seconds). The default value is 300(seconds).

③ Click **Apply** to save the changes.

9.2 Routing Rule Setting

You can manually set the network routing path of packets for data to travel from one network to another with optimal speed and minimal delay.

① Enter the **Advanced > Routing**.



IPv4

② Toggle '**On**' to use a Routing (IPv4).

Routing

IPv4 IPv6

Static Routing

Routing(IPv4) List

No.	Destination IP Address	Subnet Mask	Interface	Gateway	Edit/Delete
No Data					

To add an item

Click **Add** below to register a new rule. You can add up to 32 rules.

① Click **Add** to add a rule.

Routing (IPv4) Rule ×

Destination IP Address . . .

Subnet Mask . . .

Interface LAN WAN

Gateway . . .

② Enter the option values:

Display	Description
Destination IP Address	Enter a destination IP address.
Subnet Mask	Enter a subnet mask of destination IP address. The value is automatically entered, so you do not need to enter it.
Interface	Select the interface type of destination IP address.
Gateway	Enter a gateway address.

③ Click **Apply** to save the changes.

IPv6

① Click Ipv6 and toggle 'On'.

Routing

IPv4 **IPv6**

Static Routing

Routing(IPv6) List

No.	Destination IP Address/Prefix Length	Link Local Address	Interface	Edit/Delete
No Data				

To add an item

Click **Add** below to register a new rule. You can add up to 32 rules.

① Click **Add** to add a rule.

Routing (IPv6) Rule

Destination IP Address: 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

IPv6 Prefix Length: 0

Link Local Address: fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

Interface: LAN WAN

Cancel Apply

② Enter the option values:

Display	Description
Destination IP Address	Enter a destination IPv6 address.
IPv6 Prefix Length	Enter the Prefix Length of IPv6. • The value is automatically entered, so you do not need to enter it.
Link Local Address	Enter the IPv6 link-local address.
Interface	Select the interface type of destination IPv6 address.

③ Click **Apply** to save the changes.

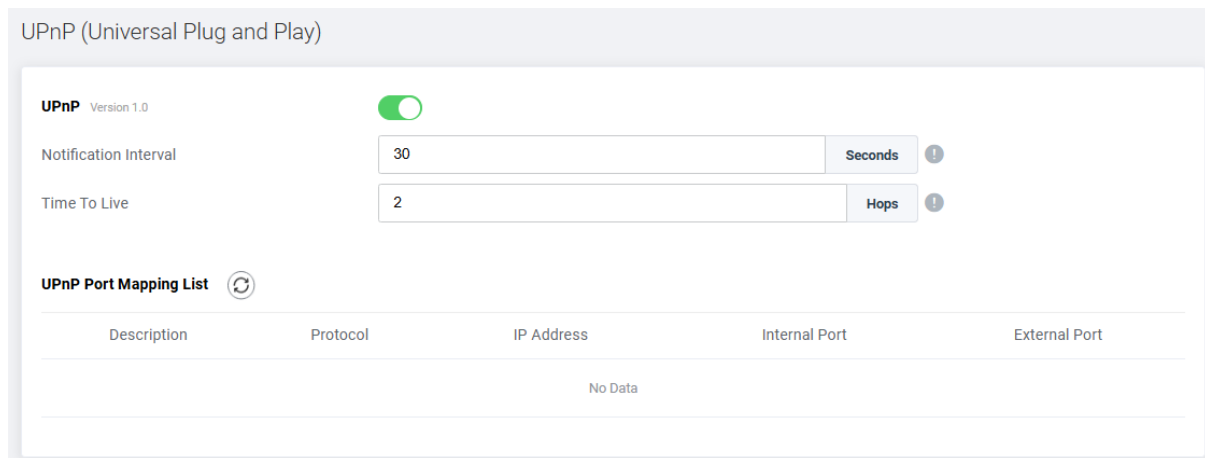
Note:

- In case of IPv6, it is available only if you have subscribed to the service.

9.3 UPnP Setting

UPnP (Universal Plug and Play) is a network protocol that allows devices on a network to discover each other and automatically establish communication without requiring manual configuration. It's commonly used in home networks to enable devices like gaming consoles, smart TVs, IoT devices, and media servers to connect seamlessly with a router or other devices on the same network. UPnP simplifies tasks such as port forwarding, enabling devices to dynamically open and close network ports as needed to communicate with external networks or services.

