User Manual

BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway

Table of Contents

User Manual Overview

User Manual Overview

This manual provides detailed instructions and information for the BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway. It is designed for technical users who wish to fully understand and configure their device for optimal performance.

1. Introduction

1.1 Purpose of this Manual

This User Manual serves as a comprehensive guide for the BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway. It provides in-depth instructions on connecting, configuring, and maintaining your device to ensure robust and efficient network experience. For experienced users, this document delves into advanced configurations, while fundamental sections are also included for those seeking a thorough understanding of the device's capabilities.

1.2 About the BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway

The BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway is a high-performance Home Gateway Unit (HGU) designed to deliver blazing-fast AX3000 Wi-Fi and Gigabit Ethernet speeds. It is engineered to provide full-service access with high bandwidth, high performance, high reliability, and ease of operation, administration, and maintenance, meeting the evolving demands of modern customers. This device is an ideal solution for high-streaming, online gaming, and smart home environments, offering ultimate connectivity for a wide range of dual-band Wi-Fi devices.

1.3 Key Features

The BIN62X2PLIRT boasts a comprehensive set of features tailored for advanced networking requirements:

- **Introducing 802.11ax Wi-Fi 6:** Supports the latest Wi-Fi standard for enhanced performance and efficiency.
- **Blazing Fast Wireless Speed:** Delivers up to 3000Mbps† wireless speeds.
- **Band Steering Support:** Optimizes client connections by steering devices to the most appropriate Wi-Fi band (2.4GHz or 5GHz).
- **Optimal for High-Demand Applications:** Great for high streaming, online gaming, and smart home devices.
- **Ultimate Connectivity:** Provides ultimate connectivity for the latest dual-band Wi-Fi devices such as smartphones, tablets, smart TVs, and more.
- **High Device Capacity:** Supports at least 50 simultaneous device connections.
- **Dual LAN GE Ports:** Equipped with two 10/100/1000Mbps Gigabit Ethernet LAN ports for wired connections.

- **Dual Band Wi-Fi:** Offers simultaneous dual-band Wi-Fi (2.4 GHz and 5 GHz) to avoid wireless interference and ensure top Wi-Fi speeds.
- **Advanced Quality of Service (QoS):** Includes advanced QoS capabilities to prioritize network traffic.
- **Wi-Fi Boost:** Features high-power radio amplifiers for extended Wi-Fi coverage.
- **Robust Protocols:** Supports PPPoE, IPOE, IPv4/6, DNS, DHCP Server, NAPT, IGMP, Dynamic DNS, TCP/UDP/Port Filtering, and WPA/WPA2/WPA3 Security.

1.4 Target Audience

This manual is intended for technical users, network administrators, and individuals with a solid understanding of networking concepts and terminology. While basic setup instructions are provided, the manual also delves into advanced configurations that require deeper technical knowledge to implement effectively.

1.5 Document Conventions

This document employs specific conventions to ensure clarity and ease of understanding.

1.5.1 Notational Conventions

- **Acronyms:** All acronyms are defined upon their first appearance in the text and are also listed in the Glossary for quick reference.
- **Device Reference:** For brevity, the BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway is often referred to as "the device" or "the gateway."
- **LAN:** The term "LAN" refers to a Local Area Network, typically a group of Ethernet-connected computers within a single site.

1.5.2 Typographical Conventions

- *Italic text*: Used for items that you select from menus, drop-down lists, and the names of displayed web pages.
- **Bold text**: Used for text strings that you are required to type when prompted by the program, and to emphasize important points or warnings.

1.5.3 Special Messages

This document utilizes specific icons to highlight important information or instructions:

- **Note:** Provides clarifying or non-essential information related to the current topic.
- **Definition:** Explains terms or acronyms that may be unfamiliar. These terms are also included in the Glossary section.
- **WARNING:** Indicates messages of high importance, including those related to personal safety or the integrity of the system.

1.6 Getting Support

For technical assistance or if you encounter issues that cannot be resolved using this manual, please contact your Internet Service Provider (ISP) or the device vendor. You may be asked to provide details about your device's hardware and firmware versions, which can be found in the device's web configuration interface under the "Status" or "Device Info" sections.

2. Package Contents

This section details the items you should find included with your BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway. Please check the package carefully upon receipt to ensure all components are present and undamaged.

2.1 Standard Package Items

The standard package for your BIN62X2PLIRT device typically includes:

- **BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway:** The main device unit.
- **Quick Installation Guide:** A brief guide for initial setup.
- **Ethernet Cable (RJ-45):** For connecting the device to your computer or other network devices.
- **Power Adapter:** The power supply unit for the gateway.

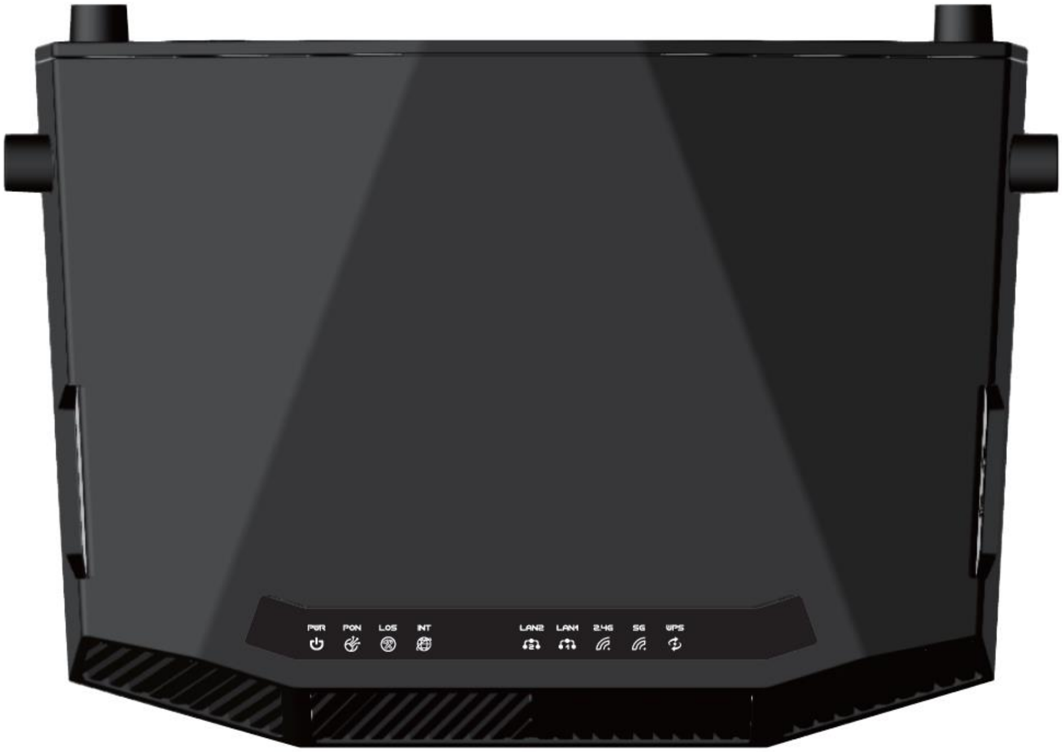
3. Hardware Overview

This section provides a detailed overview of the BIN62X2PLIRT's physical components, including its front panel indicators and rear panel connectors. Understanding these elements is crucial for proper installation and operation.

3.1 Front Panel

The front panel of the BIN62X2PLIRT features a series of LED indicators that provide a quick visual status of the device's operation.

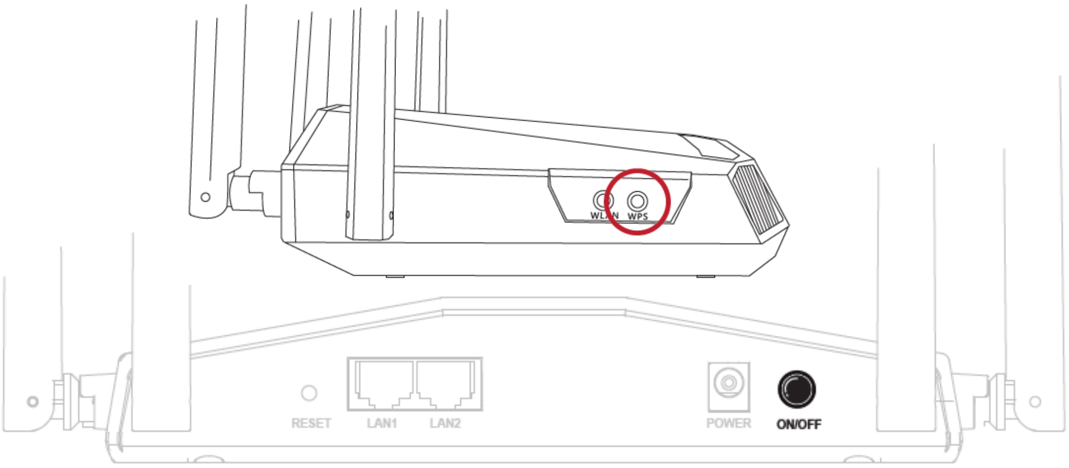
Figure 3.1. Front Panel View



3.2 Rear Panel Connectors and Buttons

The rear panel of the BIN62X2PLIRT houses all the essential ports and buttons for connectivity and device management.

Figure 3.2. Rear Panel View



The following table describes the function of each connector and switch on the device:

Connector	Description
POWER	DC jack that connect to your BIN62X2PLIRT 12Vdc power adapter.
Power On/Off Button	Controls the power supply to the device. Press to turn the device on or off.
SC / APC (B+) GPON WAN Port	This is the primary WAN (Wide Area Network) port for connecting to your Gigabit Passive Optical Network (GPON) fiber optic line.
LAN1 / LAN2	RJ-45 Gigabit Ethernet Jacks (10/100/1000Mbps). These ports connect the device to your personal computer (PC), gaming console, smart TV, or a network hub/switch for local network connectivity.
RESET	**Reset Button:** This button is used to reset the BIN62X2PLIRT to its default factory settings. To perform a factory reset, press and hold this button for at least 5 full seconds.
WPS	**WPS Button:** Wi-Fi Protected Setup (WPS) button. Press this button for at least 3 full seconds to initiate the WPS process. The WPS LED indicator will flash, indicating that WPS is active for two minutes. During this time, activate WPS on your wireless client device to establish a secure connection without entering the password.
WLAN	**WLAN Button**: A dedicated button to enable or disable the Wi-Fi (wireless) functionality of the device.

3.3 Physical Specifications

The physical characteristics of the BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway are as follows:

- **Dimensions:** 185 x 150 x 35 mm
- **Power Supply:** DC 12V, 1.5A
- **Antennas:** External Wi-Fi Antennas (2x2 for 2.4GHz, 2x2 for 5GHz)

4. Installation & Setup

This section guides you through the process of physically installing your BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway and configuring your computer for network access. It is crucial to follow each step carefully to ensure proper setup and functionality.

4.1 Safety Precautions Before Installation

WARNING:

- Ensure the device is placed on a stable, flat surface away from direct sunlight, heat sources, and moisture.
- Do not block ventilation openings, as this can lead to overheating.
- Use only the power adapter supplied with the device. Using unauthorized power adapters may damage the device and void your warranty.
- Before connecting or disconnecting any cables, ensure the power adapter is unplugged from the wall outlet.

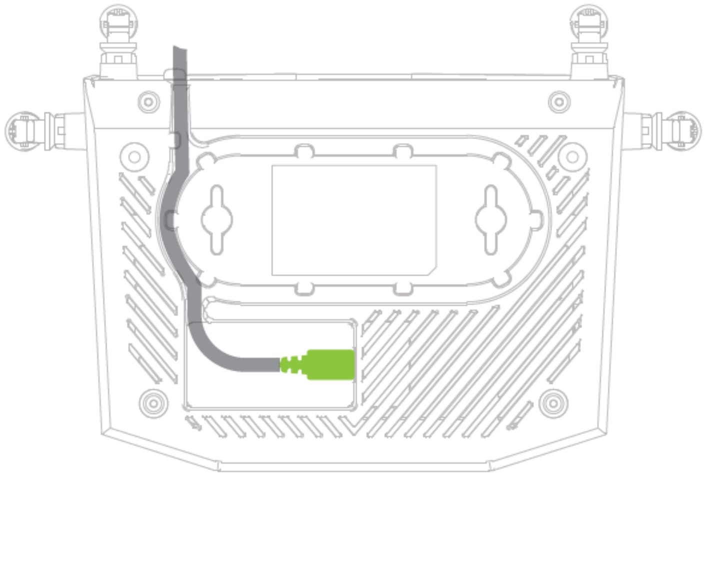
4.2 Physical Connection

The BIN62X2PLIRT connects to your network differently depending on your Internet Service Provider's (ISP) setup. This device is primarily designed for GPON networks.

4.2.1 Connecting to a GPON Network

Follow these steps to connect your BIN62X2PLIRT to a GPON fiber optic network:

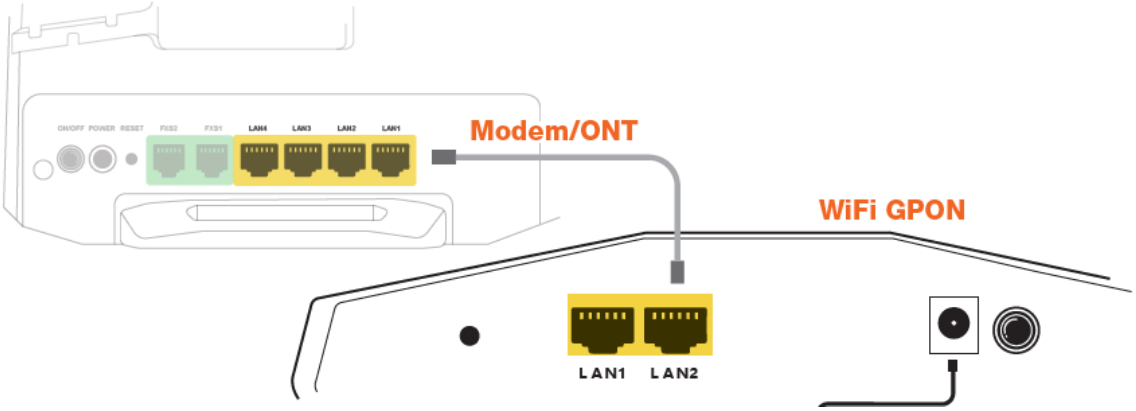
1. **Connect Fiber Optic Cable:** Connect the fiber optic cable from your GPON wall outlet to the **SC / APC (B+) GPON WAN Port** on the rear panel of your BIN62X2PLIRT. Ensure the connection is secure but do not force it.
    - Figure 4.1. GPON Connection Diagram



4.2.2 Connecting to an Ethernet WAN

If your ISP provides internet service via an Ethernet cable (e.g., from a separate fiber optic modem or a cable modem), you would typically connect that Ethernet cable to a WAN port on a router. The BIN62X2PLIRT has a dedicated GPON WAN port. If your setup requires an Ethernet WAN connection, consult your ISP for specific instructions, as this device is optimized for GPON.

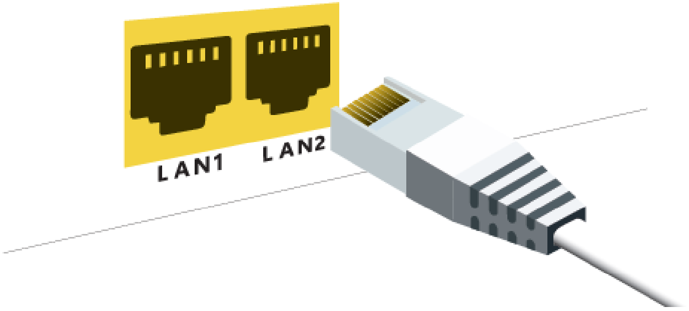
- Figure 4.2. LAN Connection Ethernet WAN



4.2.3 Connecting Local Devices

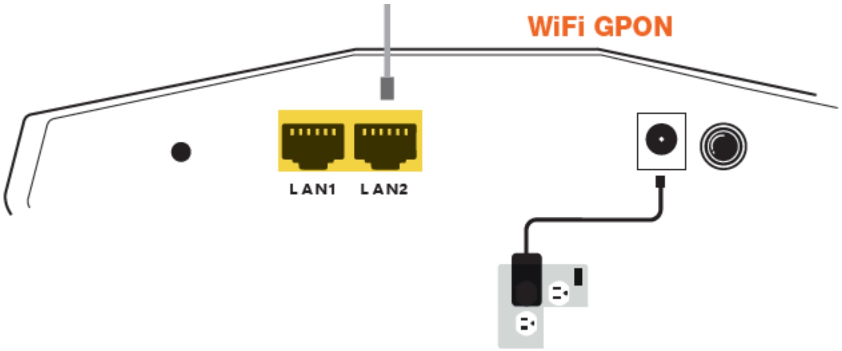
Connect your computers and other network devices to the BIN62X2PLIRT:

1. **Connect Ethernet Devices:** Use an RJ-45 Ethernet cable (supplied) to connect your PC's Ethernet port to any of the **LAN1** or **LAN2** Gigabit Ethernet ports on the rear panel of the BIN62X2PLIRT.
   - Figure 4.3. LAN Connection Diagram



4.2.4 Powering On the Device

1. **Connect Power Adapter:** Connect the supplied power adapter to the **POWER** inlet (DC Jack) on the rear panel of the BIN62X2PLIRT.
2. **Plug into Wall Outlet:** Plug the other end of the power adapter into a standard electrical wall outlet.
3. **Turn On Power:** Press the **Power On/Off Button** on the rear panel to turn on the device.
   - Figure 4.4. Power Connection Diagram



Once powered on, the LED indicators on the front panel will begin to illuminate as the device boots up. Refer to Section 5, "LED Indicator Description," for details on what each light signifies.

4.3 Computer Configuration for Automatic IP Address

Before configuring the BIN62X2PLIRT, it is essential to ensure your computer is set to obtain an IP address and DNS server address automatically via DHCP. This is the default and recommended setting for most home networks.

4.3.1 Windows Operating Systems

The steps to configure your computer for automatic IP address acquisition are similar across various Windows versions.

- **For Windows 11:**
  1. Click the **Start** button and select **Settings**, or press **Windows key + I**.
  2. Go to **Network & Internet**, then click on **Ethernet** (or **Wi-Fi**, depending on your connection).
  3. Scroll down and click **Edit** next to **IP assignment**.
  4. In the pop-up window, set **IP settings** to **Automatic (DHCP)**.
  5. Also set **DNS server assignment** to **Automatic (DHCP)**.
  6. Click **Save** to apply the changes.

- **For Windows 10:**

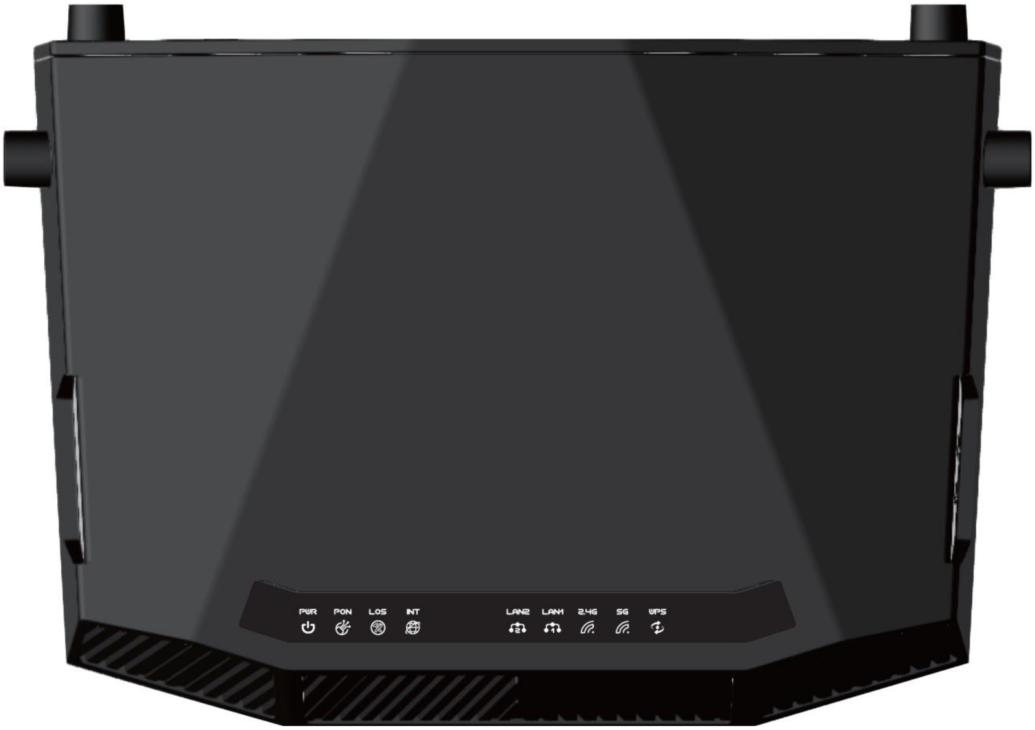
1. Move the mouse cursor or tap to the upper-right corner of the screen and click on **Settings**.
2. In the Control Panel Home, click on **Change adapter settings**.
3. Right-click on **Ethernet** (or "Local Area Connection" for older versions) and then click **Properties**.
4. Double-click on **Internet Protocol Version 4 (TCP/IPv4)**.
5. Ensure **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
6. Click **OK** to save the changes and close the windows.

5. LED Indicator Description

The BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway is equipped with various LED indicators on its front panel. These lights provide real-time status updates on the device's operation, network connectivity, and wireless activity. Understanding the meaning of each LED can help you quickly assess the device's status and diagnose potential issues.

