Grandstream Networks, Inc.

GWN Series Dual-Band Wi-Fi 6 Routers

GWN7062E(T) - User Manual

The **GWN7062E** and **GWN7062ET** are high-performance, secure dual-band routers powered by Wi-Fi 6 (802.11ax) technology, designed for small offices, home offices, shops, and remote workers. Both routers provide 2.4G 2×2:2 and 5G 3×3:2 MU-MIMO with beamforming and XTRA Range technology, ensuring maximum network throughput, expanded Wi-Fi coverage, and support for wireless Mesh networking. Equipped with a 1.3GHz dual-core processor, they deliver Wi-Fi speeds up to 3Gbps and support up to 256 wireless devices, enabling smooth 4K Ultra HD streaming, web meetings, video conferencing, online gaming, and smart home/office automation. For secure connectivity, they feature built-in VPN support, allowing remote employees to safely connect to corporate networks, and enterprise-grade security with unique security certificates and random default passwords for Wi-Fi and VPN protection. Both routers also support Deep Packet Inspection (DPI) for application identification and traffic statistics, along with firewall features like URL filtering to block insecure or inappropriate content. While both models share these advanced features, the GWN7062ET includes 2 FXS ports for VoIP telephony, making it ideal for small businesses requiring voice services. Both routers offer easy installation and management through a built-in web user interface, GDMS Networking, and GWN Manager for cloud and on-premise network control, with the GWN7062ET also supporting the GWN APP. By combining high-speed Wi-Fi, Mesh networking, VPN, intelligent QoS, and enhanced security, these routers provide a powerful and scalable solution for growing home and business networks.

Changes or modifications to these products not expressly approved by Grandstream, or operation of these products in any way other than as detailed by this User Manual, could void your manufacturer warranty.

Please do not use a different power adaptor with the GWN70xx routers as it may cause damage to the products and void the manufacturer warranty.

PRODUCT OVERVIEW

Technical Specifications

	GWN7062E	GWN7062ET
Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac/**ax**	
Antennas	**1x 5GHz:** maximum gain 3.4dBi **2x 2.4GHz & 5GHz:** maximum gain 4.7dBi for 2.4GHz, 4.3dBi for 5GHz	
Wi-Fi Data Rates	**5G:** IEEE 802.11ax: 7.3 Mbps to 2402 Mbps IEEE 802.11ac: 6.5 Mbps to 1732 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **2.4G:** IEEE 802.11ax: 7.3 Mbps to 573.5 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network.*	
Frequency Bands	● **2.4GHz radio:** 2412-2483.5MHz ● **5GHz radio:** 5150-5895MHz **Not all frequency bands can be used in all regions*	
Channel Bandwidth	HT 20/40, VHT 20/40/80, HE 20/40/80/160	
MU-MIMO	● 2×2:2 **2.4GHz** ● 3×3:2 **5GHz**	

Maximum TX Power	● **2.4G**: 23dBm ● **5G**: 24dBm **Maximum power varies by country, frequency band and MCS rate*	
Receiver Sensitivity	**2.4G** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm@6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm@MCS7; 802.11n 40MHz: -70dBm@MCS7; 802.11ax 20MHz: -60dBm@MCS11; 802.11ax 40MHz: -58dBm@MCS11; **5G** 802.11a: -92dBm@6Mbps, -74dBm@54Mbps; 802.11n 20MHz: -73dBm@MCS7; 802.11n 40MHz: -70dBm@MCS7; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac 40MHz: -63dBm@MCS9; 802.11ac 80MHz: -59dBm@MCS9; 802.11ax 20MHz: -60dBm@MCS11; 802.11ax 40MHz: -58dBm@MCS11; 802.11ax 80MHz: -56dBm@MCS11; 802.11ax 160MHz: -52dBm@MCS11;	
SSIDs	4 SSIDs total	
Concurrent Wireless Clients	Up to 256 concurrent clients	
Networking Interfaces	3x autosensing 10/100/1000Mbps Ethernet ports	
Analog Telephone FXS Ports	-	**2x** RJ11 FXS **All ports have lifeline capability in case of power outage; number of ports can be expanded by peering with an FXS gateway*
Auxiliary Ports	● 1x RESET Pinhole ● 1x SYNC	● 1x USB 3.0 ● 1x RESET Pinhole ● 1x SYNC
Mounting	● Desktop ● Wall-mount	
LED	1x tri-color LED for device tracking and status indication.	
Network Protocols	IPv4, IPv6, 802.1p, 802.11e/WMM, DSCP	
Security	● Wi-Fi encrypted types including WPA/WPA2, WPA2, WPA2/WPA3, WPA3 ● Application monitoring and traffic statistics with DPI ● Security firewall including DoS, blocklist and URL content filtering ● Anti-hack secure boot and critical data/control lockdown via digital signatures ● Unique security certificate and random default password per device	
QoS	● Support 8 queues with multiple traffic priority and bandwidth ● APP QoS ● QoS rules	
NAT	DDNS, Port Forwarding, DMZ, UPnP	
Firewall	DPI, DDNS, Port Forwarding, DMZ, UPnP, DoS	
VPN	Only support 1 VPN tunnel:	