- 1 Enter the **Advanced > UPnP**.



- 2 Enter the option values:

Display	Description
UPnP	Set whether to support UPnP protocol. <ul style="list-style-type: none"> • Enabling UPnP allows free communication between the host router and client devices.
Notification Interval	Enter the time interval between 15 and 360 in seconds to be notified. <ul style="list-style-type: none"> • The default value is 30 (Seconds).

Display	Description
Time To Live	Enter the TTL value. A packet will be discarded if the hop-count exceeds the value. <ul style="list-style-type: none"> • The default value is 2 (Hops).

③ Click **Apply** to save the changes.

UPnP Port Mapping List

The UPnP table will show the information on each UPnP device that is accessing the router, including what type of port is open and whether that port is still active for each IP address. Click the refresh button to update the UPnP port mapping table.

Note: If you want to use applications such as multiplayer gaming, peer-to-peer connections, real-time communications like an instant messaging or remote assistance (a feature in Windows OS), enable UPnP. Free the improved network connections with UPnP.

9.4 Diagnosing

You can diagnose the network connection problems with the ping test or traceroute.

① Enter the **Advanced > Diagnostic**.

Diagnostics

Utility: Ping Test

Protocol Type: IPv4

Target: IP Address Domain Name

IP Address: . . .

Ping Size: 64 Bytes

Ping Count: 4

Ping Interval: 1000 ms

Start

Results

Clear

② Select the **Utility** type either Ping Test or Traceroute. According to the test type, the following options will be changed.

- **Ping Test:** Method for checking if your PC is connected to a network. It also determines the latency or delay between two PCs.
- **Traceroute:** Method for recording the route through the Internet between your PC and a specified destination device. It also calculates and displays the amount of time each hop took.

③ Enter the Option Values:

Ping Test

Diagnostics

Utility: Ping Test

Protocol Type: IPv4

Target: IP Address Domain Name

. . .

Ping Size: 64 Bytes

Ping Count: 4

Ping Interval: 1000 ms

Results

Display	Description
Protocol Type	<ul style="list-style-type: none"> Select either "IPv4" or "IPv6."
Target IP Address/Domain Name	<ul style="list-style-type: none"> Enter the IP address or domain name to transmit ping packets.
Ping Size	<ul style="list-style-type: none"> Enter the size of the ping packet between 64 and 1518. The default setting is 64.
Ping Count	<ul style="list-style-type: none"> Enter the number of pings between 1 and 256. The default setting is 4.
Ping Interval	<ul style="list-style-type: none"> Enter the interval for transmitting pings between 100 and 3600000. The default setting is 1000.

Traceroute

Diagnostics

Utility: Traceroute

Protocol Type: IPv4

Target: IP Address Domain Name

Traceroute Maximum TTL: 20 Hops ⓘ

Start

Results

Clear

Display	Description
Protocol Type	<ul style="list-style-type: none"> Select either "IPv4" or "IPv6."
Target IP Address/Domain Name	<ul style="list-style-type: none"> Enter the IP address or domain name to transmit ping packets.
Traceroute Maximum TTL	<ul style="list-style-type: none"> Set the maximum effective duration for the transmitted packets. The available setting range is between 1 and 30, and the default setting is 20.

④ Click **Start** to run the test.

Check the test results in the table below.

⑤ You can use the results to rule out a connection issue or identify where in the network the issue is occurring. To clear the results, click **Clear**.

9.5 Statistics

Provides detailed packet information or error information for WAN, LAN, 2.4GHz, and 5GHz.

Statistics								
WAN Statistics								
Description	Received Bytes	Received Packets	Received Errors	Received Discards	Sent Bytes	Sent Packets	Sent Errors	Sent Discards
rg	0	0	0	0	0	0	0	0
voice	0	0	0	0	0	0	0	0
LAN Statistics								
Port	Received Bytes	Received Packets	Received Errors	Received Discards	Sent Bytes	Sent Packets	Sent Errors	Sent Discards
LAN1	24558982	269514	0	0	8049392	35392	0	0
LAN2	0	0	0	0	0	0	0	0
LAN3	18168274	200877	0	0	3687491	22434	0	0
LAN4	0	0	0	0	0	0	0	0
2.4GHz Statistics								
Network Name(SSID)	Received Bytes	Received Packets	Received Errors	Received Discards	Sent Bytes	Sent Packets	Sent Errors	Sent Discards
HNW_2.4G_6986E8	0	0	0	30	35949095	425191	0	74
5GHz Statistics								
Network Name(SSID)	Received Bytes	Received Packets	Received Errors	Received Discards	Sent Bytes	Sent Packets	Sent Errors	Sent Discards
HNW_5G_6986E8	0	0	0	14	35950382	425205	0	75