5.1 Understanding the LED Indicators

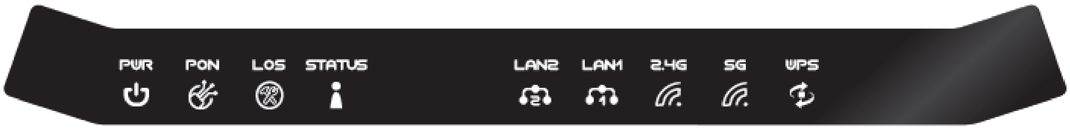
Figure 5.1. LED Indicators

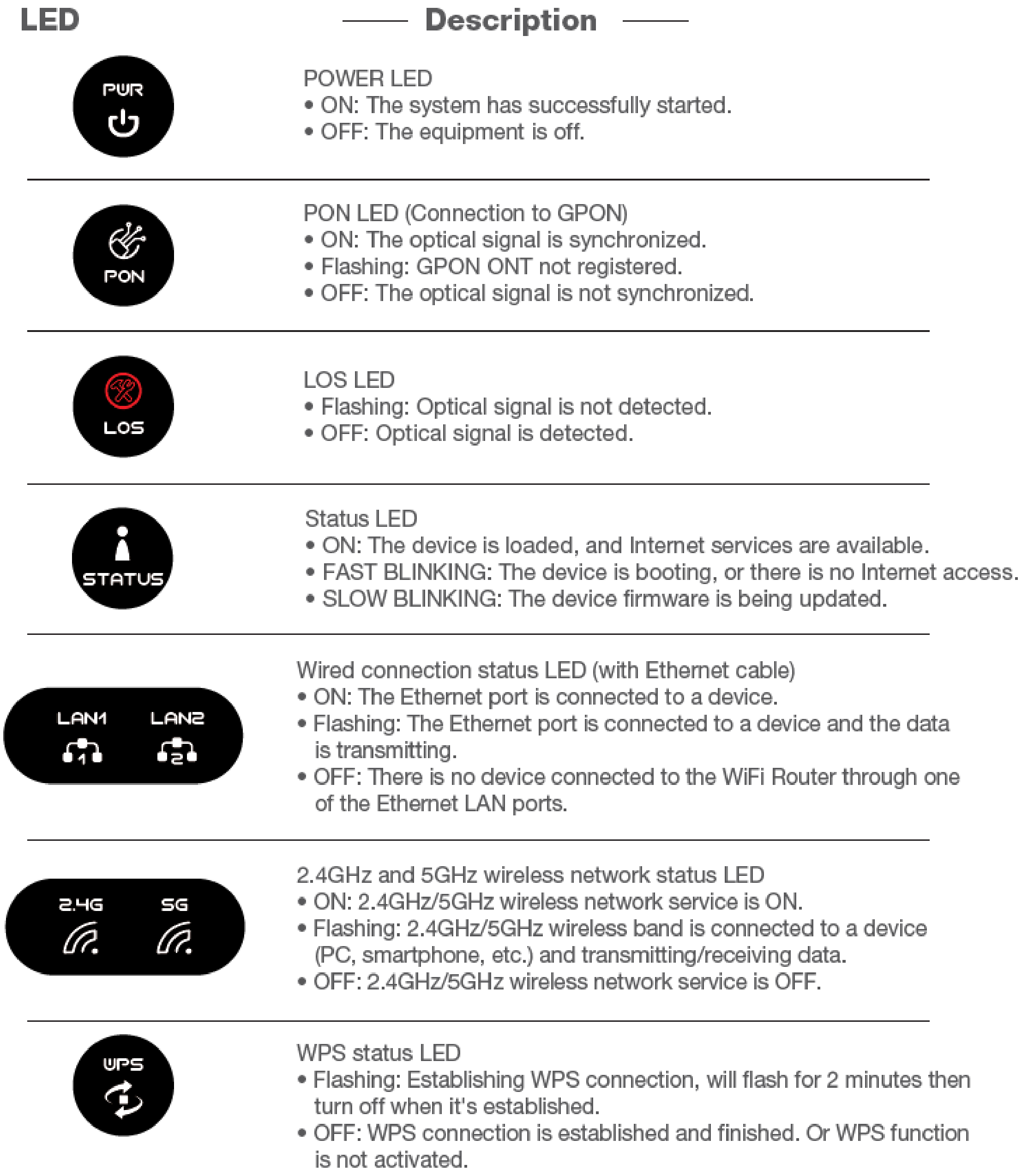


5.2 LED Function Table

The following table explains the function, color, and behavior of each indicator light on your BIN62X2PLIRT.

Note: The specific behavior (e.g., color) of some LEDs might vary slightly based on firmware versions. Always refer to this table for the general interpretation.





LED	Description
PWR	POWER LED • ON: The system has successfully started. • OFF: The equipment is off.
PON	PON LED (Connection to GPON) • ON: The optical signal is synchronized. • Flashing: GPON ONT not registered. • OFF: The optical signal is not synchronized.
LOS	LOS LED • Flashing: Optical signal is not detected. • OFF: Optical signal is detected.
STATUS	Status LED • ON: The device is loaded, and Internet services are available. • FAST BLINKING: The device is booting, or there is no Internet access. • SLOW BLINKING: The device firmware is being updated.
LAN1 LAN2	Wired connection status LED (with Ethernet cable) • ON: The Ethernet port is connected to a device. • Flashing: The Ethernet port is connected to a device and the data is transmitting. • OFF: There is no device connected to the WiFi Router through one of the Ethernet LAN ports.
2.4G 5G	2.4GHz and 5GHz wireless network status LED • ON: 2.4GHz/5GHz wireless network service is ON. • Flashing: 2.4GHz/5GHz wireless band is connected to a device (PC, smartphone, etc.) and transmitting/receiving data. • OFF: 2.4GHz/5GHz wireless network service is OFF.
WPS	WPS status LED • Flashing: Establishing WPS connection, will flash for 2 minutes then turn off when it's established. • OFF: WPS connection is established and finished. Or WPS function is not activated.

6. Web Configuration Interface

The BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway features a user-friendly web-based configuration interface that allows you to manage and customize all aspects of your network settings. This section will guide you through accessing and navigating this interface.

6.1 Accessing the Web Interface

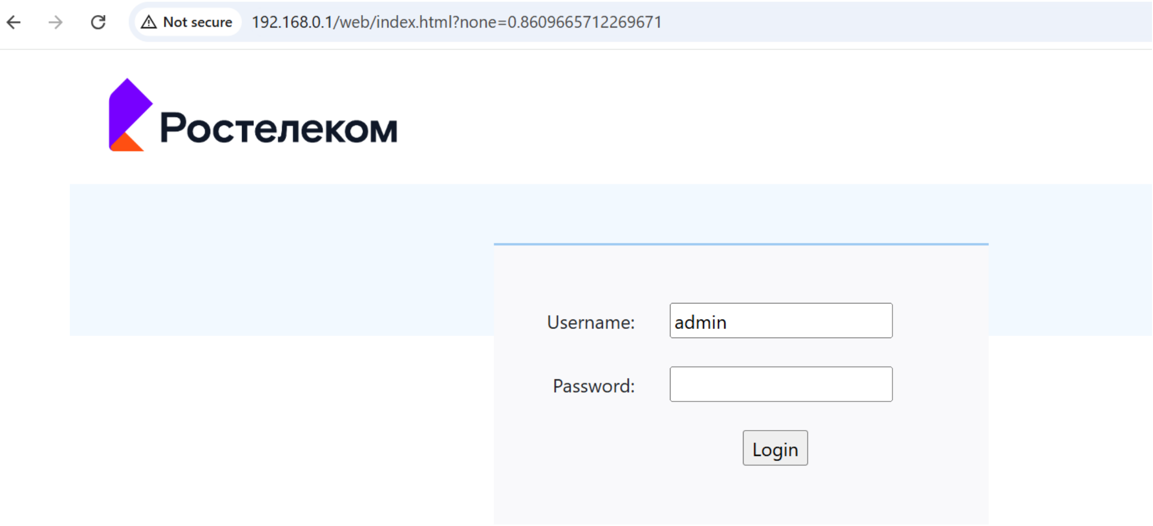
To access the web configuration interface, ensure your computer is connected to the BIN62X2PLIRT via an Ethernet cable or Wi-Fi, and that your computer's IP settings are set to "obtain automatically" (as described in Section 4.3).

1. **Launch a Web Browser:** Open any standard web browser (e.g., Google Chrome, Mozilla Firefox, Microsoft Edge, Safari) on a computer connected to the gateway.
2. **Enter IP Address:** In the web address (or location) bar of your browser, type the

6.2 Login Credentials

Upon entering the IP address, you will be presented with a login page.

Figure 6.1. Web Login Page



192.168.0.1/web/index.html?none=0.8609665712269671

Username: admin

Password:

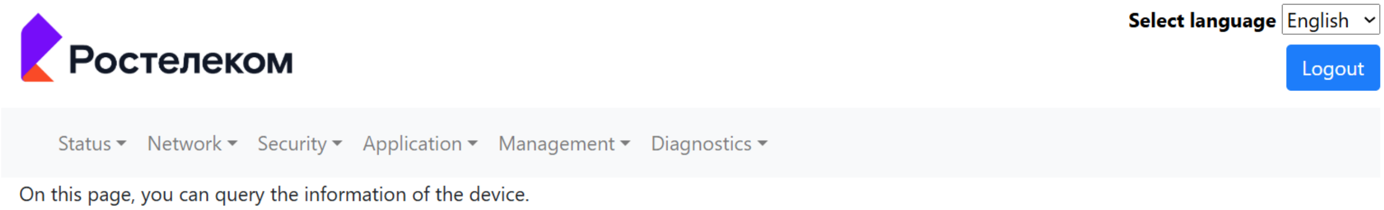
1. **Enter Username:** In the "Username" field, type the default username: **admin**
2. **Enter Password:** In the "Password" field, type the default password. The default password is typically found on a sticker on the bottom side of your BIN62X2PLIRT device.
    - **WARNING:** For security reasons, it is highly recommended to change the default login password immediately after your first successful login. Refer to Section 11.4 for instructions on changing the password.

3. **Click Login:** Click the **Login** button to access the main configuration interface.

6.3 Navigating the Interface

Once logged in, you will be presented with the main dashboard or status page of the web interface. The interface is typically organized with a head menu or a left-hand navigation pane that allows you to access various configuration sections, such as Status, Network, Security, Application, Management, and Diagnostics. Click on the relevant menu items to navigate to the desired configuration page.

Figure 6.2. Landing page Menu



On this page, you can query the information of the device.

7. Internet Configuration (PPPoE, IPoE, Static)

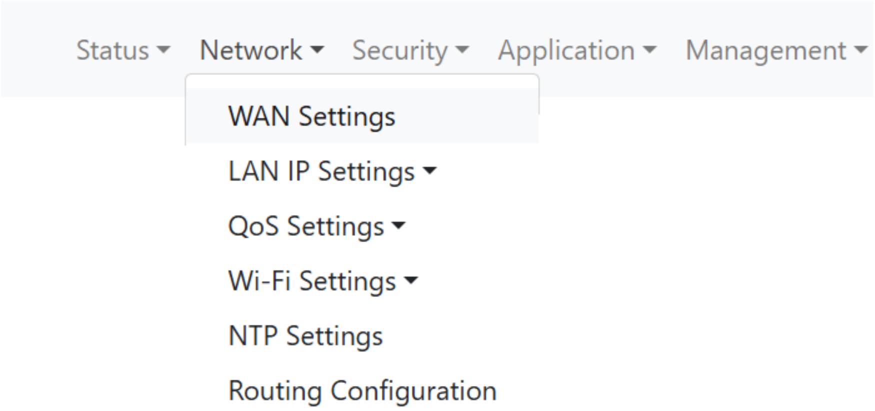
This section provides detailed instructions on configuring the BIN62X2PLIRT for various types of Internet connections (WAN settings). The specific type of connection required (PPPoE, IPoE DHCP, or IPoE Static) will be provided by your Internet Service Provider (ISP).

7.1 WAN Configuration Overview

The WAN (Wide Area Network) settings allow your BIN62X2PLIRT to connect to the Internet. It is crucial to obtain the correct connection parameters from your ISP before attempting to configure these settings.

To access the WAN configuration settings:

1. From the head menu of the web configuration interface, click on **Network**.
2. Then, click on **WAN Settings**.

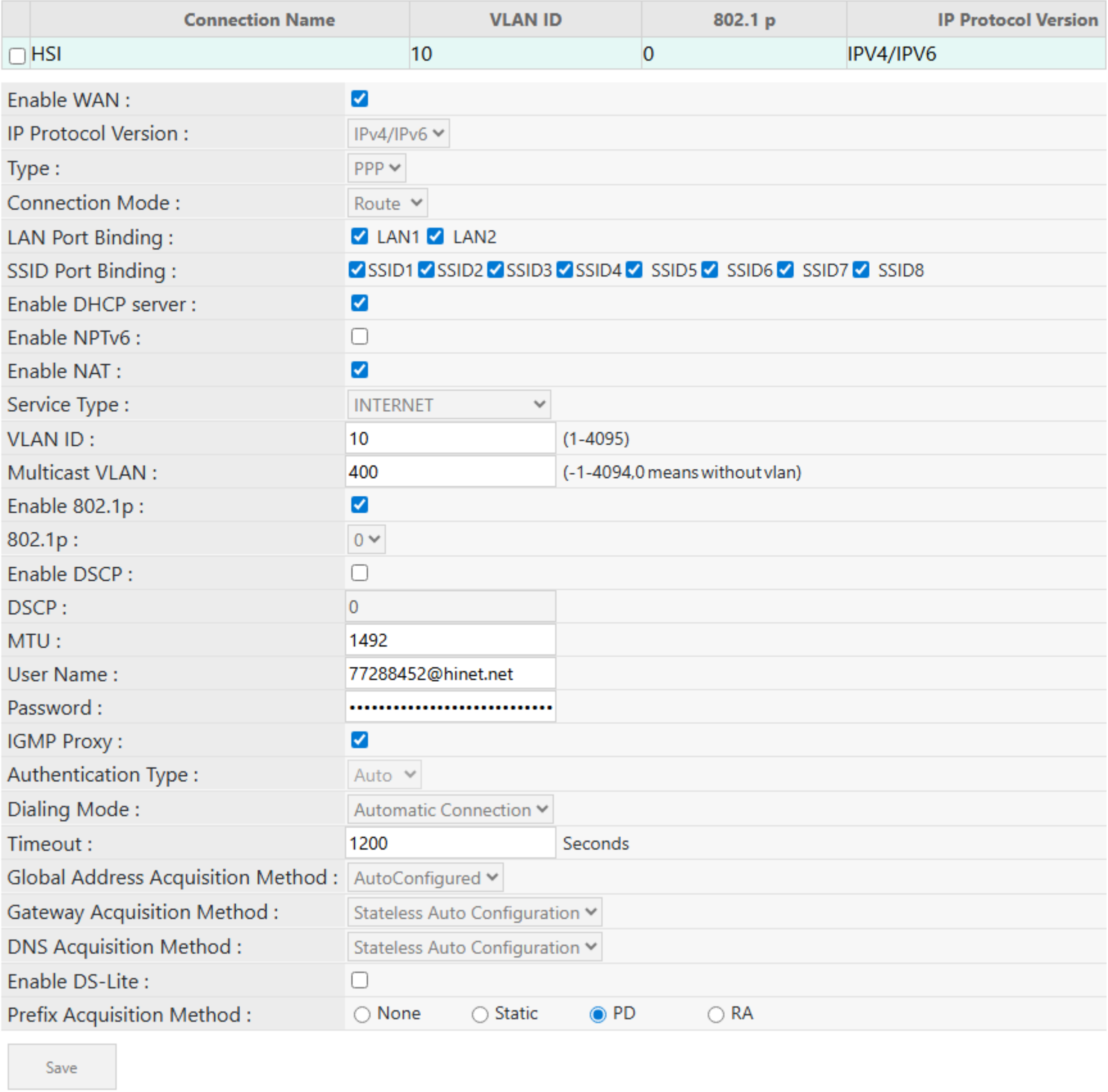


7.2 PPPoE (Point-to-Point Protocol over Ethernet) Configuration

PPPoE is a common connection type that requires a username and password provided by your ISP.

1. **IP Protocol Version:** From the **IP Protocol Version** drop-down list, select the IP Protocol (IPv4, IPv6, or Dual Stack IPv4/IPv6) as determined by your ISP.
2. **Service Type:** From the **Service Type** drop-down list, select **INTERNET**.
3. **Enter Credentials:** Enter the **User Name** and **Password** provided by your ISP into the relevant text boxes.
4. **IPv6 WAN Settings (if applicable):** Configure IPv6 WAN settings if provided by your ISP.
5. **Save Settings:** If you are satisfied with your settings, click the **Save** button.

Figure 7.1. PPPoE Configuration



	Connection Name	VLAN ID	802.1 p	IP Protocol Version
□	HSI	10	0	IPV4/IPV6

Enable WAN :	☑	
IP Protocol Version :	IPv4/IPv6	
Type :	PPP	
Connection Mode :	Route	
LAN Port Binding :	☑ LAN1 ☑ LAN2	
SSID Port Binding :	☑SSID1 ☑SSID2 ☑SSID3 ☑SSID4 ☑ SSID5 ☑ SSID6 ☑ SSID7 ☑ SSID8	
Enable DHCP server :	☑	
Enable NPTv6 :	□	
Enable NAT :	☑	
Service Type :	INTERNET	
VLAN ID :	10	(1-4095)
Multicast VLAN :	400	(-1-4094,0 means without vlan)
Enable 802.1p :	☑	
802.1p :	0	
Enable DSCP :	□	
DSCP :	0	
MTU :	1492	
User Name :	77288452@hinet.net	
Password :	•••••••••••••••••••••••••••••	
IGMP Proxy :	☑	
Authentication Type :	Auto	
Dialing Mode :	Automatic Connection	
Timeout :	1200	Seconds
Global Address Acquisition Method :	AutoConfigured	
Gateway Acquisition Method :	Stateless Auto Configuration	
DNS Acquisition Method :	Stateless Auto Configuration	
Enable DS-Lite :	□	
Prefix Acquisition Method :	○ None ○ Static ● PD ○ RA	

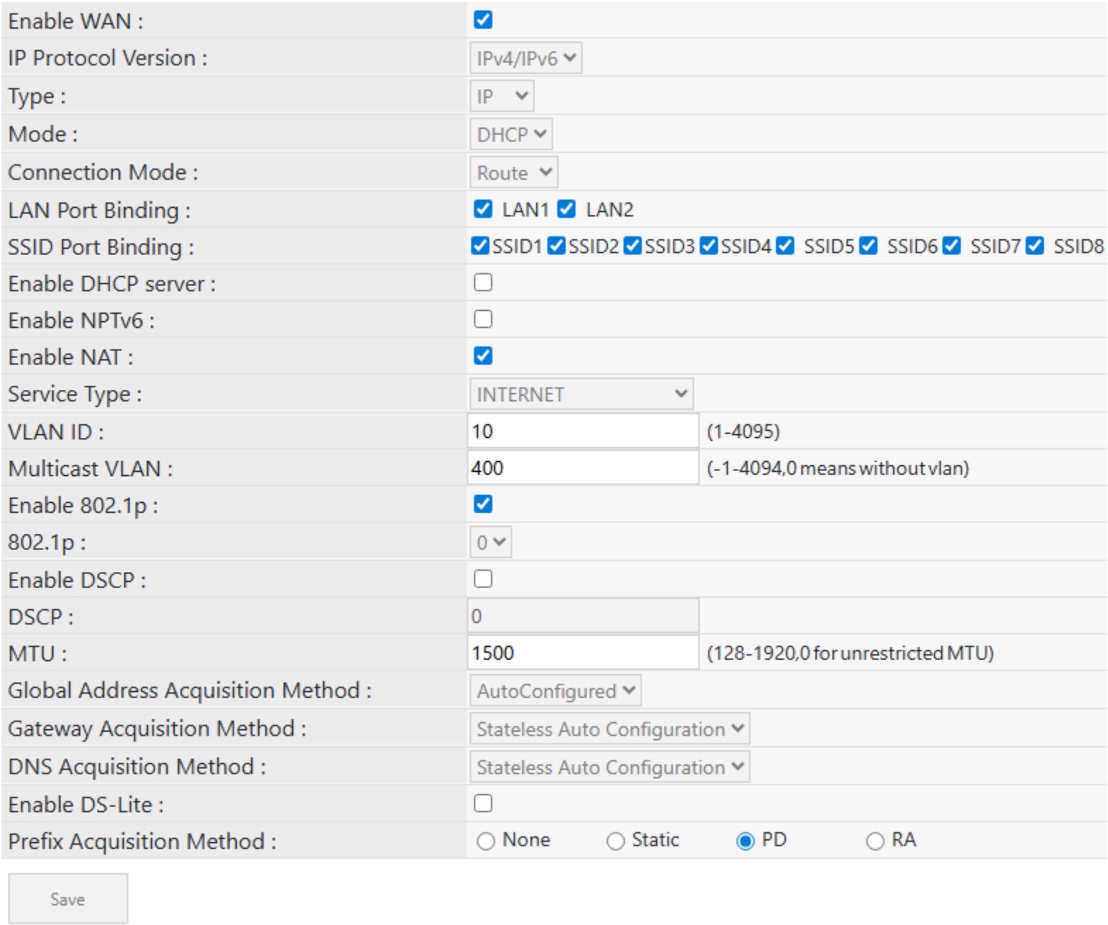
Note: After configuring PPPoE, your device will attempt to establish a connection using the provided credentials. Some ISPs may require you to load PPPoE Client Software onto your PC; however, the gateway handles the PPPoE connection directly.

7.3 IPoE (IP over Ethernet) by DHCP Configuration

IPoE DHCP connections automatically obtain IP address information from your ISP's server.

1. **IP Protocol Version:** From the **IP Protocol Version** drop-down list, select the IP Protocol (IPv4, IPv6, or Dual Stack IPv4/IPv6) as determined by your ISP.
2. **Service Type (General):** From the **Service Type** drop-down list, select **IP**.
3. **Connection Mode:** From the **Connection Mode** drop-down list, select **DHCP** setting.
4. **Service Type (Internet):** From the **Service Type** drop-down list, select **INTERNET**.
5. **IPv6 WAN Settings (if applicable):** Configure IPv6 WAN settings if provided by your ISP.
6. **Save Settings:** If you are satisfied with your settings, click the **Save** button.