	● L2TP Client ● PPTP Client ● IPSec Site-to-Site & Client-to-Site ● OpenVPN® Server ● WireGuard® Site-to-Site & Peer-to-Site	
Network Management	● Embedded controller ● GDMS (Networking) offers a free cloud management platform for unlimited GWN Routers ● GWN Manager offers premise-based software controller ● TR-069	
Power & Green Energy Efficiency	USB Type-C power adapter included: Input: 100~240V 50/60Hz Output: 5V/3A(15W)	Universal power adapter included: Input: 100~240V 50/60Hz Output: 12V/1.5A(18W)
Environmental	Operation: 0°Cto 40°C, humidity: 10% to 90% RH(Non-condensing) Storage: -20°C to 60°C, humidity: 10% to 90% RH(Non-condensing)	
Dimensions	140mm(L)*46mm(W)*90 mm(H)	Unit Dimensions: 160mm(L)*50mm(W)*98mm(H) Entire Package Dimensions: 187mm(L)*193mm(W)*76mm(H)
Package Content	● GWN7062E(T) Router ● Universal Power Supply ● Network Cable ● Quick Installation Guide	
Compliance	FCC, CE, RCM, IC	

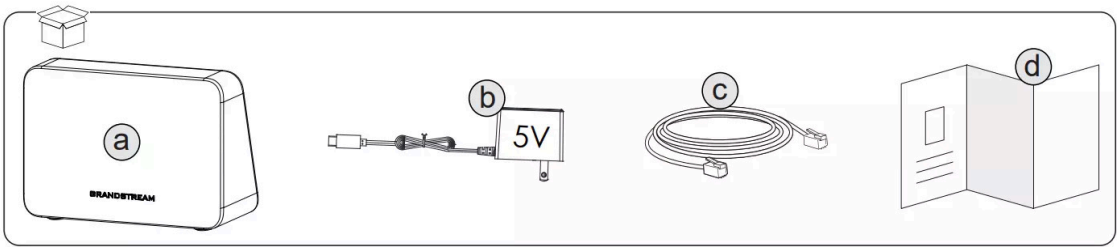
GWN7062E(T) Technical Specifications

INSTALLATION

Before deploying and configuring the GWN7062E(T) router, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN7062E(T) router.