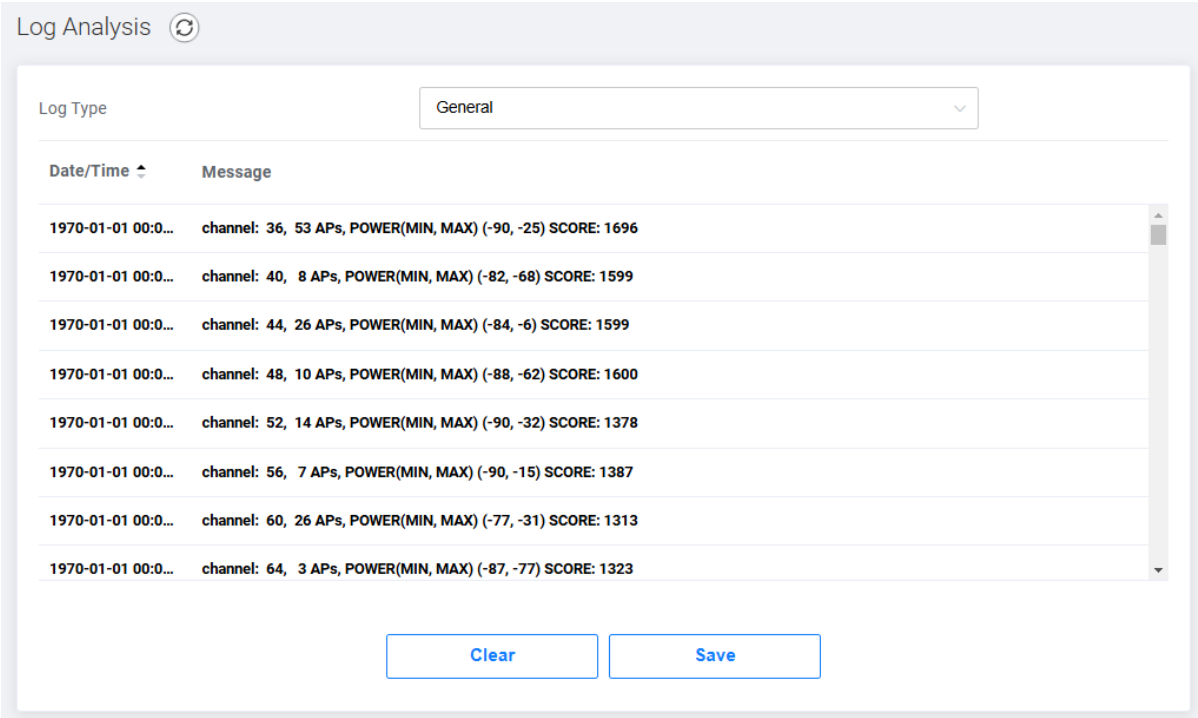
Chapter 10. Managing the System


10.1 Log Analysis

Log analysis provides a chronological view of common events such as system boots, network status changes, and interfaces going up/down.

① Enter the **Management > Log Analysis**.

You can check the log of 'General' Type. 'General' log type refers to general communication log data excluding security logs.



Log Analysis 

Log Type:

Date/Time ↑	Message
1970-01-01 00:0...	channel: 36, 53 APs, POWER(MIN, MAX) (-90, -25) SCORE: 1696
1970-01-01 00:0...	channel: 40, 8 APs, POWER(MIN, MAX) (-82, -68) SCORE: 1599
1970-01-01 00:0...	channel: 44, 26 APs, POWER(MIN, MAX) (-84, -6) SCORE: 1599
1970-01-01 00:0...	channel: 48, 10 APs, POWER(MIN, MAX) (-88, -62) SCORE: 1600
1970-01-01 00:0...	channel: 52, 14 APs, POWER(MIN, MAX) (-90, -32) SCORE: 1378
1970-01-01 00:0...	channel: 56, 7 APs, POWER(MIN, MAX) (-90, -15) SCORE: 1387
1970-01-01 00:0...	channel: 60, 26 APs, POWER(MIN, MAX) (-77, -31) SCORE: 1313
1970-01-01 00:0...	channel: 64, 3 APs, POWER(MIN, MAX) (-87, -77) SCORE: 1323

- **Clear** Button: Clear all the result of the log.
- **Save** Button: Save the current logs to a file.