Figure 7.2. IPoE by DHCP Configuration



Enable WAN :	☑
IP Protocol Version :	IPv4/IPv6
Type :	IP
Mode :	DHCP
Connection Mode :	Route
LAN Port Binding :	☑ LAN1 ☑ LAN2
SSID Port Binding :	☑SSID1 ☑SSID2 ☑SSID3 ☑SSID4 ☑ SSID5 ☑ SSID6 ☑ SSID7 ☑ SSID8
Enable DHCP server :	□
Enable NPTv6 :	□
Enable NAT :	☑
Service Type :	INTERNET
VLAN ID :	10 (1-4095)
Multicast VLAN :	400 (-1-4094,0 means without vlan)
Enable 802.1p :	☑
802.1p :	0
Enable DSCP :	□
DSCP :	0
MTU :	1500 (128-1920,0 for unrestricted MTU)
Global Address Acquisition Method :	AutoConfigured
Gateway Acquisition Method :	Stateless Auto Configuration
DNS Acquisition Method :	Stateless Auto Configuration
Enable DS-Lite :	□
Prefix Acquisition Method :	○ None ○ Static ● PD ○ RA

7.4 IPoE (IP over Ethernet) by Static IP Configuration

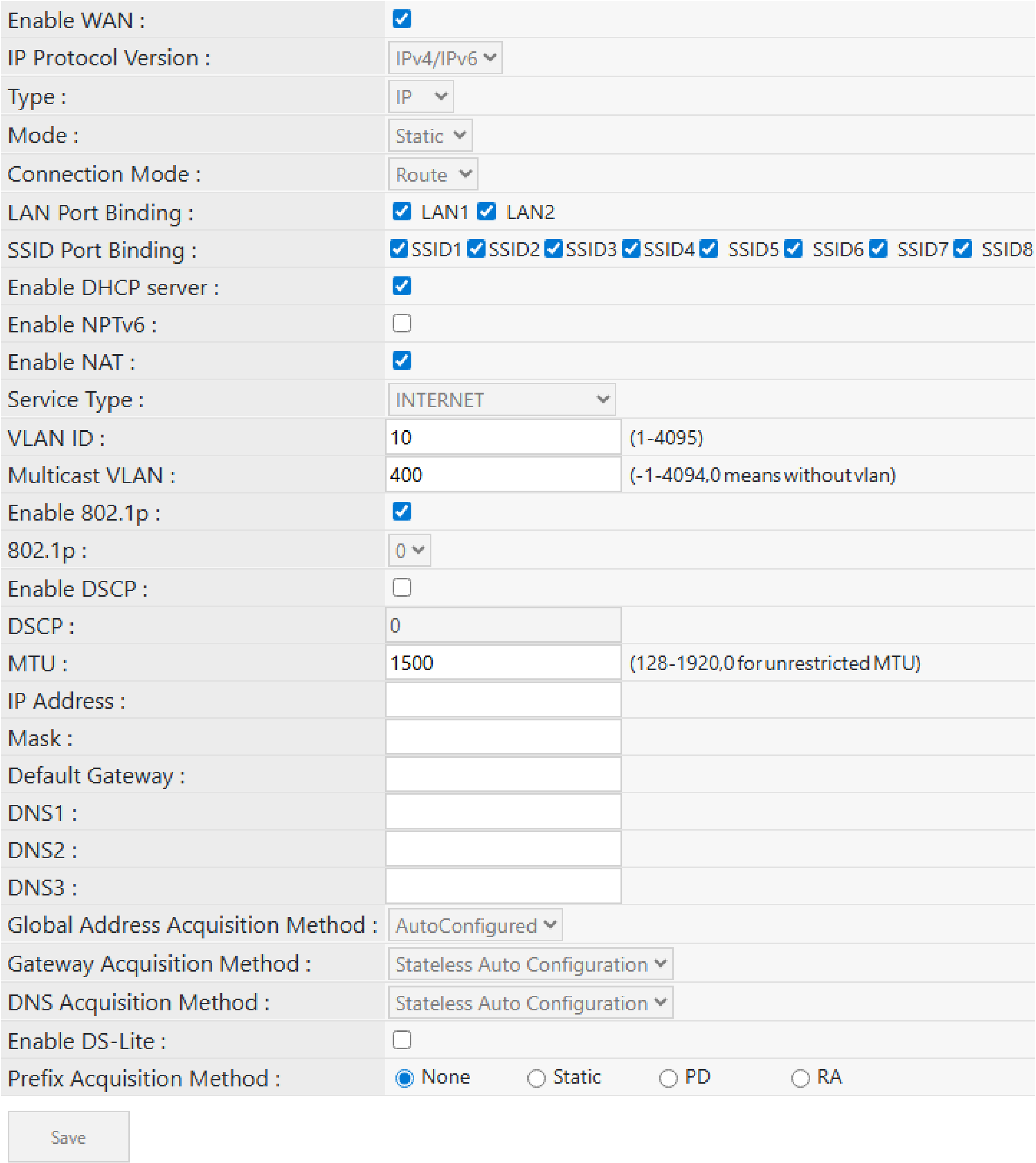
IPoE Static IP connections require you to manually enter specific IP address details provided by your ISP.

1. **IP Protocol Version:** From the **IP Protocol Version** drop-down list, select the IP Protocol (IPv4, IPv6, or Dual Stack IPv4/IPv6) as determined by your ISP.
2. **Service Type (General):** From the **Service Type** drop-down list, select **IP**.
3. **Connection Mode:** From the **Connection Mode** drop-down list, select **Static** setting.
4. **Service Type (Internet):** From the **Service Type** drop-down list, select **INTERNET**.
5. **Enter IP Details:** Enter the following information exactly as provided by your ISP:
   - **Local IP Address**
   - **Mask** (Subnet Mask)
   - **Default Gateway**
   - **DNS1** (Primary DNS Server)
   - **DNS2** (Secondary DNS Server)
   - **DNS3** (Optional Third DNS Server)

2. **IPv6 WAN Settings (if applicable):** Configure IPv6 WAN settings if provided by your ISP.

3. **Save Settings:** If you are satisfied with your settings, click the **Save** button.

Figure 7.3. IPoE by Static IP Configuration



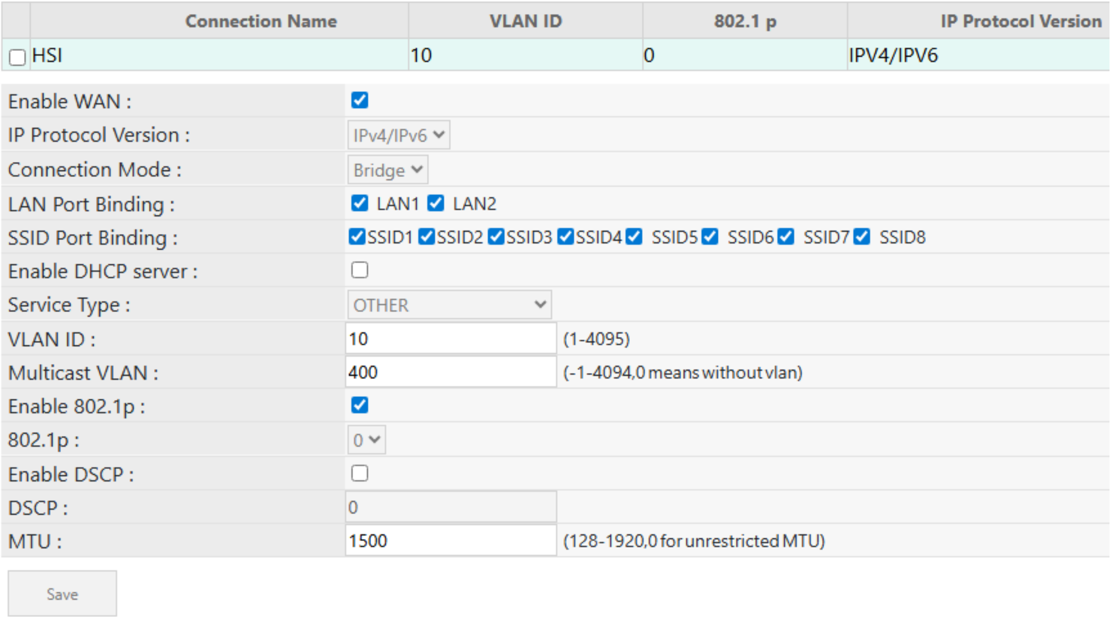
Enable WAN :	☑	
IP Protocol Version :	IPv4/IPv6	
Type :	IP	
Mode :	Static	
Connection Mode :	Route	
LAN Port Binding :	☑ LAN1 ☑ LAN2	
SSID Port Binding :	☑SSID1 ☑SSID2 ☑SSID3 ☑SSID4 ☑ SSID5 ☑ SSID6 ☑ SSID7 ☑ SSID8	
Enable DHCP server :	☑	
Enable NPTv6 :	☐	
Enable NAT :	☑	
Service Type :	INTERNET	
VLAN ID :	10	(1-4095)
Multicast VLAN :	400	(-1-4094,0 means without vlan)
Enable 802.1p :	☑	
802.1p :	0	
Enable DSCP :	☐	
DSCP :	0	
MTU :	1500	(128-1920,0 for unrestricted MTU)
IP Address :		
Mask :		
Default Gateway :		
DNS1 :		
DNS2 :		
DNS3 :		
Global Address Acquisition Method :	AutoConfigured	
Gateway Acquisition Method :	Stateless Auto Configuration	
DNS Acquisition Method :	Stateless Auto Configuration	
Enable DS-Lite :	☐	
Prefix Acquisition Method :	● None ○ Static ○ PD ○ RA	

7.5 Bridged

From the Connection Mode drop-down list, select Bridged setting. From the Service Type drop-down list, select OTHER setting. If you are done with your settings, click Save.

Now you can load your PPPoE Client Software onto your PC. Now you can load your PPPoE Client Software with user name and password which determined by your ISP onto your PC.

Figure 7.4. Bridged Configuration



	Connection Name	VLAN ID	802.1 p	IP Protocol Version
☐	HSI	10	0	IPV4/IPV6

Enable WAN :	☑	
IP Protocol Version :	IPv4/IPv6	
Connection Mode :	Bridge	
LAN Port Binding :	☑ LAN1 ☑ LAN2	
SSID Port Binding :	☑SSID1 ☑SSID2 ☑SSID3 ☑SSID4 ☑ SSID5 ☑ SSID6 ☑ SSID7 ☑ SSID8	
Enable DHCP server :	☐	
Service Type :	OTHER	
VLAN ID :	10	(1-4095)
Multicast VLAN :	400	(-1-4094,0 means without vlan)
Enable 802.1p :	☑	
802.1p :	0	
Enable DSCP :	☐	
DSCP :	0	
MTU :	1500	(128-1920,0 for unrestricted MTU)

8. Wireless Configuration (2.4GHz & 5GHz)

The BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway supports dual-band concurrent Wi-Fi, operating simultaneously on both 2.4GHz and 5GHz frequencies. This section details how to configure these wireless networks for optimal performance and connectivity.

8.1 Dual-Band Concurrent Wi-Fi

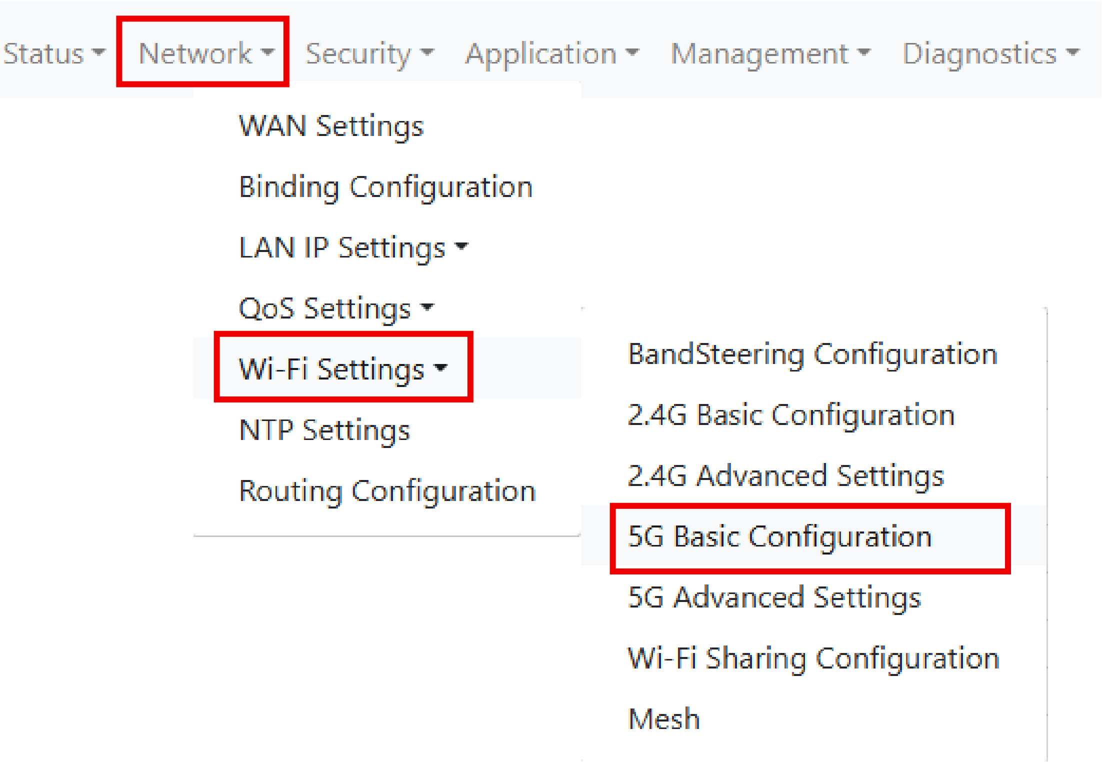
The BIN62X2PLIRT provides simultaneous dual-band Wi-Fi to avoid wireless interference and ensure top Wi-Fi speeds and reliable connections. This feature allows older devices to connect to the 2.4GHz band while newer, more demanding devices can utilize the faster 5GHz band, enhancing overall network efficiency.

8.2 5GHz Wireless Configuration

The 5GHz band offers higher speeds and less interference, ideal for applications requiring high bandwidth such as 4K video streaming and online gaming.

To access the 5GHz wireless settings:

1. From the head menu of the web configuration interface, click on **Network**.
2. Then, click on **Wi-Fi Settings**.
3. Finally, select **5G Basic Configuration**.



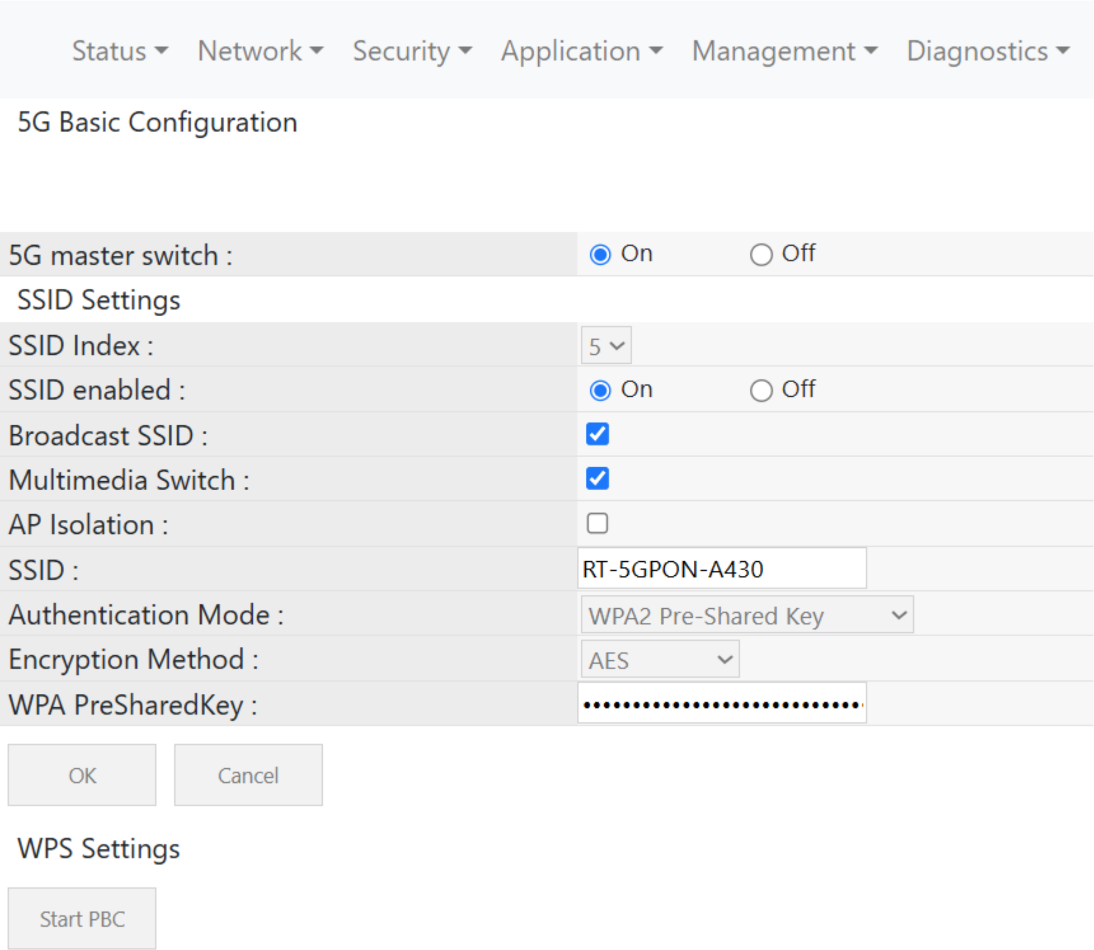
8.2.1 Basic Settings

- **5G Master switch:** Disable (Off) or enable (On) 5GHz **Band**
- **SSID (Network Name):** Enter a unique network name (SSID) for your 5GHz wireless network. For example, BIN62X2PLIRT -5G.
    - **Definition:** Each wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the name for that network. If you are setting up your own network you can make up your own name and use it on each computer. The name can be up to 32 characters long and contain letters and numbers.
    - **Note:** The default SSID is typically found on a sticker on the bottom of your device.
- **Broadcast SSID:** Choose whether to **Broadcast** or **Hide** your SSID to the network. Disabling broadcast (hiding SSID) can offer a minor security

enhancement by making your network less visible, but it also makes it harder for legitimate devices to find and connect to your network. Default: Enabled.

- **Apply Changes:** After configuring the basic settings, click **OK**. A confirmation message "save successfully!" should appear.

Figure 8.1. 5G Basic Settings



5G Basic Configuration

5G master switch :	● On ○ Off
SSID Settings	
SSID Index :	5
SSID enabled :	● On ○ Off
Broadcast SSID :	☑
Multimedia Switch :	☑
AP Isolation :	□
SSID :	RT-5GPON-A430
Authentication Mode :	WPA2 Pre-Shared Key
Encryption Method :	AES
WPA PreSharedKey :	••••••••••••••••••••••••••••

WPS Settings

8.2.2 Advanced Settings

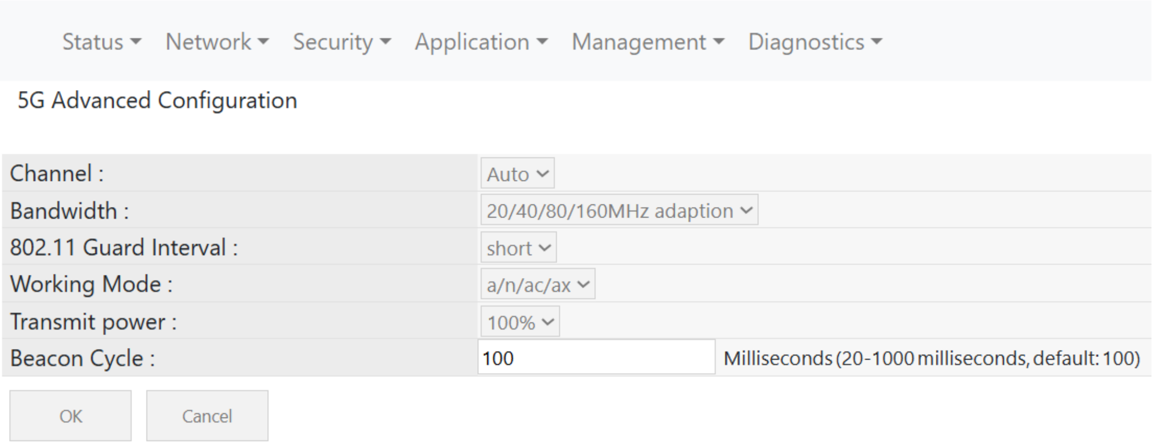
Advanced settings are intended for technically proficient users with a comprehensive understanding of wireless LAN principles. Modifying these settings without proper knowledge can negatively impact network performance.

To access the 5GHz advanced wireless settings:

1. From the head menu, navigate to **Network -> Wi-Fi Settings -> 5G Advanced Settings**.

- **Channel Number:** From the **Channel Number** drop-down list, select a specific channel. It is recommended to use auto-channel selection unless you are experiencing interference.
- **Channel Width:** From the **Channel Width** drop-down list, select a suitable channel width (e.g., 20/40/80/160 MHz for Wi-Fi 6). Wider channels offer higher speeds but can be more susceptible to interference if not properly selected.
- **Guard Interval:** Enable or Disable Short GI. Short GI can increase data rates but may reduce stability in environments with high interference.
- **Working Mode:** From the list select the Wi-Fi standards a,n,ac,ax.
- **Beacon Cycle:** This value indicates the frequency interval of the beacon frames, which are crucial for network synchronization. Enter a value between 20 and 1000 milliseconds. The default is typically 100.
- **Apply Changes**: After configuring the basic settings, click **OK**. A confirmation message "**save successfully**!" should appear.

Figure 8.2. 5G Advanced Settings



5G Advanced Configuration

Channel :	Auto	
Bandwidth :	20/40/80/160MHz adaption	
802.11 Guard Interval :	short	
Working Mode :	a/n/ac/ax	
Transmit power :	100%	
Beacon Cycle :	100	Milliseconds (20-1000 milliseconds, default: 100)

8.3 2.4GHz Wireless Configuration

The 2.4GHz band offers wider coverage and better penetration through obstacles compared to 5GHz, making it suitable for larger homes or environments with many walls.