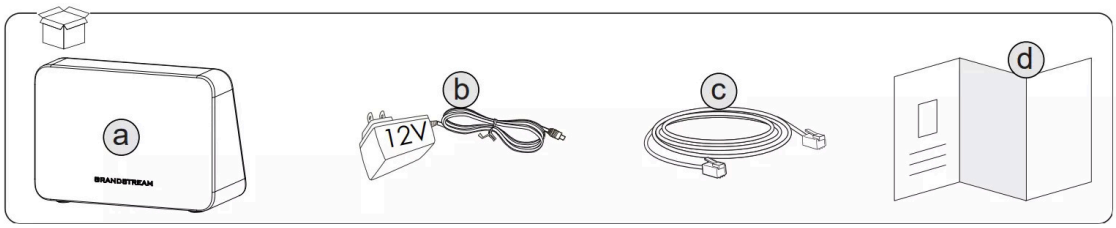
Package Contents

○ **GWN7062E**



GWN7062E Package Contents

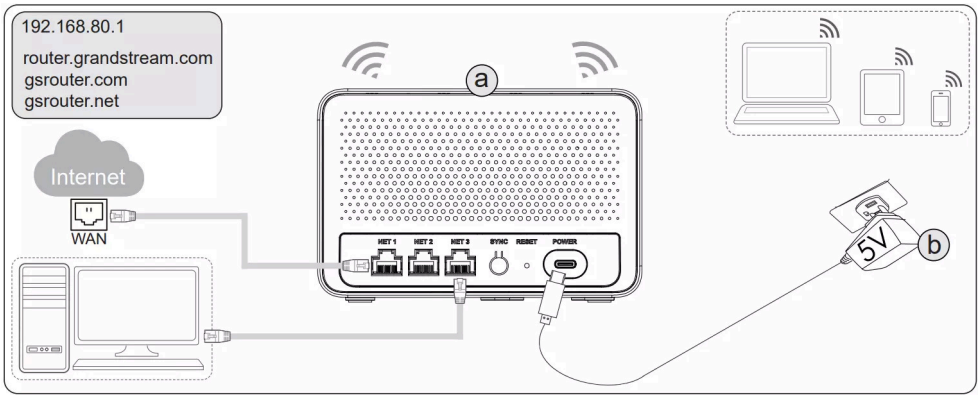
○ **GWN7062ET**



GWN7062ET Package Contents

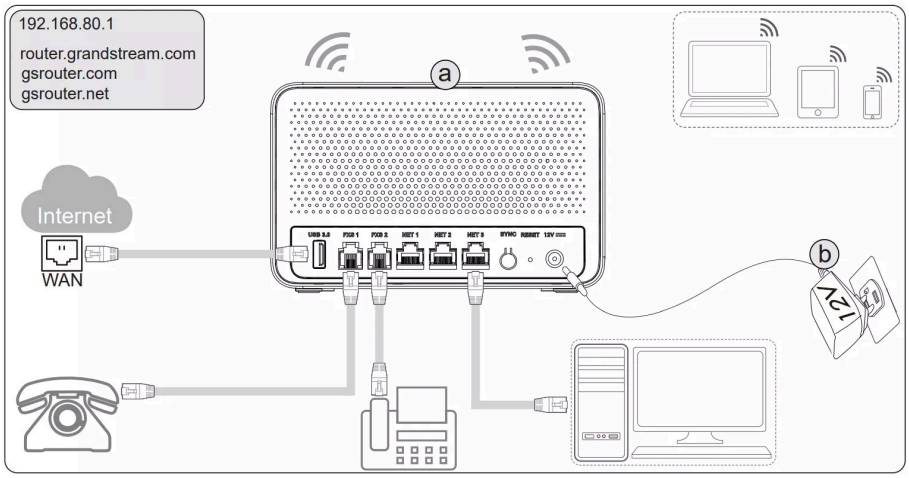
Powering and Connecting

○ **GWN7062E**



GWN7062E Ports

○ **GWN7062ET**



GWN7062ET Ports

SSID's default password information is printed on the MAC tag of the unit.

Safety Compliances

The Dual-Band Wi-Fi Router complies with FCC/CE and various safety standards. The device power adapter is compliant with the UL standard. Use the universal power adapter provided with the device package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If the device Dual-Band Wi-Fi Router was purchased from a reseller, please contact the company where the device was purchased for replacement, repair or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy the warranty policy without prior notification.

GETTING STARTED

The routers provide an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options.

This section provides step-by-step instructions on how to read LED indicators and use the Web GUI interface.

LED Indicators

The GWN7062E(T) router has a single multi-color LED indicator to display its operational status. The following table provides a detailed breakdown of the LED statuses and their meanings:

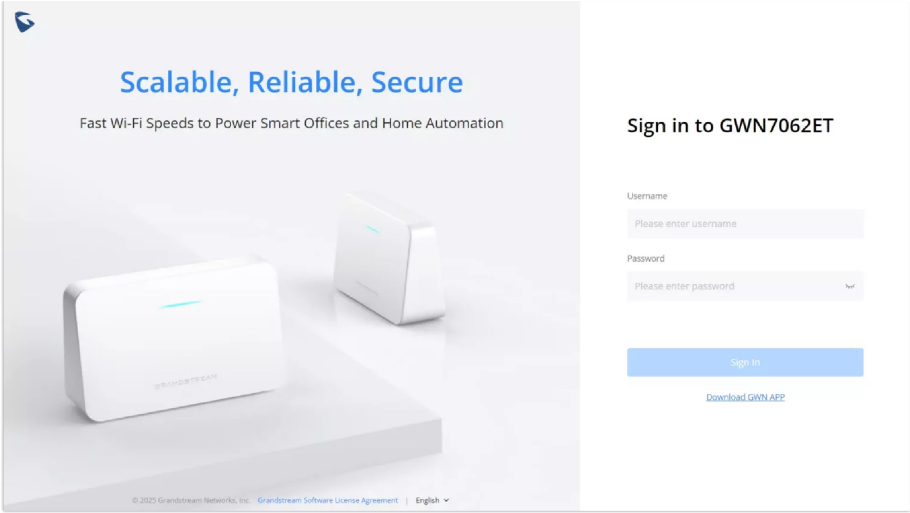
LED Status	Indication
Off	The router is powered off.
Solid Blue	● Internet is connected. ● Normal operation. ● Mesh network successfully established.
Flashing Blue	● Configuration is being applied. ● Restoring configuration.
Flashing Pink	● Searching for new Mesh node routers. ● Primary Mesh router is adding node routers (flickering frequency increases when adding).
Solid Pink	● No web login detected after reset. ● Mesh router pairing in progress.
Flashing Green	Firmware upgrade in progress.
Solid Green	● Device booting up. ● Rebooting.
Flashing Red	● Factory reset in progress. ● Device is locked.
Solid Red	● Firmware upgrade failed. ● Mesh pairing failed.
Solid Yellow	Mesh node router is disconnected from the primary router.
Flashing Yellow	No Internet connection.