Note:

- Log information is automatically deleted when the product is turned off.
- If you have never been connected to the Internet, the date may differ from the actual date.

10.2 Factory Reset/Restart

You can factory reset the product or restart it.

① Enter the **Management > Factory Reset/Restart**.

Factory Reset/Restart

Factory Reset	<input type="button" value="Factory Reset"/>
Backup	<input type="button" value="Backup"/>
Restore	<input type="text" value="Choose the file"/> <input type="button" value="Browse"/>
	<input type="button" value="Restore"/>
<hr/>	
Restart	<input type="button" value="Restart"/>

- **Factory Reset** Button: Click **Factory Default** to restore to the factory default settings. Then, the system will restart and it may take a few minutes.

Warning

- If you perform a factory reset, all current settings will be lost. If you want to keep the current settings, use the Backup function to back up the current settings. After a factory reset, you can restore the current settings using the Restore function.

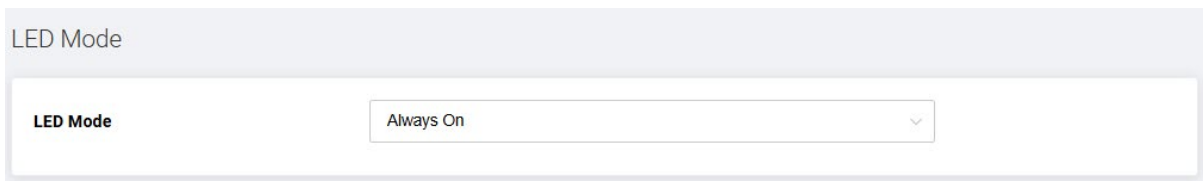
- **Backup** Button: Click **Backup** to save the current configuration. The backup file name is Setting_HPE30E.bin.
- **Restore** Button: To restore a saved backup file, click **Browse** to select the backup file. After selecting, click the [Restore] button to restore. After restoration, the system will restart and may take several minutes.
- **Restart** Button: Click **Restart** to restart the system.

Note:

- In order to complete the Factory Reset/Restore/Restart must be restart. All services cannot be used during the reboot.
- Restore and backup features are only possible on the same product.

10.3 LED Mode

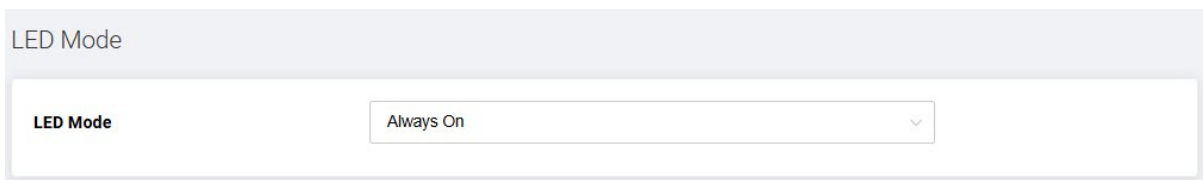
① Enter the **Management > LED Mode**.



LED Mode

LED Mode

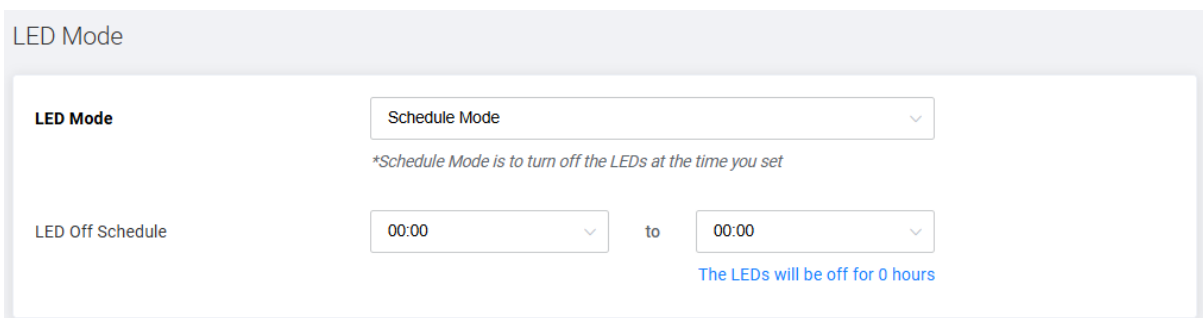
② Select the LED Mode Type.