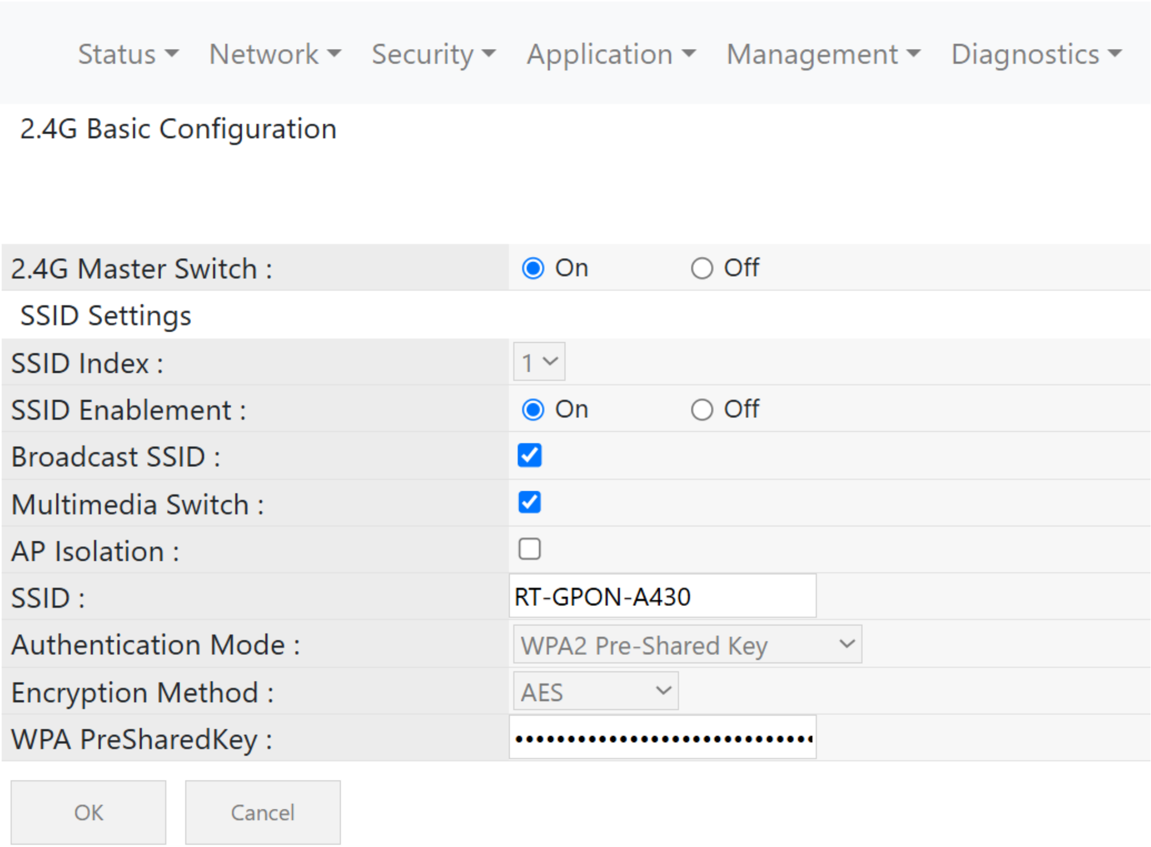
To access the 2.4GHz wireless settings:

1. From the head menu, click on **Network**.
2. Then, click on **Wi-Fi Settings**.
3. Finally, select **2.4G Basic Configuration**.

8.3.1 Basic Settings

- **2.4G Master switch:** Disable (Off) or enable (On) 2.4GHz **Band**
- **SSID (Network Name):** Enter a unique network name (SSID) for your 2.4GHz wireless network. For example, BIN62X2PLIRT-2.4G.
  - **Note:** The default SSID is typically found on a sticker on the bottom of your device.
- **Broadcast SSID:** Choose whether to **Broadcast** or **Hide** your SSID to the network. Disabling broadcast (hiding SSID) can offer a minor security enhancement by making your network less visible, but it also makes it harder for legitimate devices to find and connect to your network. Default: Enabled.
- **Apply Changes:** After configuring the basic settings, click **OK**. A confirmation message "save successfully!" should appear.

Figure 8.3. 2.4G Basic Settings



2.4G Basic Configuration

2.4G Master Switch :	● On ○ Off
SSID Settings	
SSID Index :	1
SSID Enablement :	● On ○ Off
Broadcast SSID :	☑
Multimedia Switch :	☑
AP Isolation :	□
SSID :	RT-GPON-A430
Authentication Mode :	WPA2 Pre-Shared Key
Encryption Method :	AES
WPA PreSharedKey :	••••••••••••••••••••••••••••••

8.3.2 Advanced Settings

Like the 5GHz band, advanced settings for the 2.4GHz band are for expert users.

To access the 2.4GHz advanced wireless settings:

1. From the head menu, navigate to **Network -> Wi-Fi Settings -> 2.4G Advanced Settings**.

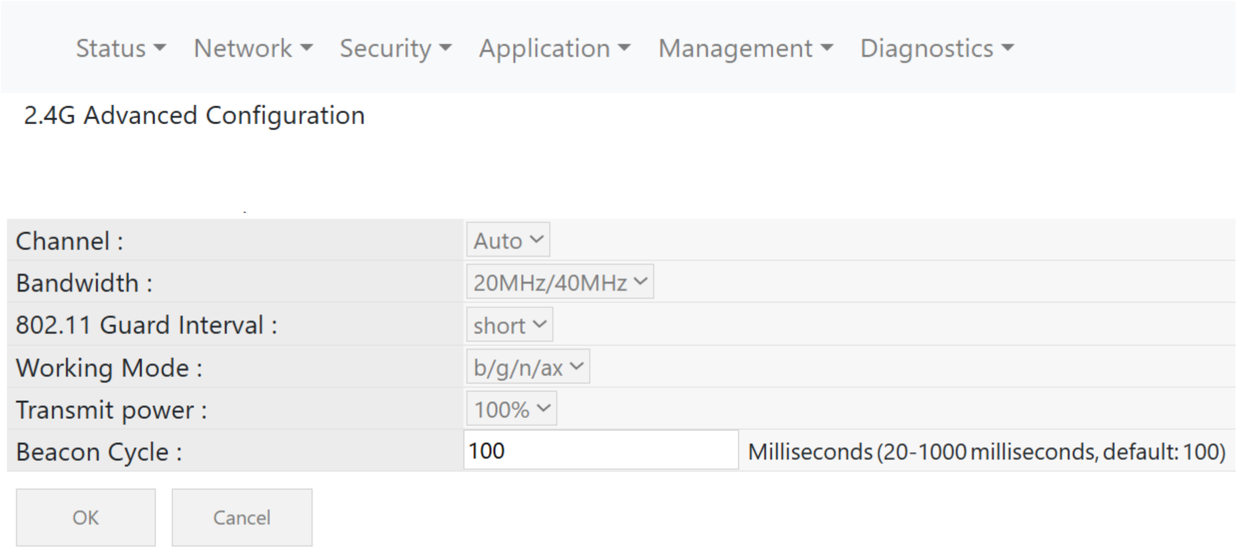
- **Channel Number:** From the **Channel Number** drop-down list, select a specific channel. It is recommended to use auto-channel selection unless you are experiencing interference.
- **Channel Width:** From the **Channel Width** drop-down list, select a suitable channel width (e.g., 20/40MHz). Wider channels offer higher speeds but can be more susceptible to interference if not properly selected.
- **Guard Interval:** Enable or Disable Short GI. Short GI can increase data rates but may reduce stability in environments with high interference.

- **Working Mode:** From the list select the Wi-Fi standards b,g,n,ax.

- **Beacon Cycle:** This value indicates the frequency interval of the beacon frames, which are crucial for network synchronization. Enter a value between 20 and 1000 milliseconds. The default is typically 100.

- **Apply Changes**: After configuring the basic settings, click **OK**. A confirmation message "**save successfully**!" should appear.

Figure 8.4. 2.4G Advanced Settings



2.4G Advanced Configuration

Channel :	Auto
Bandwidth :	20MHz/40MHz
802.11 Guard Interval :	short
Working Mode :	b/g/n/ax
Transmit power :	100%
Beacon Cycle :	100 Milliseconds (20-1000 milliseconds, default: 100)

9. Security Settings

Securing your wireless network is paramount to protect your data and prevent unauthorized access. The BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway supports various security protocols, including the latest WPA3 standard, as well as MAC filtering and Wi-Fi Protected Setup (WPS).

9.1 URL Filtering

This section allows you to control access to specific websites based on their Uniform Resource Locators (URLs). URL Filtering is a security feature that can be used to prevent access to undesirable content, enforce internet usage policies, or block malicious websites

To access these settings, navigate to **Security** > **URL Filtering**.

Configuration:

1. Enabled:

- **Description:** This checkbox acts as the master switch for the URL Filtering feature. When checked, URL filtering rules are active.
- **Configuration:**
  - **Check the box:** To activate URL filtering.
  - **Uncheck the box:** To disable URL filtering, allowing access to all URLs not restricted by other security rules.

2. URL List Type:

- **Description:** This dropdown menu defines how the URL Address Listing will be interpreted. You can choose between two primary modes:
  - **blacklist:** In this mode, URLs configured in the "URL Address Listing" are **NOT allowed** to be accessed. Any attempt to navigate to a URL present in the blacklist will be blocked.
  - **whitelist:** In this mode, URLs configured in the "URL Address Listing" are **ALLOWED** to be accessed. Only URLs explicitly present in the whitelist will be granted access; all other URLs will be denied.
- **Configuration:**
  - Select `blacklist` or `whitelist` from the dropdown menu based on your policy. The on-screen text clarifies: "When an address configured in the blacklist is not allowed to be accessed/Only when an address configured in the whitelist is allowed to be accessed."

3. URL Address Listing (Management Table):

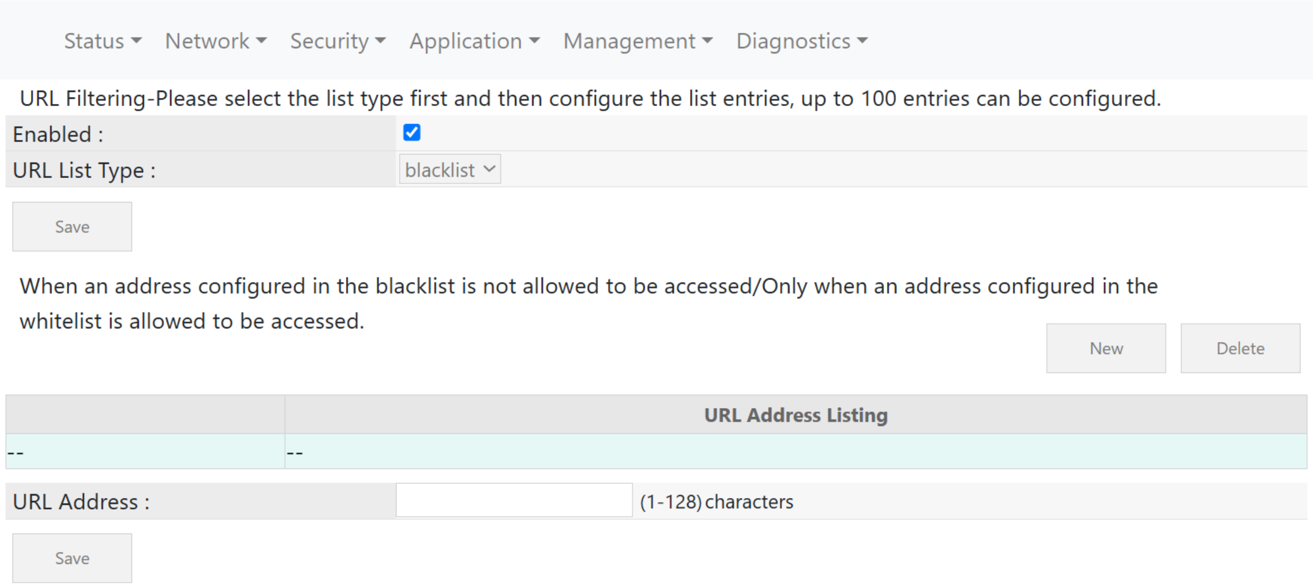
- This section displays currently configured URL filtering rules.
- *(Note: The --- indicates no entries are currently configured in this example.)*
- **New Button:** Click this button to add a new URL entry. This action will typically make the "URL Address :" input field active for data entry.

- **Delete Button:** Select one or more entries from the table (if available, usually via a checkbox or selection mechanism) and then click "Delete" to remove them from the list.

4. Add/Edit URL Address Entry:

- This section appears below the listing table when adding a new entry or editing an existing one.
- **URL Address :**
  - **Description:** This field is where you input the specific URL you wish to filter.
  - **Format:** Enter the URL. This can be a full URL (e.g., `www.example.com/page`), a domain (e.g., `example.com`), or a partial string depending on the device's capabilities (e.g., to block all subdomains of example.com, you might enter `example.com`).
  - **Character Limit:** The input field specifies "(1-128) characters," meaning the URL you enter must be between 1 and 128 characters long.
- **Save Button (for individual entry):**
  - After entering the `URL Address`, click this "Save" button to add the rule to the "URL Address Listing" table. This action adds the individual entry but does *not* save the overall URL Filtering configuration for the device yet.

Figure 9.1. URL Filtering



URL Filtering-Please select the list type first and then configure the list entries, up to 100 entries can be configured.

Enabled :	☑
URL List Type :	blacklist

When an address configured in the blacklist is not allowed to be accessed/Only when an address configured in the whitelist is allowed to be accessed.

	URL Address Listing
--	--

URL Address : (1-128) characters

9.2 Firewall

The firewall acts as a barrier between your internal network and external networks (like the internet), controlling incoming and outgoing network traffic based on a set of rules.

9.2.1 Firewall Level

The **Firewall Level** section allows users to define the degree of protection against malicious or suspicious network activity. This interface is typically used by administrators to harden the device's defense mechanisms against common forms of **Denial of Service (DoS)** attacks and **network intrusion techniques**.

Accessing Firewall Level Settings

1. Navigate to the **Security** menu from the top navigation bar.
2. Hover over **Firewall**, then select **Firewall Level** from the dropdown options.
3. The Firewall Level configuration panel will be displayed.

Configuration Parameters

Setting	Description
Enabled	Enables or disables the firewall protection feature.
Grade	Sets the intensity or strictness of firewall rules. Options may include: `Low`, `Medium`, and `High`. - `Low`: Minimal protection, least impact on traffic. - `Medium`: Balanced protection and performance (recommended). - `High`: Maximum protection; may block more traffic.
DoS Attack Protection	Master toggle to enable/disable DoS protection suite.
SYN Flooding	Protects against SYN flood attacks which exhaust connection resources using incomplete TCP handshakes.
ICMP Echo	Blocks or filters excessive ping requests to prevent **ICMP flood attacks**.
ICMP Redirection	Disables redirection of ICMP packets to prevent manipulation of routing tables.
LAND	Protects against **LAND attacks**, where packets are crafted with identical source and destination IP/port.
Smurf	Blocks **Smurf attacks** by disabling responses to ICMP requests sent to broadcast addresses.
Winnuke	Defends against **Winnuke** attacks that exploit NetBIOS vulnerabilities to crash older systems.
Ping of Death	Blocks overly large or malformed ICMP packets that can crash or freeze systems.

Recommended Configuration

For most users and enterprise environments:

- Set **Enabled**: ✅ (Checked)
- Set **Grade**: `Medium`
- Enable all checkboxes for attack types.

This configuration ensures a well-balanced approach between network protection and performance.

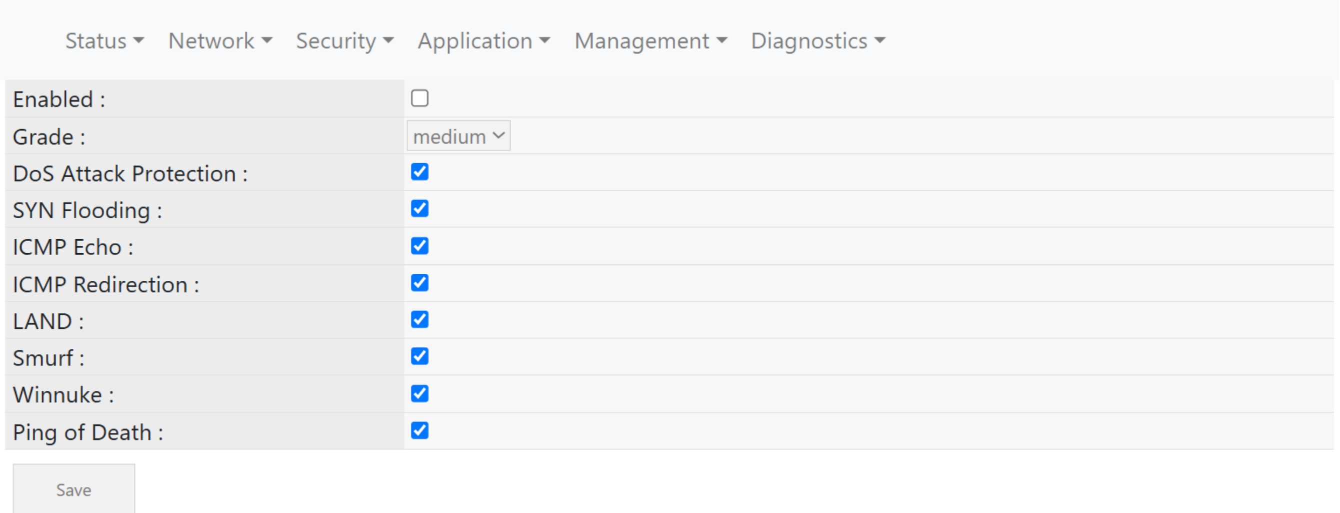
How to Configure

1. Go to **Security > Firewall > Firewall level**.
2. Check the **Enabled** box to activate protection.
3. From the **Grade** dropdown, select your preferred protection level (e.g., `Medium`).
4. Enable individual protections:
   - ✓ DoS Attack Protection
   - ✓ SYN Flooding
   - ✓ ICMP Echo
   - ✓ ICMP Redirection
   - ✓ LAND
   - ✓ Smurf
   - ✓ Winnuke
   - ✓ Ping of Death
5. Click the **Save** button to apply changes.

Notes

- **Disabling protection** may expose your network to known attack vectors.
- **ICMP Echo** disabling may affect network diagnostic tools such as `ping`.
- **High protection grade** may block some legitimate traffic, especially with custom applications or remote monitoring

Figure 9.2. Firewall Level

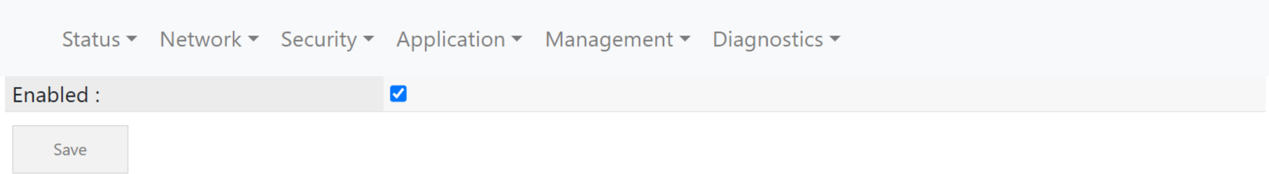


Enabled :	☐
Grade :	medium
DoS Attack Protection :	☑
SYN Flooding :	☑
ICMP Echo :	☑
ICMP Redirection :	☑
LAND :	☑
Smurf :	☑
Winnuke :	☑
Ping of Death :	☑

9.2.2 IPv6 Session Firewall

Like the standard firewall, this specifically applies to IPv6 (Internet Protocol version 6) traffic. It controls the flow of IPv6 data packets, managing inbound and outbound sessions to protect your IPv6-enabled network.

- **Configuration:**
  - **Enable/Disable:** Activate or deactivate the IPv6 session firewall.
  - Click "**Save**" to successfully enable or disable this function.



Enabled :	☑

9.3 MAC Filtering Configuration

This section allows you to control network access for devices based on their unique Media Access Control (MAC) addresses. MAC Filtering provides a layer of security by either allowing only specified devices to connect (whitelist) or blocking specified devices from connecting (blacklist). The device will then enforce access rules based on this list and the chosen "Filter Mode". Up to 100 entries can typically be configured in the list.

To access these settings, navigate to **Security** > **MAC Filtering**.

Configuration:

1. **Enabled:**
   - **Description:** This checkbox acts as the master switch for the MAC Filtering feature. When checked, MAC filtering rules are active.