LED Indicators

Use the WEB GUI

Access WEB GUI

The routers embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, or Google Chrome.



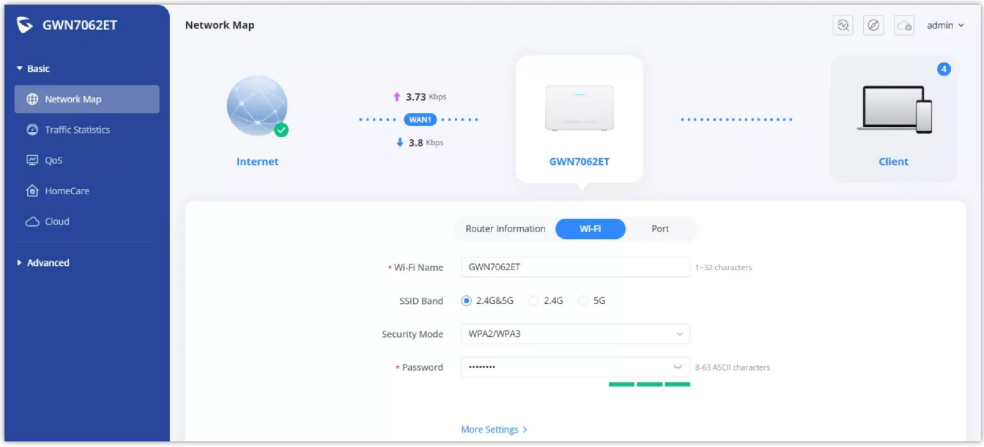
Web GUI Login Page

To access the Web GUI:

1. Connect a computer to a LAN port of the router.
2. Ensure the device is properly powered up.
3. Open a Web browser on the computer and enter the web GUI URL in the following format: https://192.168.80.1 (Default IP address).
4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username is "admin" and the default password is printed on the MAC tag of the unit.

At first boot or after factory reset, users will be asked to change the default administrator and user passwords before accessing the device web interface. The password field is case-sensitive with a maximum length of 32 characters. Using strong passwords including letters, digits, and special characters is recommended for security purposes.

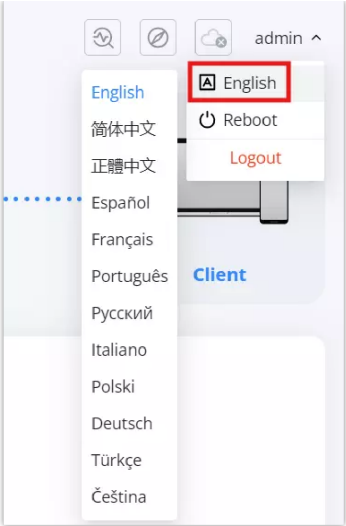
Once the user enters the password, this is the initial page that will be shown. This page contains general information and the status of the router.



WEB GUI Configuration

Web UI Language

The router web interface supports multiple languages, allowing users to navigate and configure settings in their preferred language.



Change language

Steps to Change the Language:

1. **Locate the Language Menu:**
   - In the top-right corner of the web interface, click on the **admin** dropdown menu.

2. **Select a Language:**
   - A list of available languages will appear.
   - Choose the desired language by clicking on it.

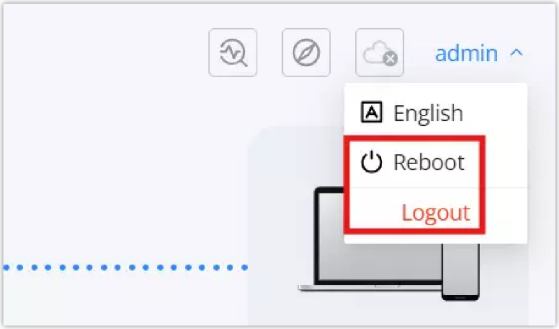
3. **Apply Changes:**
   - The interface will refresh automatically and switch to the selected language.

This setting ensures users can interact with the router's interface in their native or preferred language, improving usability and accessibility.

Rebooting or Logging Out

The **Reboot** and **Logout** options are located in the **top-right corner** of the web interface under the **admin** menu.