LED Mode

LED Mode

- **Always On:** Always turn on all LEDs.
- **Always Off:** Always turn off all LEDs.



LED Mode

LED Mode

**Schedule Mode is to turn off the LEDs at the time you set*

LED Off Schedule to

The LEDs will be off for 0 hours

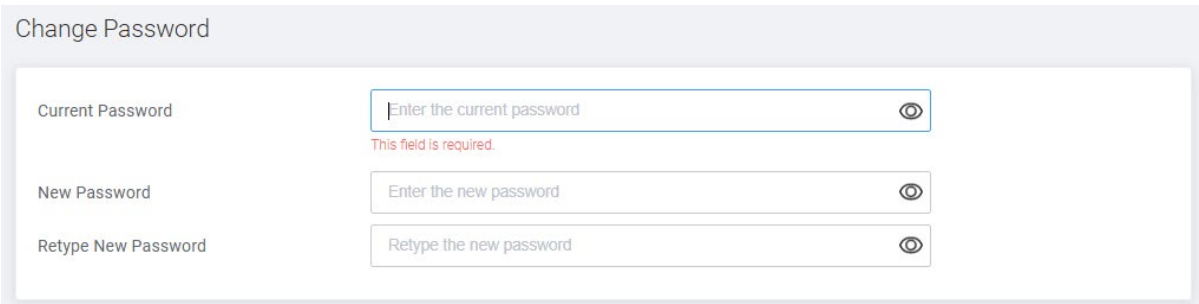
- **Schedule Mode:** Turns off all LEDs only at the set time. Set the time you want to turn off the LEDs in the 'LED Off Schedule' item.
-

③ Click **Apply** to save the changes.

10.4 Change Password

You can change the password required when logging in to the Web UI.

① Enter the **Management > Change Password**.



Change Password

Current Password	Enter the current password	👁
	This field is required.	
New Password	Enter the new password	👁
Retype New Password	Retype the new password	👁

- **Current Password:** Enter the current password. The default password is printed on the product label.
- **New Password:** Enter a new password. The new password can be from 6 to 64 characters A-Z, a-z, 0-9, and all characters. A combination of letters and numbers is recommended.
- **Retype New Password:** Enter the new password again.

② Click **Apply** to save the changes.

Note:

- If you lose your password, you must perform a factory reset, which will erase all custom settings.

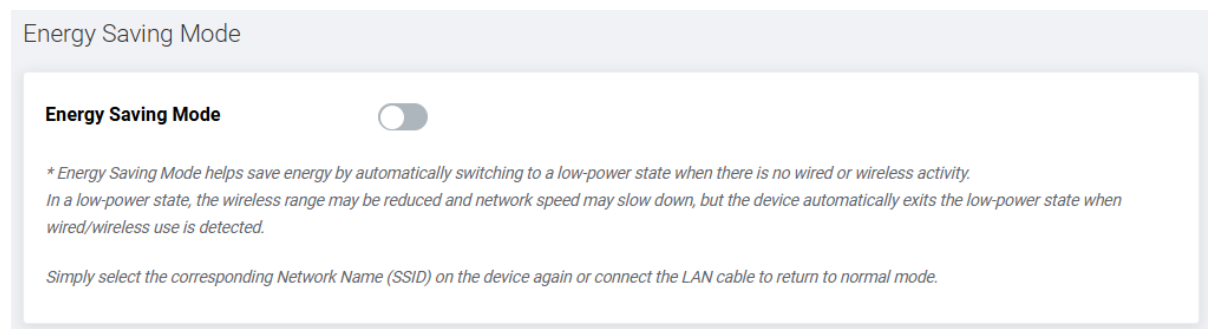
10.5 Energy Saving Mode

Energy saving mode automatically switches to low power mode (under 8W) when there is no wired/wireless activity on the product to save energy. When in low power mode, wireless coverage is reduced to maintain only minimal connections, and wired connections may also have reduced network speeds.

When wired/wireless activity is detected (SSID is re-selected, LAN cable is re-plugged in), low power mode is terminated and returns to normal mode.

Energy saving mode is only supported for European products.

① Enter the **Management > Energy Saving Mode**.