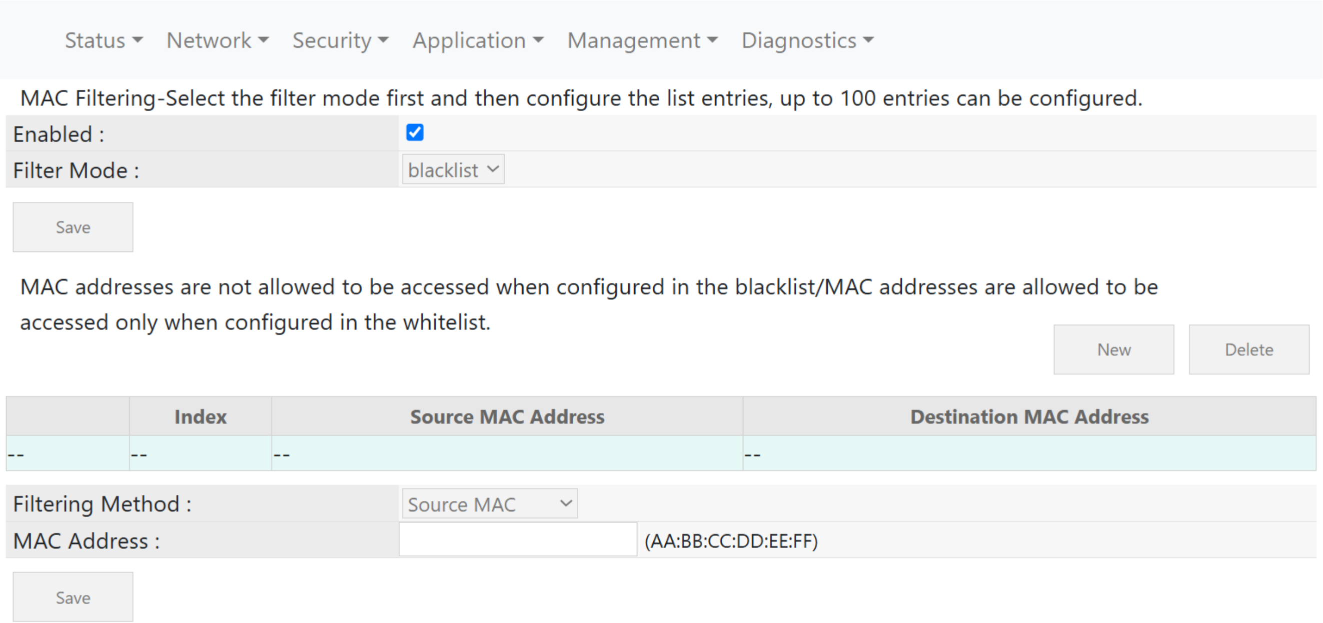
- **Configuration:**
    - **Check the box:** To activate MAC filtering.
    - **Uncheck the box:** To disable MAC filtering, allowing all devices (not restricted by other security rules) to connect regardless of their MAC address.

2. **Filter Mode:**
    - **Description:** This dropdown menu defines how the MAC address list will be interpreted. You can choose between two primary modes:
        - **Blacklist:** In this mode, MAC addresses configured in the list are **NOT allowed** to access the network. Any device whose MAC address is present in the blacklist will be prevented from connecting.
        - **Whitelist:** In this mode, MAC addresses configured in the list are **ALLOWED** to access the network. Only devices whose MAC addresses are explicitly present in the whitelist will be granted network access; all other devices will be denied.
    - **Configuration:**
        - Select blacklist or whitelist from the dropdown menu based on your security requirements. The on-screen text clarifies: "MAC addresses are not allowed to be accessed when configured in the blacklist/MAC addresses are allowed to be accessed only when configured in the whitelist."
3. **MAC Address List Management:**
    - This section allows you to view, add, and delete MAC address entries.
    - **Entry Table:** Displays existing MAC filtering rules.
        - **Index:** Sequential number of the entry.
        - **Source MAC Address:** The MAC address of the sender device.
        - **Destination MAC Address:** The MAC address of the recipient device.
        - *(Note: The --- indicates no entries are currently configured.)*
    - **New Button:** Click this button to add a new MAC filtering rule. This will typically bring up the input fields below for configuration.

  - **Delete Button:** Select one or more entries from the table (if available, usually via a checkbox next to each entry) and then click "Delete" to remove them from the list.

4. **Add/Edit MAC Address Entry:**
    - This section appears when adding a new entry or editing an existing one.
    - **Filtering Method:**
        - **Description:** This dropdown determines which MAC address (source, destination, or both) the filtering rule will apply to.
        - **Options:**
            - **Source MAC:** The rule applies to the MAC address of the device originating the connection.
            - **Destination MAC:** The rule applies to the MAC address of the device receiving the connection.
            - **(Implied) Both/Any:** Depending on the device, there might be an option to apply the rule if *either* the source or destination MAC matches, or if *both* match a specific pair. (The current dropdown only shows "Source MAC" as selected, implying other options might exist).
        - **Configuration:** Select the appropriate filtering method for the rule you intend to create.
    - **MAC Address:**
        - **Description:** This field is where you input the specific MAC address for the filtering rule.
        - **Format:** MAC addresses are typically 12 hexadecimal digits, often separated by colons or hyphens (e.g., AA:BB:CC:DD:EE:FF as shown in the example).
        - **Configuration:** Enter the 12-digit hexadecimal MAC address of the device you want to filter.
    - **Save Button (for individual entry):**
        - After entering the Filtering Method and MAC Address for a new or edited entry, click this "Save" button to add the rule to the list. It does *not* save the overall MAC Filtering configuration for the device yet

Figure 9.3. MAC Filtering configuration



MAC Filtering-Select the filter mode first and then configure the list entries, up to 100 entries can be configured.

Enabled :	☑
Filter Mode :	blacklist

MAC addresses are not allowed to be accessed when configured in the blacklist/MAC addresses are allowed to be accessed only when configured in the whitelist.

	Index	Source MAC Address	Destination MAC Address
--	--	--	--

Filtering Method :	Source MAC
MAC Address :	(AA:BB:CC:DD:EE:FF)

Overall Saving Configuration:

After making all desired changes, including enabling/disabling URL filtering, selecting the URL list type, and adding/deleting individual URL entries, ensure you click the **Save** button located at the top of the URL Filtering section (next to "Enabled :") to apply all changes permanently. Changes will not take effect until this main "Save" button is clicked

9.4 Port Filtering

This section allows you to configure rules to control traffic flowing from your Local Area Network (LAN) to the Wide Area Network (WAN), typically the internet.

9.4.1 Upstream Filtering Configuration

Upstream Filtering enables you to define rules that inspect outgoing network connections from your LAN devices to the WAN. These rules can be used to block undesirable outbound traffic (e.g., specific applications, unapproved external servers) or to ensure that only approved outbound connections are permitted.

To access these settings, navigate to **Security** > **Port Filtering**. This particular screen focuses on "LAN-To-WAN filtering to prohibit certain WAN port IP addresses from accessing through.

Configuration Options:

1. **Enabled:**

- **Description:** This checkbox is the master switch for the Upstream Filtering feature. When checked, the rules configured in this section will be actively enforced.
- **Configuration:**
    - **Check the box:** To activate Upstream Filtering.
    - **Uncheck the box:** To disable Upstream Filtering, allowing all outbound LAN-to-WAN traffic unless blocked by other firewall rules.

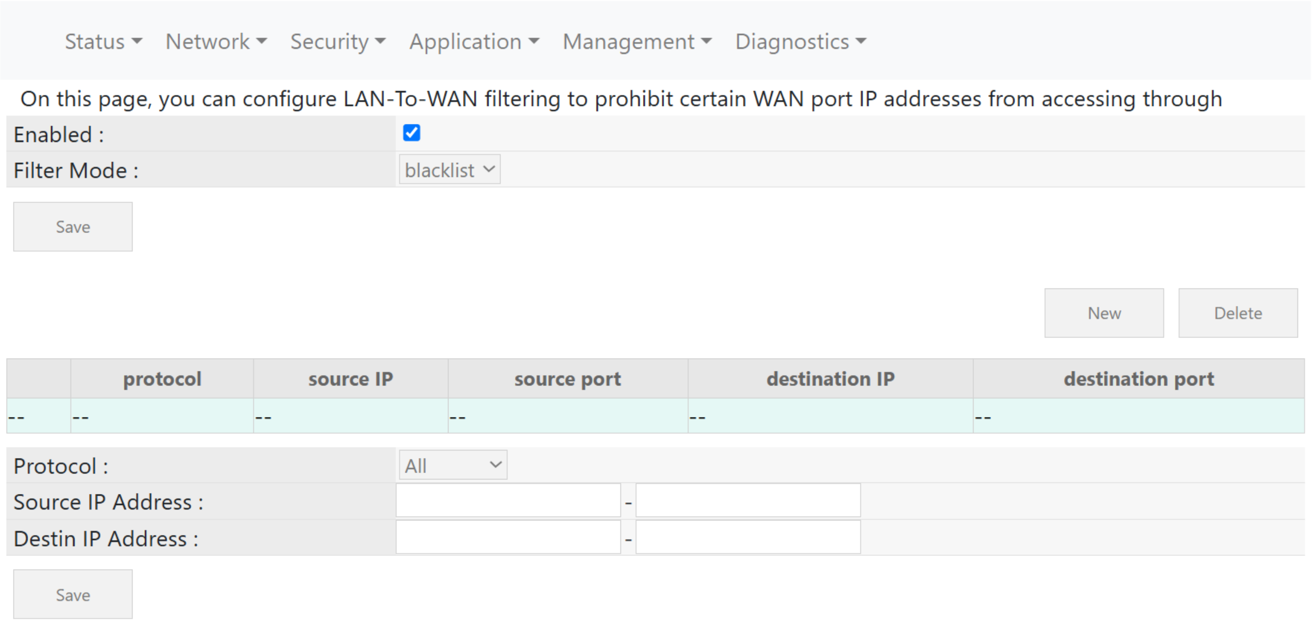
2. **Filter Mode:**
    - **Description:** This dropdown menu defines how the configured rules in the list will be interpreted.
    - **Options:**
        - **blacklist:** In this mode, any traffic matching a rule configured in the list will be **PROHIBITED** (blocked) from passing from the LAN to the WAN. All other traffic not matching a blacklist entry will be allowed.
        - **(Implied) whitelist:** While blacklist is selected in the image, the presence of a dropdown suggests whitelist is also an option. In whitelist mode, *only* traffic matching a rule configured in the list will be **ALLOWED** from passing from the LAN to the WAN. All other traffic not matching a whitelist entry will be prohibited.
    - **Configuration:**
        - Select blacklist or whitelist based on your network security policy.
3. **Rule Management (Table & Buttons):**
    - **Rule Table:** This table displays the currently configured LAN-to-WAN filtering rules.
        - **protocol:** The network protocol (e.g., TCP, UDP, ICMP, Any).
        - **source IP:** The IP address of the device on your LAN initiating the connection.
        - **source port:** The port number used by the source device.
        - **destination IP:** The IP address on the WAN that the LAN device is trying to connect to.
        - **destination port:** The port number on the destination WAN device.

        - *(Note: The --- indicates no entries are currently configured.)*
    - **New Button:** Click this button to add a new Upstream Filtering rule. This will typically activate the input fields below the table for rule definition.
    - **Delete Button:** Select one or more entries from the table (if available, usually via a checkbox next to each entry) and then click "Delete" to remove them from the list.

4. **Add/Edit Rule Entry:**
    - This section appears when adding a new rule or editing an existing one.
    - **Protocol:**
        - **Description:** Specifies the network protocol to which this rule applies.
        - **Options:** The dropdown typically includes options such as All, TCP, UDP, ICMP, etc. Selecting All applies the rule regardless of the protocol.
        - **Configuration:** Choose the specific protocol or All that the filtering rule should target.
    - **Source IP Address:**
        - **Description:** Defines the IP address range of the *originating* device(s) on your LAN for which this rule applies.
        - **Format:** Typically, you can enter a single IP address (e.g., 192.168.1.100) or an IP address range (e.g., 192.168.1.10 - 192.168.1.20). The two input fields separated by a hyphen suggest an IP range.
        - **Configuration:** Enter the source IP address or range within your LAN.
    - **Source Port:**
        - **Description:** Specifies the port number(s) used by the *originating* device on your LAN. For outbound connections, this is often a dynamic port, but can be specified if an application uses a fixed source port.
        - **Format:** Can be a single port (e.g., 80), a port range (e.g., 1024 - 5000), or left blank/set to "Any" to include all ports. The two input fields separated by a hyphen suggest a port range.
        - **Configuration:** Enter the source port or range.

- **Destination IP Address:**
  - **Description:** Defines the IP address range of the *destination* server or device on the WAN that the LAN device is attempting to connect to.
  - **Format:** Similar to Source IP, can be a single IP address or an IP address range.
  - **Configuration:** Enter the destination IP address or range on the WAN.
- **Destination Port:**
  - **Description:** Specifies the port number(s) on the *destination* server or device on the WAN. This is commonly used to block/allow specific services (e.g., port 80 for HTTP, port 443 for HTTPS, port 21 for FTP).
  - **Format:** Can be a single port, a port range, or left blank/set to "Any".
  - **Configuration:** Enter the destination port or range.
- **Save Button (for individual rule):**
  - After defining the parameters for a new or edited rule, click this "Save" button to add the rule to the "Rule Table." This action adds the individual rule but does *not* save the overall Upstream Filtering configuration for the device yet.

Figure 9.4. Upstream Filtering Configuration



On this page, you can configure LAN-To-WAN filtering to prohibit certain WAN port IP addresses from accessing through

Enabled :	☑
Filter Mode :	blacklist

	protocol	source IP	source port	destination IP	destination port
--	--	--	--	--	--

Protocol :	All
Source IP Address :	-
Destin IP Address :	-

Overall Saving Configuration:

- After making all desired changes, including enabling/disabling Upstream Filtering, selecting the filter mode, and adding/deleting individual rules, ensure you click the **Save** button located at the top of the Upstream Filtering section (next to "Enabled :") to apply all changes permanently. Changes will not take effect until this main "Save" button is clicked

9.4.2 Downstream Filtering Configuration

Downstream Filtering (also known as Inbound Filtering) enables you to define rules that inspect incoming network connections from the WAN to your LAN. These rules determine which external connections are permitted to reach your internal devices based on criteria such as source/destination IP addresses, port numbers, and protocol.

To access these settings, navigate to **Security** > **Port Filtering** > **Downstream Filtering Configuration**.

Configuration:

1. **Enabled:**
    - **Description:** This checkbox is the master switch for the Downstream Filtering feature. When checked, the rules configured in this section will be actively enforced.
    - **Configuration:**
        - **Check the box:** To activate Downstream Filtering.
        - **Uncheck the box:** To disable Downstream Filtering, which may leave your internal network more vulnerable to unsolicited connections from the internet unless protected by a default deny firewall policy.
2. **Filter Mode:**
    - **Description:** This dropdown menu defines how the configured rules in the list will be interpreted.
    - **Options:**
        - **blacklist:** In this mode, any incoming traffic matching a rule configured in the list will be **PROHIBITED** (blocked) from entering your LAN. All other incoming traffic not matching a blacklist entry will be allowed.
        - **(Implied) whitelist:** While blacklist is selected in the image, the presence of a dropdown suggests whitelist is likely another option. In whitelist mode, *only* incoming traffic matching a rule configured

        in the list will be **ALLOWED** to enter your LAN. All other traffic not matching a whitelist entry will be prohibited (default deny).

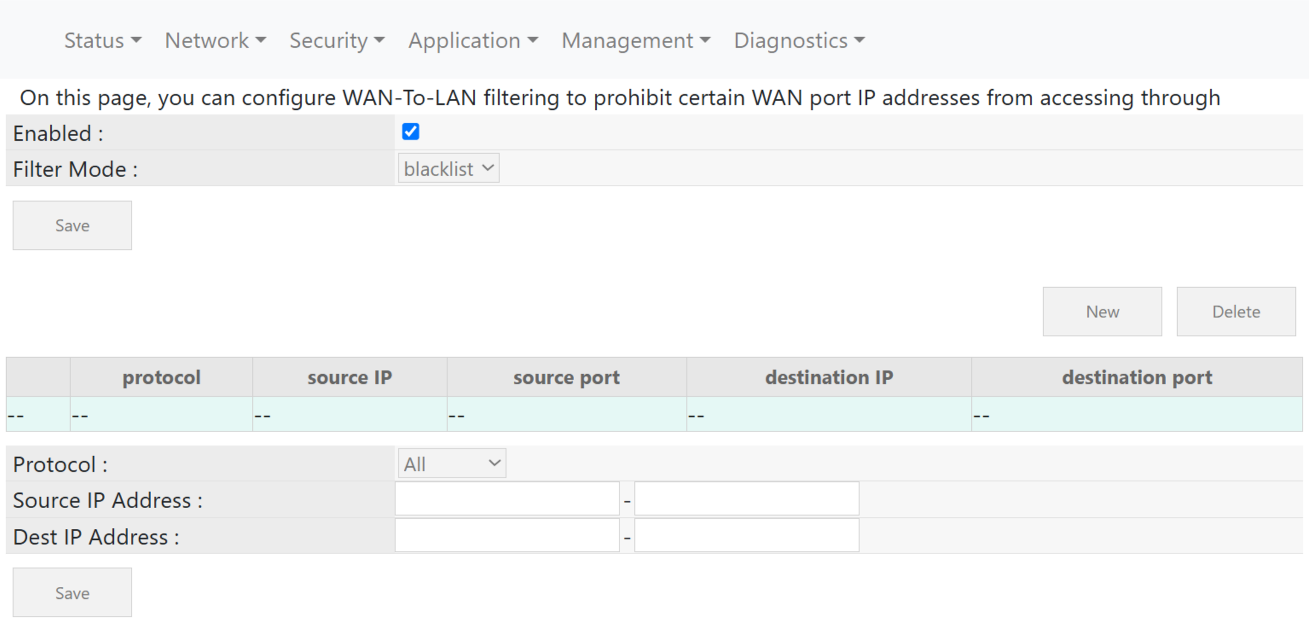
   - **Configuration:**
     - Select blacklist or whitelist based on your network security policy. A whitelist offers maximum security but requires explicit permission for all desired inbound traffic.

3. **Rule Management (Table & Buttons):**
   - **Rule Table:** This table displays the currently configured WAN-to-LAN filtering rules.
     - **protocol:** The network protocol to which the rule applies (e.g., TCP, UDP, ICMP).
     - **source IP:** The IP address or range of the *originating* device on the WAN (internet).
     - **source port:** The port number or range used by the source device on the WAN.
     - **destination IP:** The IP address of the *receiving* device on your LAN (your internal network).
     - **destination port:** The port number or range on your internal LAN device that the WAN traffic is trying to reach.
     - *(Note: The --- indicates no entries are currently configured in this example.)*
   - **New Button:** Click this button to add a new Downstream Filtering rule. This will typically activate the input fields below the table for rule definition.
   - **Delete Button:** Select one or more entries from the table (if available, usually via a checkbox next to each entry) and then click "Delete" to remove them from the list.
4. **Add/Edit Rule Entry:**
   - This section appears when adding a new rule or editing an existing one.
   - **Protocol:**
     - **Description:** Specifies the network protocol to which this rule applies.

    - **Options:** The dropdown typically includes options such as All, TCP, UDP, ICMP, etc. Selecting All applies the rule regardless of the protocol.
    - **Configuration:** Choose the specific protocol or All that the filtering rule should target.
  - **Source IP Address:**
    - **Description:** Defines the IP address range of the *originating* device(s) on the WAN from which connections are being attempted.
    - **Format:** Typically, you can enter a single IP address (e.g., 203.0.113.5) or an IP address range (e.g., 203.0.113.1 - 203.0.113.10). The two input fields separated by a hyphen suggest an IP range. Use 0.0.0.0 or leave blank for "Any" source IP.
    - **Configuration:** Enter the external source IP address or range you wish to filter.
  - **Source Port:**
    - **Description:** Specifies the port number(s) used by the *originating* device on the WAN. For incoming connections, this is often a dynamic port, but can be specified if you need to block/allow traffic from specific external source ports.
    - **Format:** Can be a single port (e.g., 12345), a port range (e.g., 1024 - 5000), or left blank/set to "Any" to include all ports. The two input fields separated by a hyphen suggest a port range.
    - **Configuration:** Enter the external source port or range.
  - **Dest IP Address:**
    - **Description:** Defines the IP address range of the *destination* device(s) on your LAN that the incoming WAN traffic is trying to reach.
    - **Format:** Similar to Source IP, can be a single internal IP address or an internal IP address range.
    - **Configuration:** Enter the internal destination IP address or range. This is often the IP address of a server or a specific device you are protecting.
  - **Destination Port:**

        - **Description:** Specifies the port number(s) on the *destination* internal device. This is crucial for controlling access to specific services (e.g., 80 for HTTP, 443 for HTTPS, 22 for SSH, 3389 for RDP).
        - **Format:** Can be a single port, a port range, or left blank/set to "Any".
        - **Configuration:** Enter the destination port or range on your internal device.
    - **Save Button (for individual rule):**
        - After defining the parameters for a new or edited rule, click this "Save" button to add the rule to the "Rule Table." This action adds the individual rule but does *not* save the overall Downstream Filtering configuration for the device yet.

Figure 9.5. Upstream Filtering Configuration



On this page, you can configure WAN-To-LAN filtering to prohibit certain WAN port IP addresses from accessing through

Enabled :	☑
Filter Mode :	blacklist

	protocol	source IP	source port	destination IP	destination port
--	--	--	--	--	--

Protocol :	All
Source IP Address :	-
Dest IP Address :	-

Overall Saving Configuration:

- After making all desired changes, including enabling/disabling Downstream Filtering, selecting the filter mode, and adding/deleting individual rules, ensure you click the **Save** button located at the top of the Downstream Filtering section (next to "Enabled :") to apply all changes permanently. Changes will not take effect until this main "Save" button is clicked.

9.5 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is a feature designed to simplify the process of connecting wireless devices to your network without needing to manually enter complex network names (SSIDs) or security keys.

9.5.1 Introduction to WPS

WPS aims to make connecting new devices to a secure Wi-Fi network easier. Users do not need knowledge about SSIDs, channels, or security settings. Instead, they can use simple methods like Push Button Configuration (PBC) or a Personal Identification Number (PIN) to establish a secure connection.

When WPS is initiated, a registration protocol occurs between the "registrar" (typically the BIN62X2PLIRT gateway) and the "enrollee" (the client device). The enrollee receives the SSID and security settings from the registrar and then joins the network securely.

9.5.2 Supported WPS Features

The BIN62X2PLIRT supports WPS features for various operational modes, including AP mode and Infrastructure-Client mode. It offers both the Push Button method and the PIN method.

For each method, the gateway offers different security levels for network credentials, such as Open Security, WEP 64/128 bits, WPA2-Personal TKIP, and WPA2-Personal AES.

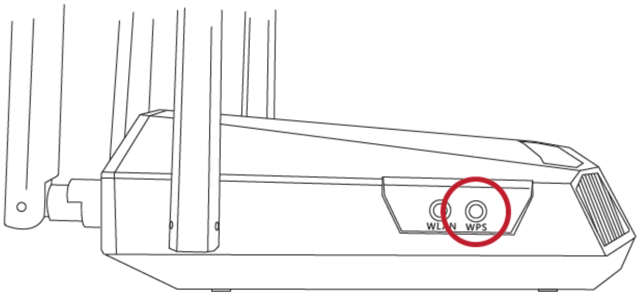
WARNING: Certain unsupported modes (e.g., WDS mode, Infrastructure-Adhoc mode) will cause WPS to be disabled if enforced.