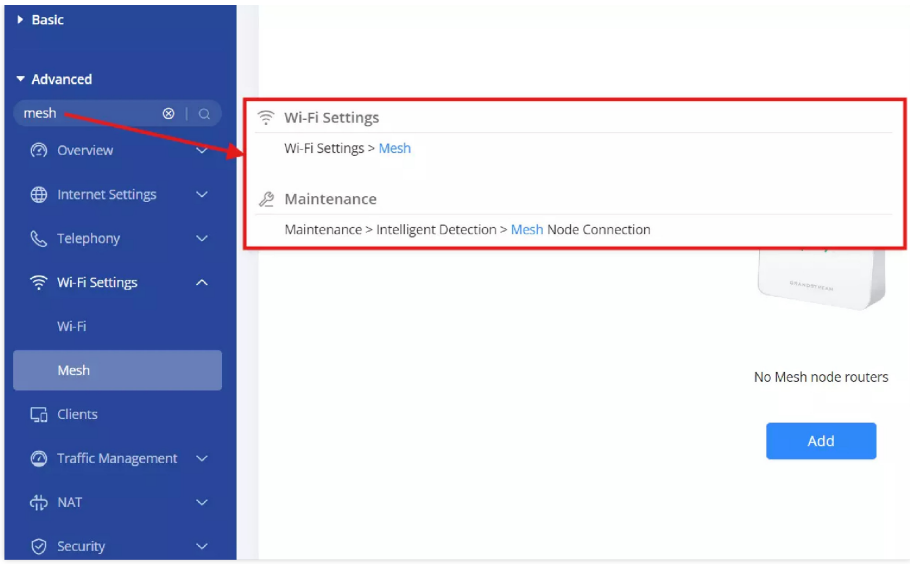
- **Reboot:** Click on **Reboot** to restart the router. This will temporarily disconnect all network connections and may take a few minutes to complete.
- **Logout:** Click on **Logout** to securely exit the web interface. You will need to log in again to access the settings.



Rebooting or Logging Out

Search

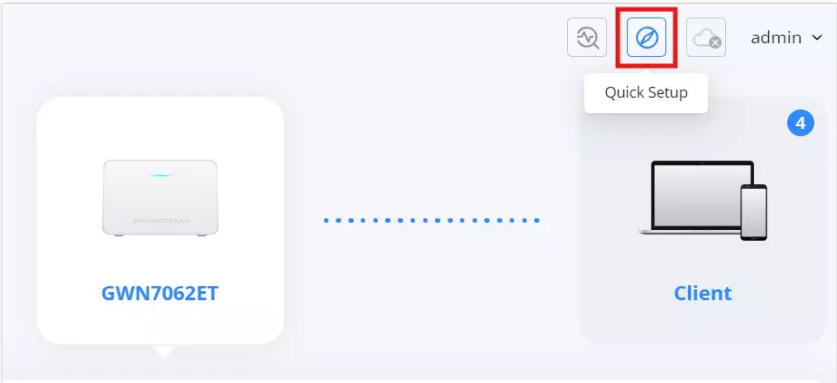
To make it easier for the user to find a particular option quickly, the device web UI has a search feature. Users can access this feature by clicking on the search bar at the top of the left-hand menu under Advanced and typing the desired option name.



Search

Quick setup

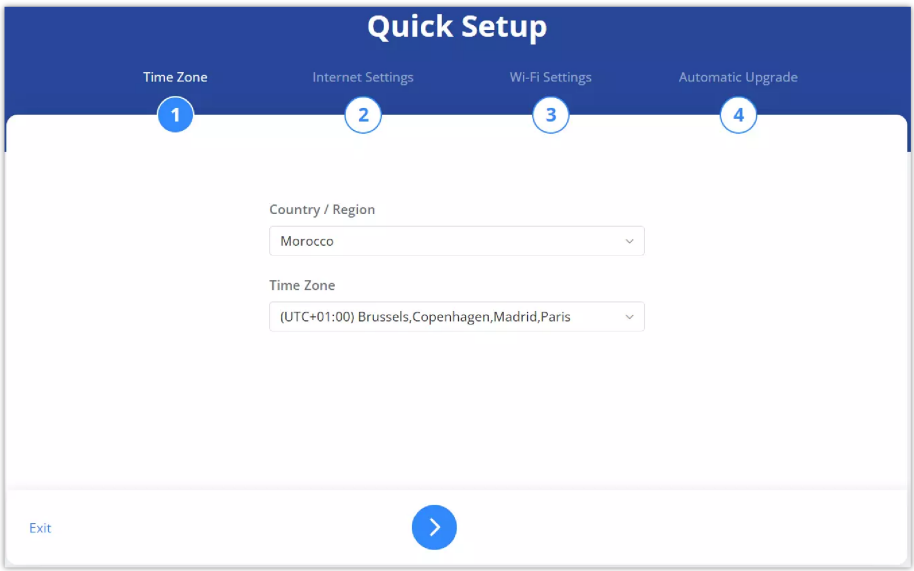
If the user missed the Setup Wizard at the first boot of device. It's accessible all the time at the top of the page and it contains the necessary settings that the user must configure in 4 steps.