② Toggle **On** to use Energy Saving Mode.

Note:

- When low power mode is running, you can check it through LED Color. 2.4GHz, 5GHz LEDs are displayed in White Color.

10.6 Date/Time


You can set the date and time of the product.

When connected to the Internet, the current time is automatically set. If correction is required, you can set it manually.

① Enter the **Management > Date/Time**.







You can check the currently set time.

Date/Time

1970.01.01 07:21:48 

Time Zone (GMT+01:00) Ceuta, Longyearbyen, Amsterdam, Andorra, Belgrade, Bei ▾

NTP (Network Time Protocol) Server List

No.	Description	Server URL	Edit/Delete
1	NTP Server 1	0.pool.ntp.org	 
2	NTP Server 2	1.pool.ntp.org	 
3	NTP Server 3	2.pool.ntp.org	 

- **Time Zone:** Set the Time Zone.

NTP(Network Time Protocol) Server List

It shows the rules set by default. You can edit or delete items by clicking **Edit** or **Delete**. It is recommended to modify it only if necessary.

② Click **Apply** to save the changes.

10.7 Remote Access

You can set whether to allow remote access.

① Enter the **Management > Remote Access**.

Remote Access

Remote Access

② Toggle **On** to use Remote Access.

Remote Access

Remote Access

Remote Access Port ⓘ

HTTPS Access

ⓘ Remote Access(IPv4): -
Remote Access(IPv6): -

Remote Access Control

③ Enter the option values:

Display	Description
Remote Access	Toggle to use Remote Access or not.
Remote Access Port	Set the port used for remote access. • Enter a number between 1 to 65535.
HTTPS Access	Set whether to allow HTTPS Access. • Enabling HTTPS access allows HTTPS access connections.
Remote Access Control	Set whether to use the Remote Control Access feature. • Enabling Remote Access Control allow only registered devices to access remotely.

④ Click **Apply** to save the changes.

Chapter 11. Voice

11.1 Status

① Enter the **Voice > Status**.


Status

Voice Status List					
Line	Registration	Line Status	Telephone Number	Extension Number	Description
Tel 1	Unregistered	On-Hook		***1	
Tel 2	Unregistered	On-Hook		***2	

View the connection status, telephone number and extension number of telephone lines connected to Tel ports 1 and 2.

11.2 Call History

① Enter the **Voice > Call History**.

Call History 

Call History List							
Date	Number/Name	Call Type ↕	Duration	Line	Allow/Block	Phone Block	Delete
No Data							

Shows call history for both incoming and outgoing calls, arranged by date. Individual call records can be deleted.

Chapter 12. Troubleshooting

You can find information to diagnose and solve problems you might have with your product. Before contacting the customer service center, make sure to read the tips below carefully. If the problem persists after you complete the following procedure, please contact the customer service for further instructions.

√ The product does not work

- Check the Power LEDs light green.
- Check the power adaptor is plugged into a suitable power outlet.
- Connect the power adaptor to another power outlet.
- Restart the system and wait until the Power LEDs light green.

√ Cannot access the web interface

- Check the Ethernet cable is correctly connected between the product and PC.
- If the PC is connected to the Wi-Fi, check with the SSID the connected product is correct.
- Try to access with IP address 192.168.1.1.
- Power off the product by detaching the power adaptor and then restart the system within a few seconds.

√ Cannot log in to this product

- Check the IP address of your PC is on the same subnet as the product.
- Check your login information is correct. The default password is printed on the label of your product. The password is case-sensitive.

√ Cannot remember the login password

- Reset the product to the factory settings. Press the reset button for 3 seconds. Then, log in to the product with a default password. The password is printed on the label of your product.

√ Cannot search for SSID on the network devices

- Check if the wireless Radio is enabled or not in Wireless > Basic Setting.
- Check if Hide SSID feature is turned on in Wireless > Primary Wireless.

√ Cannot remember the Wi-Fi password

- Go to Home menu and click the eye icon at the password option. You can change the password in Wireless > Primary Wireless.