9.5.3 Push Button Method

The Push Button Method (PBC) is the simplest way to establish a WPS connection.

1. **Initiate WPS on Gateway:** Press the **WPS button** on the rear panel of your BIN62X2PLIRT for at least 3 full seconds. The WPS LED indicator on the front panel will begin to flash, signifying that the gateway is actively searching for a WPS-enabled client device for the next 120 seconds (2 minutes).

Figure 9.6. WPS Button Location



2. **Initiate WPS on Client Device:** Within 2 minutes of pressing the WPS button on the gateway, activate the WPS function on your wireless client device (e.g., laptop, smartphone, wireless printer). This is typically done by pressing a physical WPS button on the device or by selecting a WPS option in its software.
3. **Connection Establishment:** The devices will automatically exchange security information and establish a secure wireless connection. The WPS LED on the gateway will likely change its state (e.g., solid green) to indicate a successful connection.

10. QoS Settings

Quality of Service (QoS) is a set of technologies that guarantee a certain level of performance for data flow over a network. The BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway includes advanced QoS prioritizes certain types of network traffic over others, ensuring optimal performance for critical applications (e.g., VoIP, online gaming, video conferencing) even during periods of high network congestion.

The BIN62X2PLIRT's QoS implementation allows you to:

- Prioritize specific applications, devices, or types of traffic.
- Allocate bandwidth more efficiently.
- Reduce latency and jitter for real-time services.

10.1 Uplink QoS Configuration

Uplink QoS allows you to manage and allocate your upstream bandwidth by assigning different priorities, weights, or dedicated bandwidth to various types of data queues. This helps prevent bandwidth-intensive but less time-sensitive traffic from negatively impacting latency-sensitive or critical applications.

To access these settings, navigate to **Network** > **QOS Settings** > **Uplink QoS Configuration**

Configuration:

1. **Template Index:**
    - **Description:** This field likely indicates a pre-configured QoS template being used or selected. "TR069,VOIP,IPTV,INTERNE" suggests that this template might be optimized for services like TR-069 (remote management), Voice over IP, IPTV, and general internet Browse, possibly implying predefined priority rules for these services.
    - **Configuration:** This is usually a display-only field or a dropdown to select a different pre-existing QoS template, if available. For a technical user, understanding the services included in a template is key.

2. **Enable QoS Module:**
   - **Description:** This checkbox is the master switch to enable or disable the entire QoS functionality for the uplink.
   - **Configuration:**
     - **Check the box:** To activate Uplink QoS and apply the configured rules.
     - **Uncheck the box:** To disable Uplink QoS, meaning all uplink traffic will be treated equally without prioritization.
3. **Total Upstream Bandwidth:**
   - **Description:** This field specifies the maximum uplink bandwidth available for your internet connection, in Kilobits per second (Kbps). It is crucial for the QoS module to accurately allocate and prioritize traffic within the limits of your actual internet service speed.
   - **Configuration:** Enter your provisioned upstream bandwidth provided by your Internet Service Provider (ISP). An accurate value is critical for effective QoS.
   - **Units:** (Kbps) - Kilobits per second.
4. **QoS Scheduling Mode Selection:**
   - **Description:** This dropdown determines the algorithm the QoS module uses to manage and prioritize traffic across different queues.
   - **Options:** The image shows "Scheduling by Priority" is selected. Other common modes might include:
     - **Strict Priority (SP):** High-priority queues are served completely before lower-priority queues get any bandwidth.
     - **Weighted Fair Queuing (WFQ):** Distributes bandwidth among queues based on their assigned weights, ensuring all queues get some bandwidth.
     - **Deficit Weighted Round Robin (DWRR):** Similar to WFQ but designed to handle variable packet sizes more efficiently.
   - **Configuration:** Choose the scheduling mode that best suits your network's traffic patterns and prioritization needs. "Scheduling by Priority" implies that the "Priority" values in the queue settings table will directly dictate service order.
5. **Enable DCSP/TC Re-tagging:**

- **Description:** This option relates to re-marking QoS tags in outgoing packets.
    - **DSCP (Differentiated Services Code Point):** A field in the IP header used to classify and manage network traffic.
    - **TC (Traffic Class):** A similar field used in IPv6.
- **Configuration:** When enabled, the device can modify or assign DSCP/TC values to outgoing packets based on your QoS rules, ensuring that downstream network devices (like your ISP's equipment) can also potentially apply QoS policies based on these tags. This helps maintain QoS across multiple network hops.

6. **Select 802.1p remarking:**
    - **Description:** This option pertains to remarking 802.1p priority bits in the Ethernet frame header (Layer 2 QoS). 802.1p is commonly used in LANs and VLANs to prioritize traffic at the local network level.
    - **Configuration:** You can typically choose a specific 802.1p value (0-7, where 7 is the highest priority) to assign to prioritized traffic. "Mark as 0" (Best Effort) is selected, implying no specific 802.1p remarking is currently active. If you have managed switches that support 802.1p, this can extend QoS prioritization to your internal wired network.
7. **Queue Settings:**
    - **Description:** This table allows you to define individual traffic queues and their specific QoS parameters. Your QoS rules (defined elsewhere, often in "Flow Classification Rule Configuration" or "Services Queue Configuration" - not shown here) would direct specific traffic types into these queues.
    - **Columns:**
        - **Queue number:** An identifier for the queue (1 to 8 shown).
        - **Enable:** A checkbox to activate or deactivate a specific queue. Only enabled queues will participate in QoS.
        - **Priority (1 is the highest priority):** Assigns a priority level to the queue. As "Scheduling by Priority" is selected, queues with a lower priority number (e.g., 1) will be served before queues with a higher priority number (e.g., 8).
        - **Weight (%):** If the scheduling mode supports weighted fairness (e.g., WFQ), this field would define the proportion of available

bandwidth this queue receives. In "Scheduling by Priority" mode, weight might be secondary or unused.

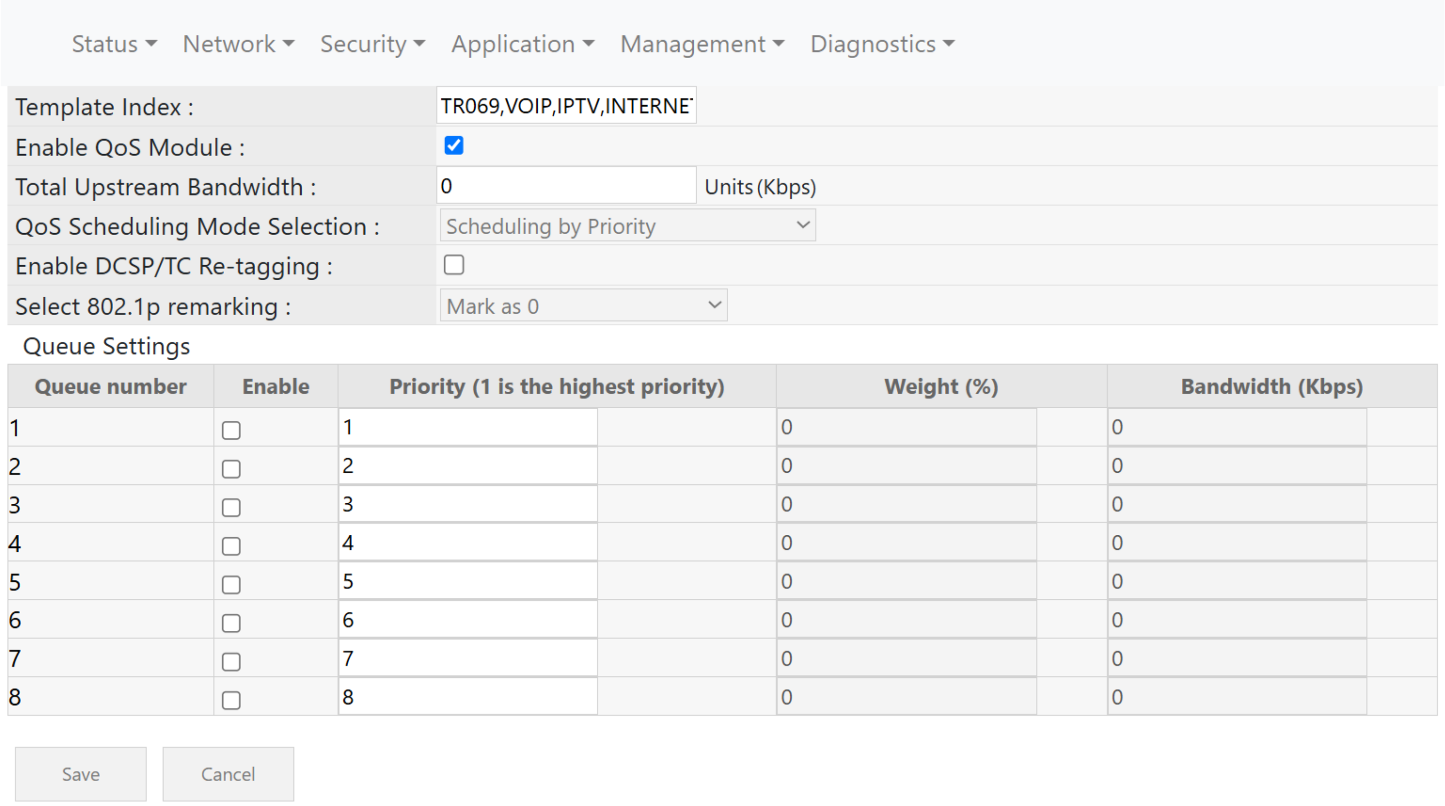
    - **Bandwidth (Kbps):** Allows you to allocate a minimum guaranteed bandwidth or a maximum limit for this specific queue.

  - **Configuration:** For each queue you intend to use:
    - Check "Enable".
    - Assign a "Priority" level (lower number = higher priority).
    - Set "Weight (%)" and/or "Bandwidth (Kbps)" as needed, based on your scheduling mode and traffic requirements.

General Actions:

- **Save:** After configuring all Uplink QoS settings, click the **Save** button to apply your changes. The device will then implement the new QoS policies.
- **Cancel:** Discards any unsaved changes and returns to the previous state.

Figure 10.1. Uplink QoS Configuration



Template Index :	TR069,VOIP,IPTV,INTERNE
Enable QoS Module :	☑
Total Upstream Bandwidth :	0 Units (Kbps)
QoS Scheduling Mode Selection :	Scheduling by Priority
Enable DCSP/TC Re-tagging :	☐
Select 802.1p remarking :	Mark as 0

Queue Settings

Queue number	Enable	Priority (1 is the highest priority)	Weight (%)	Bandwidth (Kbps)
1	☐	1	0	0
2	☐	2	0	0
3	☐	3	0	0
4	☐	4	0	0
5	☐	5	0	0
6	☐	6	0	0
7	☐	7	0	0
8	☐	8	0	0

10.2 Priority Tag

This feature enables you to classify and re-tag network packets with specific priority markers (802.1p, DSCP, TC). Priority Tagging, or remarking, involves modifying the QoS fields within network packet headers. By setting these tags, you can align your internal QoS policies with external network capabilities or ensure that your internal switches properly prioritize traffic within your LAN. Each entry typically corresponds to a "stream" or flow of traffic that has been previously classified (e.g., in "Flow Classification Rule Configuration," if available on this device).

To access these settings, navigate to Network > QOS Settings > priority tag.

Configuration:

1. **Stream Sequence Number / Rule Table:**
    - **Description:** This table lists the configured traffic streams for priority tagging. Each row represents a specific rule.
    - **Columns:**
        - **Stream Sequence Number:** An identifier for the rule/stream.
        - **802.1p Re-tag:** The new 802.1p priority value assigned to packets in this stream.
        - **DSCP Re-tag (for IPv4 messages only):** The new DSCP value assigned to IPv4 packets in this stream.
        - **TC Re-tag (for IPv6 messages only):** The new Traffic Class value assigned to IPv6 packets in this stream.
        - **Queue:** The QoS queue to which traffic for this stream will be directed.
    - *(Note: The --- indicates no entries are currently configured.)*
    - **New Button:** Click this button to add a new priority tagging rule. This will typically activate the input fields below for rule definition.
    - **Delete Button:** Select one or more entries from the table (if available, usually via a checkbox next to each entry) and then click "Delete" to remove them from the list.
2. **Add/Edit Priority Tag Rule Entry:**
    - This section appears below the listing table when adding a new rule or editing an existing one.
    - **802.1p Retagging :**

    - **Description:** This field specifies the 802.1p priority value (Layer 2 QoS) to be assigned to packets in this stream. 802.1p values are typically used for prioritization within local area networks (VLANs, managed switches).
    - **Range:** (0-7), where 0 is the lowest priority (best effort) and 7 is the highest priority.
    - **Configuration:** Select the desired 802.1p priority value.
  - **DSCP remarking (IPv4 packets only) :**
    - **Description:** This field specifies the Differentiated Services Code Point (DSCP) value (Layer 3 QoS) to be assigned to IPv4 packets in this stream. DSCP values are used for per-hop behavior (PHB) and can influence how packets are treated across different routers and networks, including your ISP's network if they honor DSCP markings.
    - **Range:** (0-63). Common values include EF (Expedited Forwarding - 46 for VoIP), AF (Assured Forwarding), and CS (Class Selector).
    - **Configuration:** Select the desired DSCP value.
  - **TC Re-tagging (for IPv6 messages) :**
    - **Description:** This field specifies the Traffic Class (TC) value (Layer 3 QoS) to be assigned to IPv6 packets in this stream. It serves a similar purpose to DSCP for IPv4, classifying traffic for QoS treatment in IPv6 networks.
    - **Range:** (0-63).
    - **Configuration:** Select the desired TC value.
  - **Queue:**
    - **Description:** This dropdown allows you to associate this traffic stream with a specific QoS queue that you have configured in the "Uplink QoS Configuration" (or similar queue management section). Traffic marked by this rule will be directed into the selected queue for further scheduling and bandwidth management.
    - **Configuration:** Select the appropriate queue number (e.g., 1-8, as seen in "Uplink QoS Configuration").

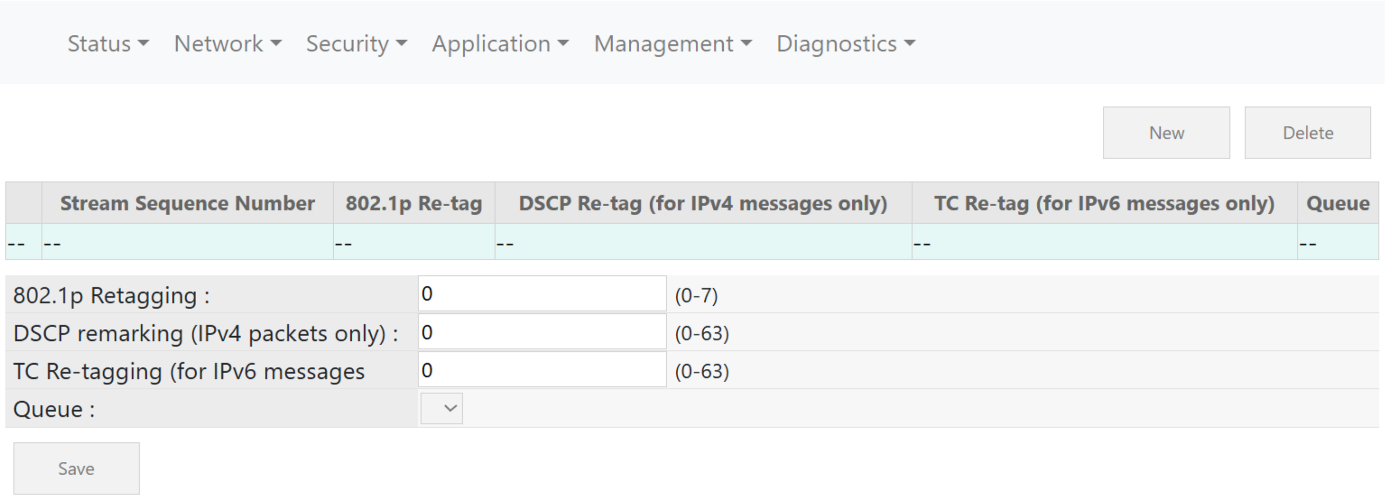
General Actions:

- **Save:** After defining the parameters for a new or edited rule (802.1p, DSCP, TC, and Queue), click the **Save** button to add/update the rule in the "Stream Sequence Number" table. This button saves the individual rule.
- **Overall Save (Implied):** While not explicitly shown with a dedicated button at the top like in other sections, changes to these priority tags would typically need to be applied by a main "Save" button for the entire QoS configuration or an "Apply" button within the "priority tag" section to ensure all rules become active.

Important Notes for Technical Users:

- **Traffic Classification:** This "Priority Tag" section *re-marks* traffic. The process of *identifying* which traffic belongs to which stream is typically done in a "Flow Classification Rule Configuration" section (visible in the QoS dropdown), where you define rules based on source/destination IP, port, protocol, etc.
- **End-to-End QoS:** For QoS to be truly effective across the internet, your ISP and all intermediate network devices must honor and act upon the QoS tags you apply. This is often limited for standard consumer internet services.
- **Internal QoS:** 802.1p remarking is highly effective for prioritizing traffic within your local network if you have managed switches that support VLANs and 802.1p priority queuing.
- **Consistency:** Ensure that your re-tagging values (802.1p, DSCP, TC) are consistent with the QoS policies and capabilities of your downstream/upstream network devices to avoid unexpected behavior or dropped packets.
- **Monitoring:** Monitor network performance after configuring priority tags to ensure that critical traffic is receiving the desired prioritization and that other traffic is not unduly impacted.

Figure 10.2. Priority Tag



	Stream Sequence Number	802.1p Re-tag	DSCP Re-tag (for IPv4 messages only)	TC Re-tag (for IPv6 messages only)	Queue
--	--	--	--	--	--

802.1p Retagging :	0	(0-7)
DSCP remarking (IPv4 packets only) :	0	(0-63)
TC Re-tagging (for IPv6 messages	0	(0-63)
Queue :		

10.3 Flow Classification Rule Configuration

Flow Classification rules are essentially the "IF" part of a QoS policy: "IF traffic matches these conditions, THEN it belongs to this class/flow." Once traffic is classified, it can be directed to a specific QoS queue, re-marked with priority tags, or subjected to bandwidth limits.

To access these settings, navigate to **Network** > **QOS Settings** > **Flow Classification Rule Configuration**.

Configuration:

1. **Rule Table:**
   - **Description:** This table lists the currently configured traffic classification rules. Each row represents a specific rule that defines a traffic flow.
   - **Columns:**
     - **Classification Type Number:** An identifier for the type of classification (e.g., typically indicating a specific service or application category).
     - **Flow Sequence Number:** A unique identifier for the specific rule within a classification type.
     - **Protocol:** The network protocol(s) (e.g., TCP, UDP, ICMP, RTP, ICMPv6) that this rule matches.
     - **Type:** The classification method used (e.g., source MAC, destination IP, port range).
     - **Min.:** The minimum value for the specified "Type" (e.g., minimum port number, start of IP range).
     - **Max.:** The maximum value for the specified "Type" (e.g., maximum port number, end of IP range).
   - *(Note: The --- indicates no entries are currently configured.)*
   - **New Button:** Click this button to add a new classification rule. This will typically activate the input fields below for rule definition.
   - **Delete Button:** Select one or more entries from the table (if available, usually via a checkbox next to each entry) and then click "Delete" to remove them from the list.
2. **Add/Edit Flow Classification Rule Entry:**
   - This section appears below the listing table when adding a new rule or editing an existing one.

- **Data Stream Sequence Number :**
  - **Description:** This dropdown likely allows you to assign a unique identifier or associate this rule with a broader data stream category. "None" is selected, implying you might assign it manually or it's auto-assigned when a new rule is created.
  - **Configuration:** Select or assign a sequence number for the rule.
- **Protocol :**
  - **Description:** Specifies the network protocol(s) that packets must use to match this rule.
  - **Options:** Checkboxes for TCP, UDP, ICMP, RTP, ICMPv6. You can select one or more.
    - **TCP (Transmission Control Protocol):** Connection-oriented protocol used by web Browse, email, file transfers.
    - **UDP (User Datagram Protocol):** Connectionless protocol used by DNS, VoIP, video streaming.
    - **ICMP (Internet Control Message Protocol):** Used for network diagnostics (e.g., ping, traceroute).
    - **RTP (Real-time Transport Protocol):** Commonly used for real-time audio/video streaming (e.g., VoIP calls). This is a critical protocol for prioritizing voice/video.
    - **ICMPv6 (Internet Control Message Protocol version 6):** ICMP for IPv6 networks.
  - **Configuration:** Select the protocol(s) relevant to the traffic you want to classify.
- **Type :**
  - **Description:** This dropdown defines the specific criteria used to classify the traffic flow. This is where you specify *what* characteristic of the packet you're looking at (e.g., MAC address, IP address, port number).
  - **Options:** The image shows "source MAC" is selected. Other common options typically include:
    - **Source IP:** IP address of the sender.
    - **Destination IP:** IP address of the receiver.
    - **Source Port:** Port number used by the sender application.

- **Destination Port:** Port number used by the receiver application (e.g., 80 for HTTP, 443 for HTTPS, 5060 for SIP/VoIP).
- **DSCP:** Differentiated Services Code Point value.
- **802.1p:** 802.1p priority value.
- **Configuration:** Select the classification type. Once selected, additional input fields (like min/max for IP ranges or port ranges) will typically appear for you to define the specific values for that type.
- **Save Button (for individual rule):**
  - After defining all parameters for a new or edited rule, click this "Save" button to add the rule to the "Rule Table." This action adds the individual rule but does *not* save the overall Flow Classification Configuration for the device yet.