Quick Setup

1. Time Zone

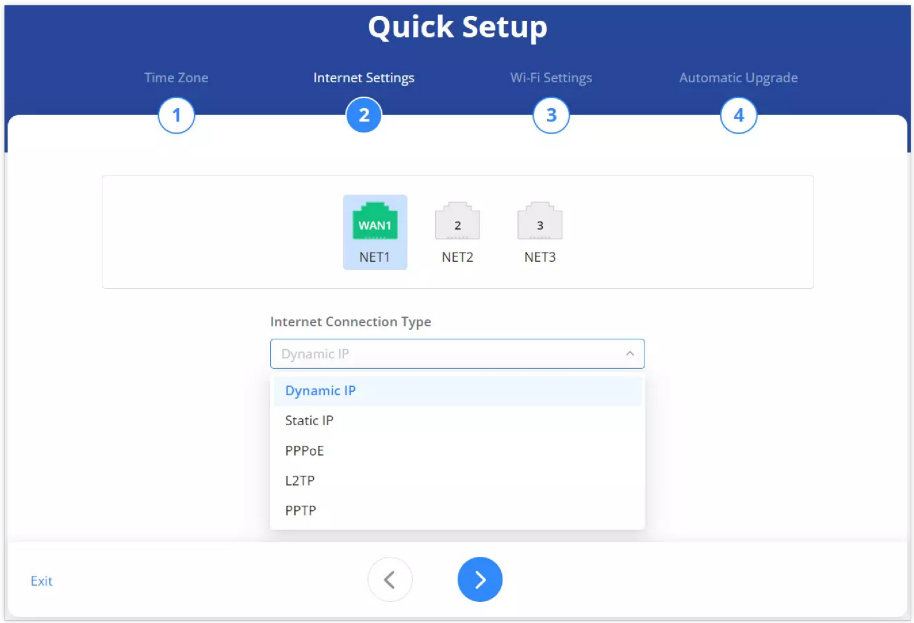
In this step, the user configures the time settings for the device. The **Country/Region** should be selected from the dropdown menu to ensure accurate localization. The **Time Zone** will be set automatically based on the selected region, but the user can adjust it manually if needed. Once the appropriate settings are selected, the user should click the **Next** button (blue arrow) to proceed to the next step.



Quick Setup – Time Zone

2. Internet Settings

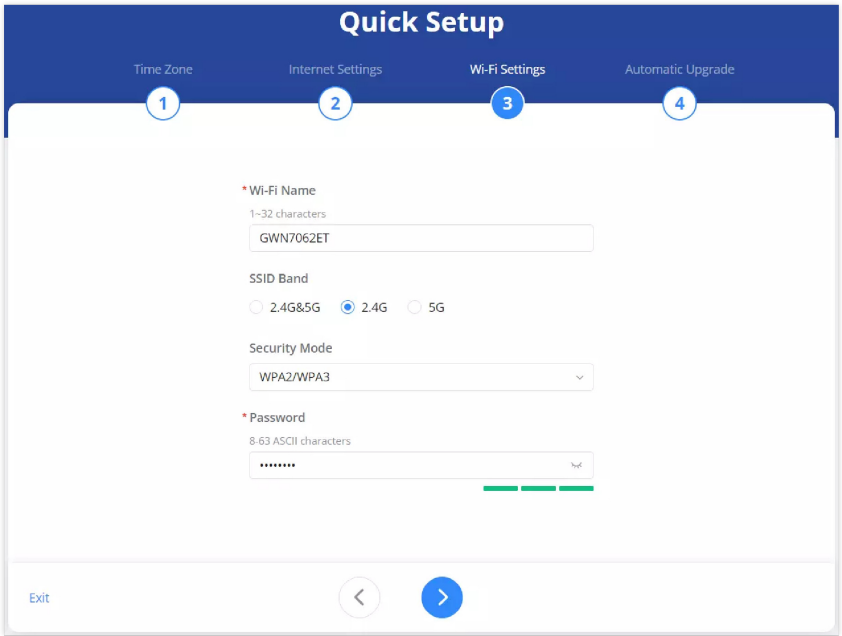
In this step, the user selects the appropriate **Internet Connection Type** to establish network connectivity. The available options include **Dynamic IP, Static IP, PPPoE, L2TP,** and **PPTP**. The selection should be based on the user's internet service provider (ISP) requirements. If unsure, the user should consult their ISP for the correct settings. Once the connection type is chosen, the user should click the **Next** button (blue arrow) to proceed to the next step.