√ If the product lasts a long time with high temperature,

- If the temperature of the CPU is over 110 degrees Celsius or the wireless interface is maintained over 110 degrees Celsius for more than 300 seconds, the system will be shutdown Wi-Fi interfaces and degrade 10G LAN to 1Gbps. 2.4GHz and 5GHz LEDs are off and Wi-Fi (wireless) is not available. (Cutoff Stage 1)
- In Cutoff Stage 1, if the cumulative duration lasts more than 600 seconds, the system will be shut down all LAN interfaces. All of the LAN port LEDs on the back are turned off, and LAN (wired) cannot be used. (Cutoff Stage 2)
- In Cutoff Stage 2, when the CPU temperature lasts more than 120 degrees and more than 60 seconds, the system automatically reboots. (Cutoff Stage 3)
- When the temperature of the CPU falls below 90 degrees for more than 60 seconds, all interfaces are restored.

√ Can check the detailed status of the system through log data.

Chapter 13. Supplemental Information

13.1 Safety and Regulatory Information

Please read these instructions carefully before installation/use, and install/use correctly. The precautions given are intended to help you use the product safely and correctly and prevent harm or damage to you or others.

Installation Safety

- Conducted only by professional installer who has been accurately trained.
- Use only the power adapter provided. Using a different one may cause device damage.
- The power supply must be connected to a main outlet with a protective earth connection.
- Do not defeat the protective earth connection.
- Do not install the device in wet or damp conditions.
- Do not install near heat sources such as fire, boilers, or air conditioners.
- Do not install in a location where electromagnetic interference (EMI) does not occur.

Laser Safety

Invisible laser radiation may be emitted from disconnected fibers or connectors. Never stare into beams or look directly to optical connectors.

- Invisible radiation might be emitted from the aperture of the port when no fiber cable is connected.

Usage Caution

Please read these instructions before using your product. We do not want you to get hurt or your product to get damaged.

- Do not place any object on the device to avoid damaging the device.
- Do not open the enclosure without permission and technical support, which voids

the provider's warranty.

- If need to clean the dust of the equipment, please cut off the power supply first and unplug the relevant connecting cable, then use dry cloth to clean, do not use any liquid.
- Power off the device and unplug the cables when the device is not using for a long Time.

13.2 Specification

10 LEDs	
Power, PON, LOS, Internet, TEL 1, TEL 2, 2.4GHz, 5GHz, Upgrade, WPS	
2 Buttons	
WPS (Front), Reset (Back panel)	
Interface	
Fiber Optical Interface	1 x SC/APC Optical Interface Supports EPON (Transmitting: 1270 nm, Receiving: 1577 nm)
LAN Ports	LAN 1~3 : 3 x 1 Gigabit Ethernet (RJ-45) - 1G/100M/10Mbps (Full Duplex) 10G : 1 x 10 Gigabit Ethernet(RJ-45) - 10G/5G/2.5G/1G/100Mbps (Full Duplex)
TEL	2 x FXS (RJ-11)
Wireless (2.4GHz)	
Frequency	2,400~2,484MHz : 1~13ch
802.11 Mode	IEEE802.11 b/g/n/ax
Transmission Speed	IEEE802.11ax up to 1147Mbps (HE40)
	IEEE802.11n up to 600Mbps (HT40)
	IEEE802.11g up to 54Mbps
	IEEE802.11b up to 11Mbps
Antenna	4(Tx) x 4(Rx) Internal Antenna
Wireless (5GHz)	
Frequency	[W52] 5.2GHz (5,150~5,250MHz) : 36/40/44/48ch
	[W53] 5.3GHz (5,250~5,350MHz) : 52/56/60/64ch
	[W56] 5.6GHz (5,470~5,730MHz) : 100/104/108/112/116/120/124/128/132/136/140ch
802.11 Mode	IEEE802.11 a/n/ac/ax
Transmission Speed	IEEE802.11ax up to 4803Mbps (HE160)
	IEEE802.11ac up to 3466Mbps (VHT160)
	IEEE802.11n up to 600Mbps (HT40)
	IEEE802.11a up to 54Mbps
Antenna	4(Tx) x 4(Rx) Internal Antenna
Environmental	
Input	AC100-240V ~ 50/60Hz

Output	DC12V, 2A (Standby under 8W)
Operating Temperature	0° ~ 40°C
Storage Temperature	-20°C ~ 60°C
Operating Humidity	10% ~ 95% (Non-condensing)
Physical Specification	
Dimension	52.2 (H) x 204 (W) x 230 (D) mm (with foot)

Note:

* Depending on the usage environment and connected devices, it may be connected with a lower bandwidth than the actual setting.

* The maximum speed is the theoretical speed according to the standard, and the actual data transmission speed may vary depending on the usage environment and connected devices.