General Actions:

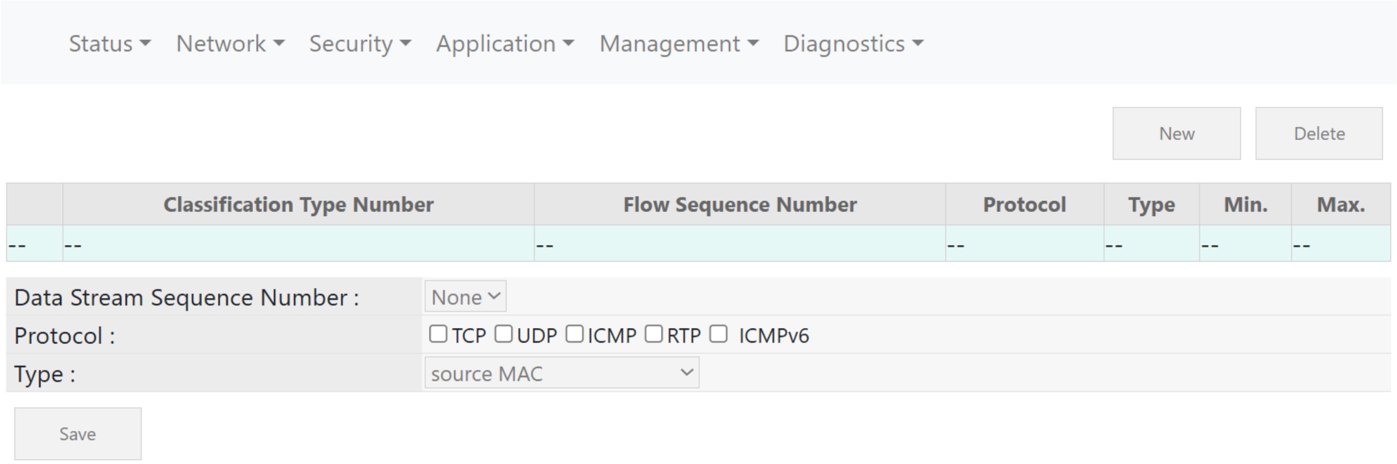
- **Save:** After adding or deleting rules, there would typically be a main "Save" button for the entire "Flow Classification Rule Configuration" page (not explicitly shown in the current view) to apply all changes permanently.

Important Notes for Technical Users:

- **Interdependence with other QoS settings:** These classification rules *identify* traffic. The identified traffic then needs to be mapped to specific QoS queues (as seen in "Uplink QoS Configuration") or re-marked with priority tags (as seen in "Priority Tag Configuration") for QoS to be truly effective. This is the "IF" part; the other QoS sections are the "THEN" part.
- **Precision:** Be precise when defining classification rules. Overly broad rules might prioritize unintended traffic, while overly narrow rules might miss traffic you intend to classify.
- **Order of Rules:** In some implementations, the order of classification rules can matter (e.g., the first matching rule applies). Consult the full device manual if you encounter unexpected classification behavior.
- **Common Use Cases:**
  - **VoIP:** Classify UDP traffic on specific VoIP ports (e.g., 5060 for SIP, RTP port ranges) and prioritize it.
  - **Video Streaming:** Classify TCP/UDP traffic on common streaming ports or by destination IPs of streaming services.

- **Gaming:** Classify traffic on specific game ports and prioritize it

Figure 10.3. Flow Classification Rule Configuration



	Classification Type Number	Flow Sequence Number	Protocol	Type	Min.	Max.
--	--	--	--	--	--	--

Data Stream Sequence Number :	None
Protocol :	☐ TCP ☐ UDP ☐ ICMP ☐ RTP ☐ ICMPv6
Type :	source MAC

10.4 Services Queue Configuration

The "Services Queue Configuration" acts as a bridge between a list of pre-defined or recognized services and the QoS queues. It streamlines the process of applying QoS policies by allowing you to simply select a service and assign it to a queue, rather than manually defining all the parameters (like IP addresses, ports, protocols) that constitute that service.

To access these settings, navigate to **Network** > **QOS Settings** > **Services Queue Configuration**.

Configuration:

1. **Service Mapping Table:**
   - **Description:** This table lists the available network services and their current mapping to QoS queues.
   - **Columns:**
     - **Service Name:** The name of the recognized network service (e.g., "TR069", "VOIP"). These services are typically pre-defined by the device's firmware based on common applications and protocols.
     - **Queue Name:** A dropdown menu that allows you to select which QoS queue this specific service's traffic will be assigned to. The queue numbers (e.g., 1, 2) correspond to the queues configured in the "Uplink QoS Configuration" (or a similar queue definition section), where priorities, weights, and bandwidth limits are set.
   - **Example Entries:**

- **TR069:** A protocol for remote management of customer-premises equipment (CPE). It's often critical for ISP support and firmware updates, hence it's mapped to Queue 1, which typically implies a higher priority.
- **VOIP:** Voice over IP traffic. VoIP is highly sensitive to latency and packet loss, so it's mapped to Queue 2, indicating it will also receive preferential QoS treatment.

2. **Mapping Configuration:**
   - **Configuration:** For each Service Name listed, use the Queue Name dropdown menu to select the desired QoS queue. The available queue numbers (e.g., 1 through 8, if those are your configured queues) correspond to the queues set up in the "Uplink QoS Configuration" (or similar queue management area).
   - **Prioritization:** By mapping a service to a higher priority queue, you instruct the device to give that service's traffic preference over traffic assigned to lower priority queues when network congestion occurs.

General Actions:

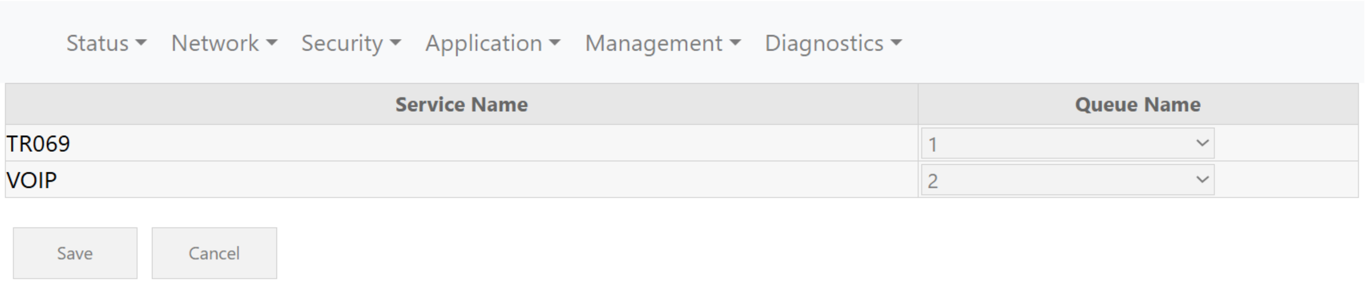
- **Save:** After making any changes to the service-to-queue mappings, click the **Save** button to apply your configuration. The device will then begin applying the QoS policies for the re-mapped services.
- **Cancel:** Click this button to discard any unsaved changes and revert to the previous configuration.

Important Notes for Technical Users:

- **Pre-defined Services:** The "Service Name" entries are typically built-in and cannot be modified or added to directly from this interface. If you need to classify custom applications or protocols, you would usually use the "Flow Classification Rule Configuration" (as previously discussed) to define those specific traffic types and then map them to queues.
- **Queue Definition is Key:** This section only *maps* services to queues. The actual QoS parameters (priority, weight, bandwidth) for each queue are defined in the "Uplink QoS Configuration" or a similar queue management section. Ensure your queues are configured appropriately for the services you are mapping.
- **Consistency:** Ensure that the services you map to queues truly represent the traffic you want to prioritize. For instance, if you prioritize "VOIP" but your VoIP traffic is not correctly classified by the device, the QoS will be ineffective.

- **Monitoring:** After configuring services queue mappings, monitor your network performance, especially for the prioritized services, to ensure that the QoS is working as expected and providing the desired performance improvements.

Figure 10.4 Services Queue Configuration



Service Name	Queue Name
TR069	1
VOIP	2

10.5 Speed Limit Configuration

Speed limits work by restricting the maximum data rate (bandwidth) that a defined flow of traffic can utilize. This is particularly useful in environments where you need to guarantee a minimum level of service for critical users or services, or to prevent a single user from consuming all available bandwidth.

To access these settings, navigate to **Network** > **QOS Settings** > **Speed limit configuration**.

Configuration Options:

1. **Uplink speed limit mode:**
   - **Description:** This dropdown menu controls how uplink (outgoing, LAN-to-WAN) bandwidth limits are applied.
   - **Options (inferred):** The image shows "Unlimited Speed" as selected. Other common options would typically include:
     - **Unlimited Speed:** No speed limit is applied.
     - **By Port:** Apply speed limits to specific physical LAN ports.
     - **By VLAN:** Apply speed limits to traffic associated with specific Virtual LANs.
     - **By IP Segment:** Apply speed limits to traffic originating from or destined for specific IP address ranges.
   - **Configuration:** Select the desired mode based on how you wish to control outgoing bandwidth.
2. **Downlink speed limit mode:**

- **Description:** This dropdown menu controls how downlink (incoming, WAN-to-LAN) bandwidth limits are applied.
- **Options (inferred):** Similar to the uplink, "Unlimited Speed" is selected. Other options would typically mirror those for uplink (e.g., By Port, By VLAN, By IP Segment).
- **Configuration:** Select the desired mode based on how you wish to control incoming bandwidth.

3. **Speed Limit Format Notes:**
   - **Description:** This critical note provides examples of how to format the speed limit configuration string based on the selected mode. The unit for the speed limit is **512Kbps**. This means if you enter '1', the limit is 512Kbps; if you enter '2', it's 1024Kbps (1Mbps), and so on.
   - **Formats Explained:**
     - **If the port speed limit is selected, the speed limit format is m1/n1,m2/n2, such as LAN1/1,LAN2/2, and the unit is 512Kbps.**
       - **Explanation:** This format is used when you select a "By Port" speed limit mode. m refers to the LAN port number (e.g., LAN1, LAN2). n refers to the speed limit value (a multiplier of 512Kbps).
       - **Example:** LAN1/1 would limit LAN port 1 to 1 * 512 Kbps = 512 Kbps. LAN2/2 would limit LAN port 2 to 2 * 512 Kbps = 1024 Kbps (1 Mbps). You can configure multiple ports separated by commas.
     - **If VLAN speed limit is selected, the speed limit format is m1/n1,m2/n2, such as 85/1,3001/2, and the unit is 512Kbps.**
       - **Explanation:** This format is used when you select a "By VLAN" speed limit mode. m refers to the VLAN ID (e.g., 85, 3001). n refers to the speed limit value (a multiplier of 512Kbps).
       - **Example:** 85/1 would limit traffic on VLAN ID 85 to 1 * 512 Kbps = 512 Kbps. 3001/2 would limit traffic on VLAN ID 3001 to 2 * 512 Kbps = 1024 Kbps (1 Mbps).
     - **If the IP segment speed limit is selected, the speed limit format is m1/n1,m2/n2, such as 192.168.1.10-192.168.1.20, with 512Kbps.**

  - **Explanation:** This format is used when you select a "By IP Segment" speed limit mode. m refers to an IP address or an IP address range (e.g., 192.168.1.10-192.168.1.20). n (implied, not explicitly shown in the example's n1) would refer to the speed limit value (a multiplier of 512Kbps) applied to that segment. The example 192.168.1.10-192.168.1.20, with 512Kbps implies the n value for this segment is 1 (meaning 1 * 512 Kbps). It's crucial to understand how to specify the limit for each IP segment.
  - **Example:** If the input field works with "IP_Start-IP_End/Limit_Value", then 192.168.1.10-192.168.1.20/1 would limit devices in that IP range to 512 Kbps.

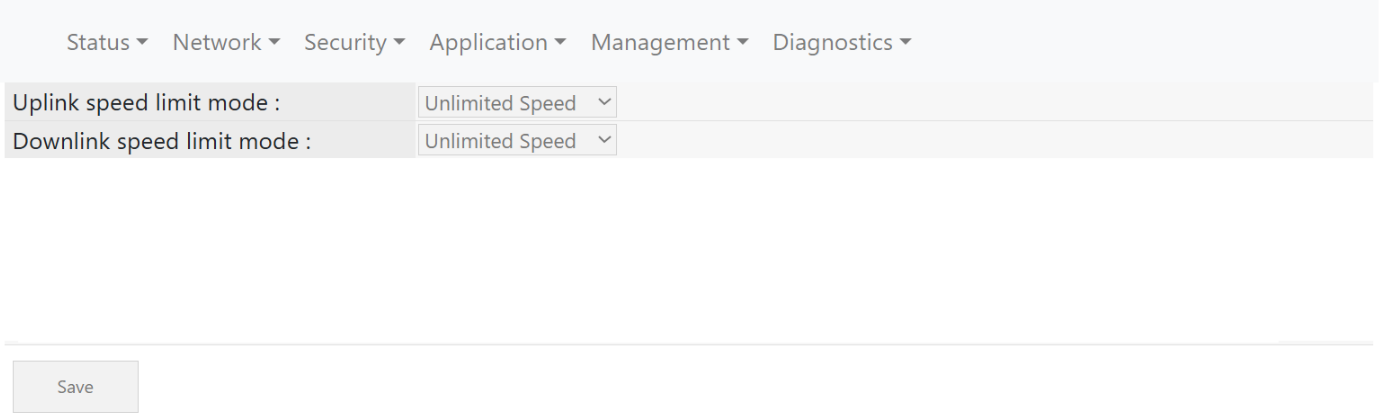
General Actions:

- **Save:** After configuring the uplink and downlink speed limit modes and entering the specific limits in the provided format (which would appear based on your mode selection, likely in a text field below the dropdowns), click the **Save** button to apply your changes. The new speed limits will take effect.

Important Notes for Technical Users:

- **Unit Conversion:** Always remember that the unit for the speed limit values (n) is **512Kbps**. Convert your desired speed (e.g., 5 Mbps) into the correct multiplier for 512Kbps. (e.g., 5 Mbps = 5120 Kbps; 5120 Kbps / 512 Kbps = 10. So you would enter 10 for a 5 Mbps limit).
- **Actual Bandwidth:** Ensure your configured speed limits do not exceed your total ISP provisioned bandwidth. Setting limits higher than your actual capacity is ineffective.
- **Granularity:** Choose the speed limit mode (Port, VLAN, IP Segment) that best matches the granularity of control you require.
- **Testing:** Test your speed limit configurations thoroughly, especially after implementation, to ensure they are working as intended and not causing unintended performance issues for critical applications.
- **Overlap:** Be careful about overlapping rules or potential conflicts if you are using multiple QoS features simultaneously (e.g., speed limits, queue prioritization, flow classification).

Figure 10.5. Speed Limit Configuration



Uplink speed limit mode :	Unlimited Speed
Downlink speed limit mode :	Unlimited Speed

11. Firmware Upgrade & Maintenance

Regular maintenance of your BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway, including firmware upgrades, is essential for optimal performance, security, and access to new features. This section outlines how to manage firmware, back up/restore settings, and reset the device to its factory defaults.

11.1 About Firmware Versions

Firmware is the embedded software that controls the hardware functions of your BIN62X2PLIRT. Manufacturers regularly release new firmware versions to:

- Improve device performance and stability.
- Fix bugs and security vulnerabilities.
- Introduce new features and capabilities.
- Enhance compatibility with new standards or devices.

It is advisable to periodically check for updated firmware versions on your ISP's or the manufacturer's support website. Your ISP's support team may also need to know your current hardware and firmware versions for troubleshooting purposes.

11.2 Manually Updating Firmware

WARNING:

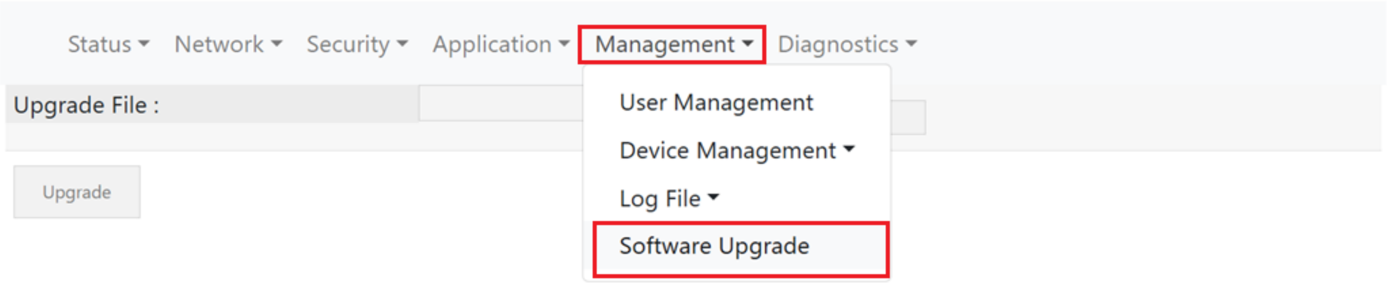
- **Do not interrupt the firmware upgrade process.** Power loss or disconnection during an upgrade can permanently damage the device, rendering it inoperable.
- Perform firmware upgrades when network usage is low.
- It is highly recommended to back up your current configuration settings before performing a firmware upgrade.

To manually update the firmware:

1. **Download Firmware:** Obtain the latest firmware file for your specific BIN62X2PLIRT model from your ISP's support portal or the manufacturer's website. Ensure the downloaded file is compatible with your device. The firmware file is typically a .bin or .img file.
2. **Access Firmware Upgrade Section:**

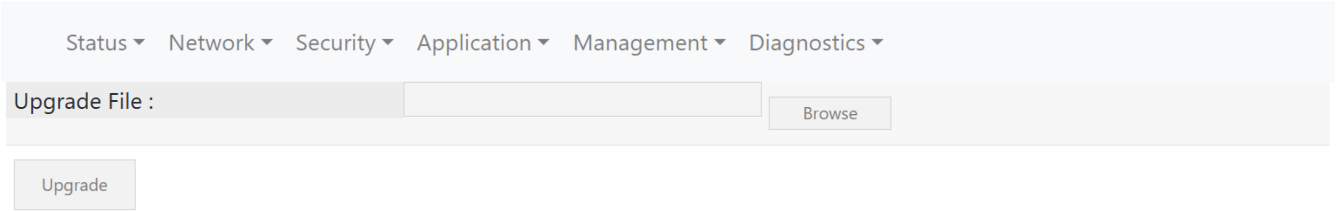
From the head menu of the web configuration interface, navigate to **Management -> Software Upgrade**

Figure 11.1. Management → Software Upgrade



3. **Browse for File:** Click the **Browse** or **Choose File** button. Navigate to the location where you saved the downloaded firmware file and select it.
4. **Start Upgrade:** Click the **Upload** or **Upgrade** button.
5. **Wait for Completion:** The device will upload the firmware and initiate the upgrade process. This may take several minutes. Do not close your browser, disconnect power, or attempt to use the device during this time. The device will typically reboot automatically upon successful completion.
6. **Verify Firmware Version:** After the device reboots, log back into the web interface and verify the firmware version under the "Status" or "Device Info" section to confirm the upgrade was successful.

Figure 11.2. Software Upgrade



11.3 Backup and Restore Settings

Regularly backing up your device's configuration settings allows you to quickly restore your preferred network setup in case of a factory reset or configuration error.

To **back up** your settings:

1. From the head menu, navigate to

Management -> Device Management -> Configuration Management

2. Click the **Backup Setting to File** button. Your browser will download a configuration file (e.g., config.conf or settings.cfg) to your computer. Store this file in a safe location.

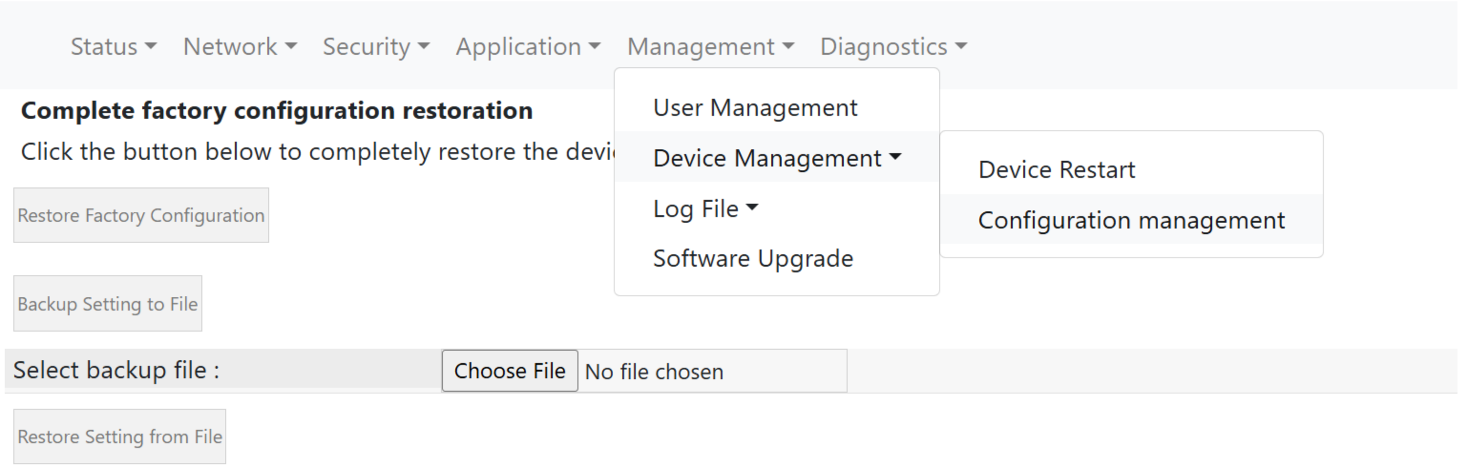
To **restore** your settings:

1. From the head menu, navigate to

Management-> Device Management -> Configuration Management

2. Click the **Choose File** button and select your previously saved configuration file.
3. Click the **Restore Setting from File** button. The device will load the settings from the file and may reboot automatically.

Figure 11.3. Backup and Restore Settings



Complete factory configuration restoration

Click the button below to completely restore the devi

Select backup file : No file chosen

11.4 Resetting to Factory Defaults

Resetting the BIN62X2PLIRT to its factory defaults will erase all custom configurations and return the device to its original out-of-the-box settings. This can be useful for troubleshooting persistent issues or when preparing to redeploy the device in a new environment.