Quick Setup – Internet Settings

3. Wi-Fi Settings

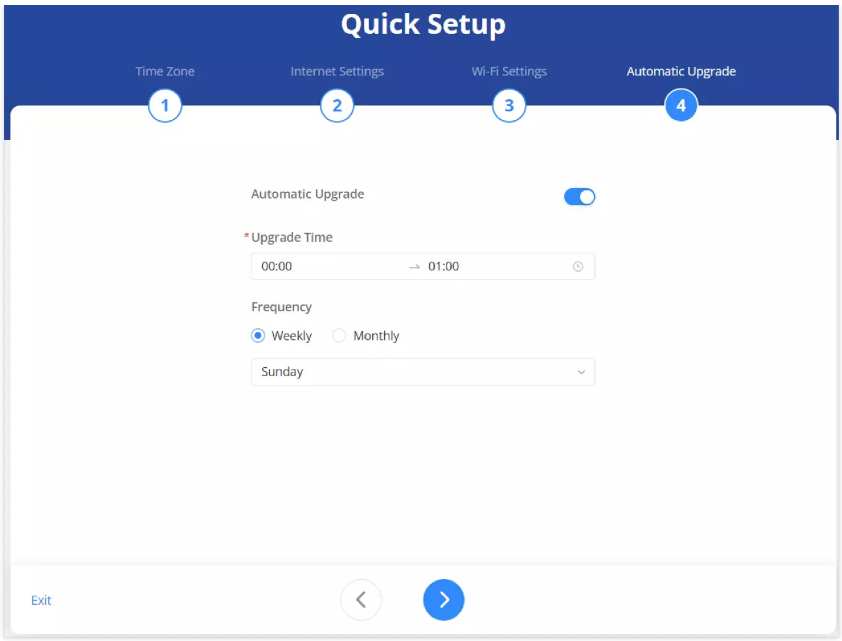
In this step, the user sets up the **Wi-Fi network** by specifying a **Wi-Fi Name (SSID)** within the allowed character range. The user selects the **SSID Band**, choosing between **2.4G & 5G, 2.4G,** or **5G**, depending on the desired frequency. The **Security Mode** should be set to ensure a secure connection, with options such as **WPA2/WPA3** available. A strong **Wi-Fi password** (8-63 ASCII characters) must be entered to protect the network. Once the settings are configured, the user should click the **Next** button (blue arrow) to proceed.



Quick Setup – Wi-Fi Settings

4. Automatic Upgrade

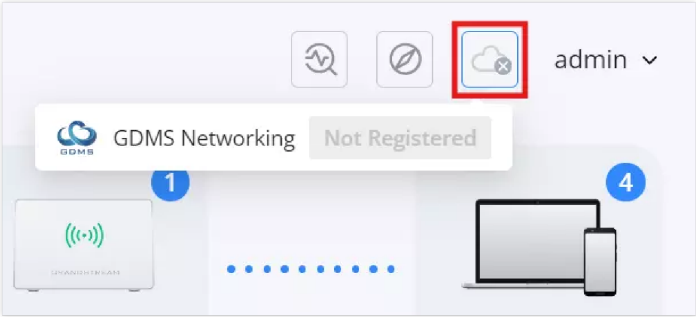
In this step, the user sets up the **Automatic Upgrade** feature to ensure the device stays updated with the latest firmware. The user can enable or disable automatic upgrades using the toggle switch. If enabled, the **Upgrade Time** must be specified within a chosen time range. The user also selects the **Frequency** of updates, either **Weekly** or **Monthly**, and specifies the preferred day for the upgrade. Once the settings are configured, the user should click the **Next** button (blue arrow) to complete the setup.



Quick Setup – Automatic Upgrade

GDMS Networking – Cloud Management

GDMS (Grandstream Device Management System) Networking allows users to register and manage the router remotely via the cloud. Once registered, the router can be monitored and configured from anywhere, providing enhanced flexibility and centralized control.



GDMS Networking – Cloud Management

Benefits of GDMS Networking:

- **Remote Management:** Configure and monitor the router from anywhere.
- **Multi-Device Control:** Manage multiple routers under one platform.
- **Firmware Updates:** Apply updates remotely for enhanced security and performance.
- **Real-Time Monitoring:** Track network status, connected devices, and traffic analytics.