WARNING: Performing a factory reset will erase all your custom settings, including Wi-Fi passwords, WAN configurations, and any other personalized settings. Ensure you have a backup of your settings if you wish to restore them later.

There are two methods to reset the device:

1. **Hardware Reset Button:**
   - Locate the

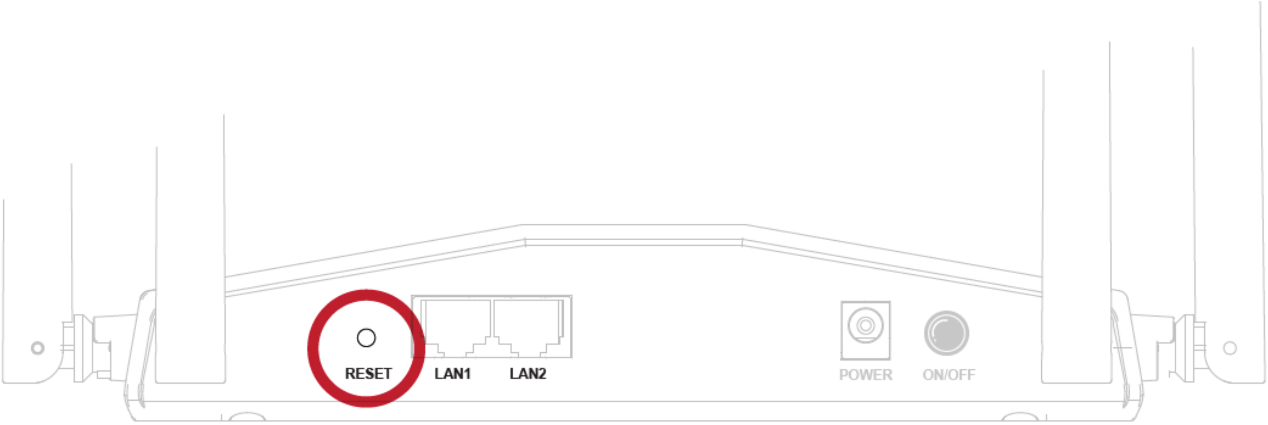
RESET button on the rear panel of the BIN62X2PLIRT (often a small, recessed pinhole).

   - With the device powered on, use a pointed object (e.g., a paperclip or a pin) to

press and hold the RESET button for at least 5 full seconds.

   - Release the button. The device will reboot, and all settings will be restored to their factory defaults.

Figure 11.4. Device Reset Button



2. **Software Reset via Web Interface:**
   - From the head menu of the web configuration interface, navigate to

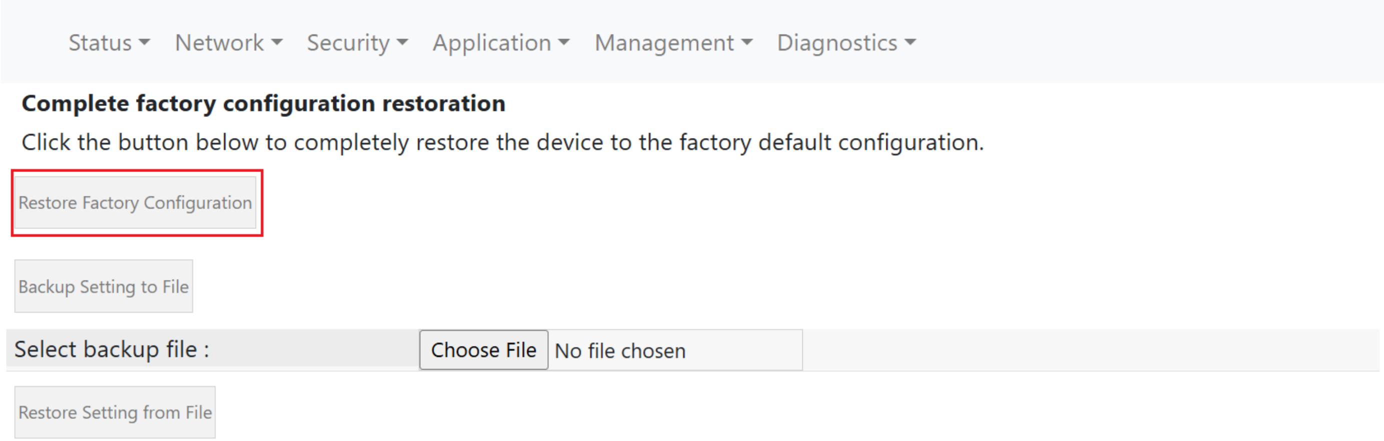
Management -> Device Management -> Configuration Management

   - Click the "**Restore Factory Configuration"** button.

- Confirm your action if prompted. The device will reboot and apply the default settings.

After a factory reset, you will need to reconfigure your Internet connection and wireless settings as if it were a new device. The default login credentials for the web interface will be reinstated.

Figure 11.5. Restore Factory Configuration



Complete factory configuration restoration

Click the button below to completely restore the device to the factory default configuration.

Select backup file : No file chosen

12. Troubleshooting

This section provides common troubleshooting suggestions and outlines how to use basic IP utilities to diagnose network connectivity issues with your BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway.

12.1 General Troubleshooting Suggestions

If you encounter problems with your network or the BIN62X2PLIRT, try the following general troubleshooting steps:

- **Check All Cable Connections:** Ensure all Ethernet cables, the fiber optic cable, and the power adapter are securely and correctly plugged into their respective ports on the gateway and other devices. Loose connections are a common cause of network issues.
- **Check LED Indicators:** Refer to Section 5, "LED Indicator Description," to understand the status indicated by the LEDs on the front panel. Abnormal LED behavior (e.g., red lights, unlit indicators) can point to the source of a problem.
- **Reboot the Device:** Often, simply restarting the BIN62X2PLIRT can resolve temporary glitches.
  1. Unplug the power adapter from the device.
  2. Wait for about 10-15 seconds.

3. Plug the power adapter back into the device.
4. Wait for the device to fully boot up (allow a few minutes for all LEDs to stabilize).

- **Reboot Connected Devices:** Restart your computer, smartphone, or other network devices. This can resolve IP address conflicts or refresh network connections.
- **Verify Internet Service:** Confirm with your ISP that there are no service outages in your area.
- **Check Router's Web Interface:** Log into the BIN62X2PLIRT's web configuration interface (refer to Section 6). Check the WAN status to ensure an IP address has been obtained and the Internet connection is active.
- **Temporarily Disable Firewall/Antivirus:** If you can connect to the router but not the internet, temporarily disable any firewall or antivirus software on your computer to see if it's blocking the connection. Remember to re-enable it afterwards.
- **Test with a Different Device:** If one device cannot connect, try connecting another device (e.g., a different computer or smartphone) to the network (wired or wireless) to determine if the issue is with the BIN62X2PLIRT or the specific device.
- **Factory Reset (Last Resort):** If all other troubleshooting steps fail, you may consider performing a factory reset (refer to Section 11.4). Remember that this will erase all your custom settings.

12.2 Diagnosing Problems Using IP Utilities

Command-line IP utilities can provide valuable information for diagnosing network connectivity issues directly from your computer.

12.2.1 Using the Ping Utility

The ping utility is used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

- **On Windows-based computers:**
  1. Open the Command Prompt:
     - Type cmd in the Start search bar and press Enter.
  2. At the command prompt, type ping followed by the IP address or hostname you want to test.

    - **Test Connectivity to Gateway:** ping 192.168.1.1 (assuming 192.168.1.1 is your gateway's IP address)
    - **Test Connectivity to Internet:** ping google.com or ping 8.8.8.8 (Google's DNS server)

  3. Press **Enter**.

  - **Interpretation:**
    - **"Reply from** Indicates a successful connection and the time taken for the reply.
    - **"Request timed out."** Indicates no reply was received, suggesting a connectivity issue.
    - **"Destination host unreachable."** Indicates that the computer cannot find a path to the destination.

12.2.2 Using the Nslookup Utility

The nslookup (name server lookup) utility is used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. It is useful for diagnosing DNS-related issues.

- **On Windows-based computers:**

  1. Open the Command Prompt (as described for

ping).

  2. At the command prompt, type

nslookup and press **Enter**.

  3. At the

> prompt, type the domain name you want to resolve (e.g., www.microsoft.com) and press **Enter**.

  - **Interpretation:**
    - The utility will display the associated IP address(es) for the domain name if known.
    - If it fails to resolve the name, it indicates a DNS problem.

  4. To exit

nslookup, type exit and press **Enter**.

13. Technical Specifications

This section provides detailed technical specifications for the BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway. This information is crucial for technical users requiring precise data on the device's capabilities and hardware components.

13.1 Performance

- **Wi-Fi Standard:** IEEE® 802.11 b/g/n/ax (2.4GHz) , IEEE® 802.11 a/an/ac/ax (5GHz)
- **Wireless Speed:** Up to 3000Mbps† (AX3000)
- **Simultaneous Dual Band Wi-Fi:** 2.4 GHz and 5 GHz operation concurrently
- **5 GHz Channel Bandwidth:** 20/40/80/160 MHz
- **Wi-Fi Transmitters/Receivers (Tx/Rx):** 2x2 (2.4GHz) + 2x2 (5GHz)
- **Sensitivity:** -90dBm
- **Device Connections:** Supports at least 50 device connections
- **Quality of Service (QoS):** Advanced Quality of Service (QoS)
- **Wi-Fi Boost:** High-power radio amplifiers

13.2 Interfaces

- **GPON WAN Port:** 1 x SC / APC (B+) GPON WAN Port
- **Gigabit Ethernet LAN Ports:** 2 x 10/100/1000Mbps Gigabit Ethernet LAN ports
- **Phone Ports:** (If applicable) 2 x FXS ports for VoIP (not explicitly in datasheet, but common for "Home Gateway")
- **Power Input:** DC Jack
- **Buttons:**
  - Power on/off Button
  - Reset Button
  - WPS Button
  - Wi-Fi On/Off Button

13.3 Wireless Features

- **Security:** WPA/WPA2/WPA3 Security
- **Band Steering Support:** Yes
- **Easy Mesh:** Yes

13.4 Physical Specifications

- **Dimensions:** 185 x 150 x 35 mm

13.5 Standards and Protocols

- **Wi-Fi Standards:**
    - IEEE® 802.11 b/g/n/ax (2.4GHz)
    - IEEE® 802.11 a/an/ac/ax (5GHz)
- **Networking Standards:** IEEE 1905.1
- **GPON Standards:**
    - ITU-I G.984
    - ITU-I G.988 (OMCI)
- **Protocols:**
    - PPPoE
    - IPOE
    - IPv4/6
    - DNS
    - DHCP Server
    - NAPT
    - IGMP
    - Dynamic DNS
    - TCP/UDP/Port Filtering

13.6 Memory and Chipset

- **Memory:** 256MB flash, 512MB RAM
- **Chipset:** Hi5662YV100
- **Wi-Fi Chip:** Hi5622V100
- **CPU:** Dual core, ARM Cortex-A... (partial information from snippet)

14. Safety Information

This section provides important safety guidelines for the proper and safe operation of your BIN62X2PLIRT AX3000 GPON Wi-Fi 6 Home Gateway. Adhering to these guidelines will help prevent damage to the device, ensure personal safety, and maintain optimal performance.

14.1 General Safety Guidelines

- **Read Instructions:** Always read and follow all installation and operation instructions carefully.
- **Intended Use:** Use the device only for its intended purpose as a home gateway.
- **Ventilation:** Ensure adequate ventilation around the device. Do not block any ventilation openings or place the device in an enclosed space that restricts airflow. Overheating can lead to device malfunction or damage.
- **Placement:** Place the device on a stable, flat surface. Avoid placing it near heat sources (e.g., radiators, heat registers, stoves, amplifiers), direct sunlight, or in areas with excessive moisture, dust, or vibrations.
- **Cleaning:** Clean the device only with a soft, dry cloth. Do not use liquid cleaners or aerosol cleaners.
- **Disassembly:** Do not attempt to open or disassemble the device. There are no user-serviceable parts inside. Opening the device will void your warranty and may expose you to dangerous components.
- **Disposal:** Dispose of the device and its components (e.g., power adapter) in accordance with local environmental regulations. Do not dispose of electronic devices in regular household waste.

14.2 Electrical Safety

- **Power Source:** Use only the power adapter supplied with your BIN62X2PLIRT. Using an unauthorized power adapter can damage the device and pose a fire or electric shock hazard.
- **Power Cord Protection:** Protect the power cord from being walked on or pinched, particularly at plugs, convenience receptacles, and the point where they exit from the device.
- **Overloading:** Do not overload wall outlets, extension cords, or power strips, as this can result in a risk of fire or electric shock.
- **Moisture and Liquids:** Never expose the device to water or any other liquids. Do not operate the device if your hands are wet. If the device comes into contact with liquid, immediately unplug the power adapter.
- **Lightning:** For added protection during a lightning storm, or when left unattended and unused for long periods of time, unplug the device from the wall outlet and disconnect the network cables.

14.3 Environmental Considerations

- **Temperature:** Operate the device within the specified temperature range (typically 0°C to 40°C or 32°F to 104°F). Extreme temperatures can affect performance and device lifespan.
- **Humidity:** The device is designed to operate within a specific humidity range (typically 10% to 90% non-condensing). Avoid environments with very high or very low humidity.

15. Glossary

- **802.1p**: A QoS (Quality of Service) mechanism used at Layer 2 (Ethernet frame header) to prioritize traffic within a Local Area Network (LAN), often in conjunction with VLANs and managed switches. Values range from 0 (lowest priority/best effort) to 7 (highest priority).
- **AX3000**: Refers to the maximum theoretical wireless speed of 3000 Mbps supported by the Wi-Fi 6 (802.11ax) standard on the Home Gateway.
- **Band Steering**: A feature that optimizes client connections by automatically steering devices to the most appropriate Wi-Fi band (either 2.4GHz or 5GHz) to ensure optimal performance.
- **Blacklist**: In MAC filtering or port filtering, a list of MAC addresses or rules that are explicitly **not allowed** to access the network or pass traffic.
- **CPE (Customer-Premises Equipment)**: Telecommunications equipment located on the customer's physical premises, such as the BIN62X2PLIRT Home Gateway.
- **DHCP (Dynamic Host Configuration Protocol)**: A network protocol that automatically assigns IP addresses and other network configuration parameters to devices connected to a network, simplifying network management.
- **DNS (Domain Name System)**: A hierarchical and decentralized naming system for computers, services, or any resource connected to the Internet or a private network. It translates human-readable domain names into numerical IP addresses.
- **DSCP (Differentiated Services Code Point)**: A 6-bit field in the IP header used for Layer 3 QoS, allowing classification and prioritization of network traffic across different routers and networks. Values range from 0 to 63.
- **Dual-Band Concurrent Wi-Fi**: The ability of a Wi-Fi device to operate simultaneously on both the 2.4 GHz and 5 GHz wireless frequency bands.
- **Dynamic DNS**: A service that automatically updates a Domain Name System (DNS) record for a host whenever its IP address changes.

- **Ethernet**: A family of wired computer networking technologies commonly used in local area networks (LANs).
- **Firmware**: The embedded software that provides the low-level control for the hardware of the device, allowing it to function. Firmware updates can improve performance, add features, or fix bugs.
- **Flow Classification Rules**: QoS rules that identify, and group specific types of network traffic (flows) based on criteria like protocol, IP address, port number, or MAC address, for the purpose of applying QoS policies.
- **GE Ports (Gigabit Ethernet Ports)**: Ethernet ports capable of supporting data transfer speeds of up to 1000 Megabits per second (Mbps), commonly used for wired LAN connections.
- **GPON (Gigabit Passive Optical Network)**: A fiber-optic access network technology that uses passive optical splitters to deliver high-speed broadband services over a single optical fiber.
- **Home Gateway Unit (HGU)**: A device that serves as a central point for network connectivity in a home, typically combining functions of a modem, router, and Wi-Fi access point.
- **ICMP (Internet Control Message Protocol)**: A network layer protocol used by network devices to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.
- **ICMPv6 (Internet Control Message Protocol version 6)**: The version of ICMP used for IPv6 networks.
- **IGMP (Internet Group Management Protocol)**: A communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.
- **IP (Internet Protocol)**: The fundamental protocol for communicating data across a network, defining how data packets are addressed and routed.
- **IPoE (IP over Ethernet)**: An internet connection type where IP addresses are obtained directly over an Ethernet connection, either automatically via DHCP or through static IP configuration.
- **IPv4 (Internet Protocol version 4)**: The fourth version of the Internet Protocol, still widely used for addressing and routing network traffic.
- **IPv6 (Internet Protocol version 6)**: The latest version of the Internet Protocol, designed to replace IPv4 due to address exhaustion and offer improvements like larger address space and enhanced security.

- **ISP (Internet Service Provider)**: A company that provides individuals and organizations access to the Internet.
- **LAN (Local Area Network)**: A computer network that interconnects computers within a limited area, such as a residence, school, or office building.
- **LED (Light Emitting Diode)**: Electronic light indicators on the device's front panel that show its operational status.
- **LOS LED**: An LED indicator that signals a Loss of Signal, specifically indicating that the optical signal from the GPON network is not detected.
- **MAC Address (Media Access Control Address)**: A unique identifier assigned to network interfaces for communications within a network segment. Used in MAC Filtering for device access control.
- **MTU (Maximum Transmission Unit)**: The largest size packet or frame that can be sent in a network.
- **Multicast VLAN**: A VLAN specifically configured for efficient delivery of multicast traffic.
- **NAPT (Network Address Port Translation)**: A form of NAT (Network Address Translation) that allows multiple devices on a private network to share a single public IP address by using different port numbers.
- **ONT (Optical Network Terminal)**: A device used in fiber-optic networks that terminates the optical fiber in a subscriber's premises. The term "Modem/ONT" in the diagram refers to this.
- **PIN Method**: A method of Wi-Fi Protected Setup (WPS) where a Personal Identification Number (PIN) is exchanged between the wireless client and the router to establish a secure connection.
- **Ping Utility**: A network utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.
- **PON LED**: An LED indicator that shows the status of the Passive Optical Network connection. "ON" typically means the optical signal is synchronized.
- **Port Filtering**: A security feature that allows you to block or permit network traffic based on specific port numbers and IP addresses, controlling inbound (downstream) and outbound (upstream) connections.
- **PPPoE (Point-to-Point Protocol over Ethernet)**: A network protocol used for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It's commonly used to provide authentication and connection management for broadband internet connections.

- **Priority Tagging**: The process of re-marking network packets with QoS priority markers (802.1p, DSCP, TC) to influence how traffic is prioritized.
- **Protocol**: A set of rules governing the exchange of information between two or more entities.
- **Push Button Method**: A method of Wi-Fi Protected Setup (WPS) where a physical button is pressed on both the router and the wireless client to establish a secure connection.
- **QoS (Quality of Service)**: A set of technologies and mechanisms that manage network traffic to reduce packet loss, latency, and jitter on the network, ensuring predictable throughput for critical data.
- **RADIUS (Remote Authentication Dial-In User Service)**: A networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect to a network service. Used in WPA/WPA2 Enterprise security.
- **RJ-45**: A standard type of connector for Ethernet cables.
- **RTP (Real-time Transport Protocol)**: A network protocol for delivering audio and video over IP networks, commonly used in VoIP and video streaming applications.
- **SC/APC (B+) GPON WAN Port**: The specific type of fiber optic connector and port used for connecting to a GPON (Gigabit Passive Optical Network) Wide Area Network.
- **Speed Limit Configuration**: A QoS feature that allows you to set maximum bandwidth limits for specific LAN ports, VLANs, or IP segments, for both uplink and downlink traffic.
- **SSID (Service Set Identifier)**: The name of a Wi-Fi network that users see when scanning for available wireless networks.
- **TCP (Transmission Control Protocol)**: A core protocol of the Internet Protocol Suite that provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network.
- **TC (Traffic Class)**: A field in the IPv6 header that serves a similar purpose to DSCP in IPv4, used for QoS classification in IPv6 networks.
- **TR069**: A technical specification that defines a mechanism for auto-configuration of a CPE (Customer-Premises Equipment) and other CPE management functions.
- **UDP (User Datagram Protocol)**: A connectionless protocol of the Internet Protocol Suite that provides a simple and fast way for applications to send data, commonly used for real-time services like VoIP and video streaming.

- **Uplink QoS Configuration**: QoS settings specifically for outgoing (uplink) network traffic, allowing prioritization and bandwidth management from your local network to the internet.
- **VLAN (Virtual Local Area Network)**: A logical grouping of network devices that allows them to communicate as if they were on the same physical LAN, even if they are connected to different network switches.
- **VOIP (Voice over IP)**: A technology that allows you to make voice calls using a broadband Internet connection instead of a traditional phone line.
- **WAN (Wide Area Network)**: A telecommunications network that extends over a large geographical area, primarily referring to the Internet connection from your ISP.
- **Web Configuration Interface**: A browser-based interface that allows users to access and manage the device's settings and functions.
- **WEP (Wired Equivalent Privacy)**: An older and less secure security protocol for Wi-Fi networks.
- **Whitelist**: In MAC filtering or port filtering, a list of MAC addresses or rules that are explicitly **allowed** to access the network or pass traffic; all other traffic is denied.
- **Wi-Fi 6 (802.11ax)**: The latest generation of Wi-Fi technology, designed to improve speed, efficiency, and performance in congested environments compared to previous standards.
- **WPA/WPA2 Personal (Pre-Shared Key)**: Wi-Fi Protected Access security protocols that use a pre-shared key (PSK) for authentication, commonly used in home networks.
- **WPA/WPA2 Enterprise (RADIUS)**: Wi-Fi Protected Access security protocols that use an external RADIUS server for authentication, typically used in larger enterprise networks.
- **WPA3 (Wi-Fi Protected Access 3)**: The newest and most secure Wi-Fi security protocol, offering enhanced encryption and authentication.
- **WLAN (Wireless Local Area Network)**: Another term for Wi-Fi, referring to the wireless networking functionality of the device.
- **WPS (Wi-Fi Protected Setup)**: A network security standard that attempts to create an easier and more secure wireless home network.