For more details, visit: GDMS Networking – User Guide

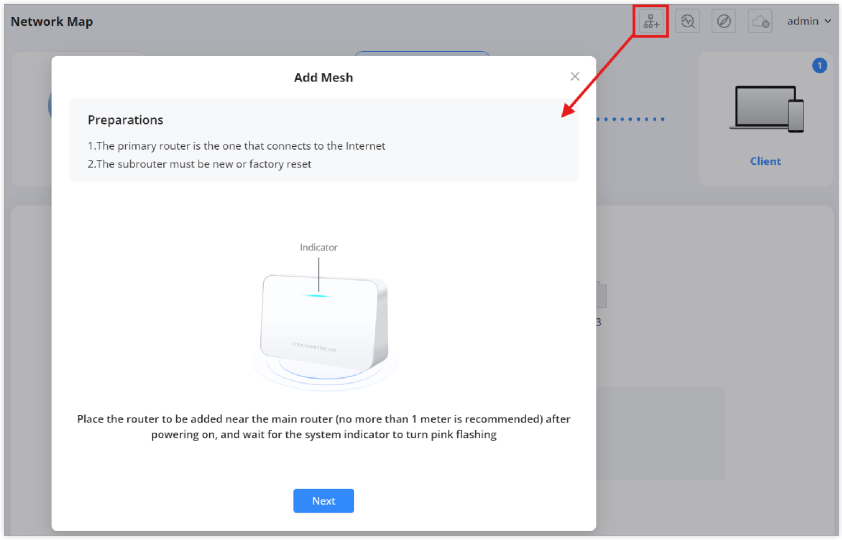
Mesh Network Shortcut

A **Mesh Network shortcut** is available in the **top-right corner** of the **Network Map** page, allowing users to quickly add a new router to their existing **Mesh Network**. This shortcut is always visible, providing easy access to initiate the **Mesh pairing process**.

Mesh Network Shortcut

How to Use the Mesh Shortcut:

1. Click on the **"Add New Router"** shortcut (highlighted icon in the top-right corner).
2. A setup window will appear, guiding you through the **Mesh Network pairing process**.
3. Ensure the following conditions are met before proceeding:
   - The **primary router** is already connected to the internet.
   - The **sub-router** is either **new** or has been **factory reset**.
   - The **sub-router** is placed **close to the primary router** (recommended distance: **1 meter or less**).
   - Wait for the **system indicator to flash pink**, signaling it is ready for pairing.



Mesh Network Shortcut – Add New Router

For **detailed configuration instructions**, refer to the **Mesh Section**.

BASIC

Basic mode is designed for users who need quick access to essential networking features without the complexity of advanced configurations. This mode includes:

- **Network Map:** A visual representation of the network, displaying the router's connection status, internet speed, and connected clients.
- **Traffic Statistics:** Real-time data on network traffic, helping users monitor bandwidth usage.
- **QoS (Quality of Service):** Basic settings for prioritizing network traffic to enhance performance for specific applications.
- **HomeCare:** A suite of features that may include parental controls and security protections.
- **Cloud Management:** Integration with Grandstream's cloud services for simplified remote management.

This mode is ideal for **home users, small businesses, and non-technical users** who need a functional network without deep customization.

Network Map

The **Network Map** page provides a comprehensive overview of the router's current status, network connections, and active clients. It dynamically updates based on user interaction, displaying relevant details about the router, connected devices, and network settings.

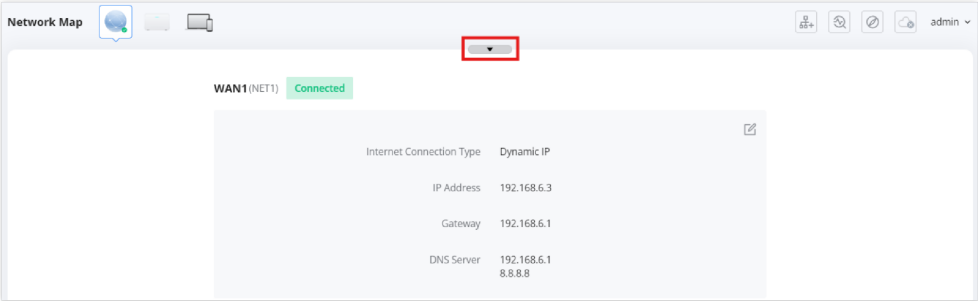
To navigate to the **Network Map**:

1. Log in to the **Web UI** of the router.
2. In the left menu, click on **Basic > Network Map**.

This page displays an **overview of the router's network topology**, including Internet connection, primary router status, Mesh Nodes and connected clients.

Collapsible Network Map:

The **Network Map** includes a **collapsible panel feature**, allowing users to expand or collapse detailed network information for a cleaner and more efficient interface.



Collapsible Network Map

How to Use the Collapse/Expand Feature:

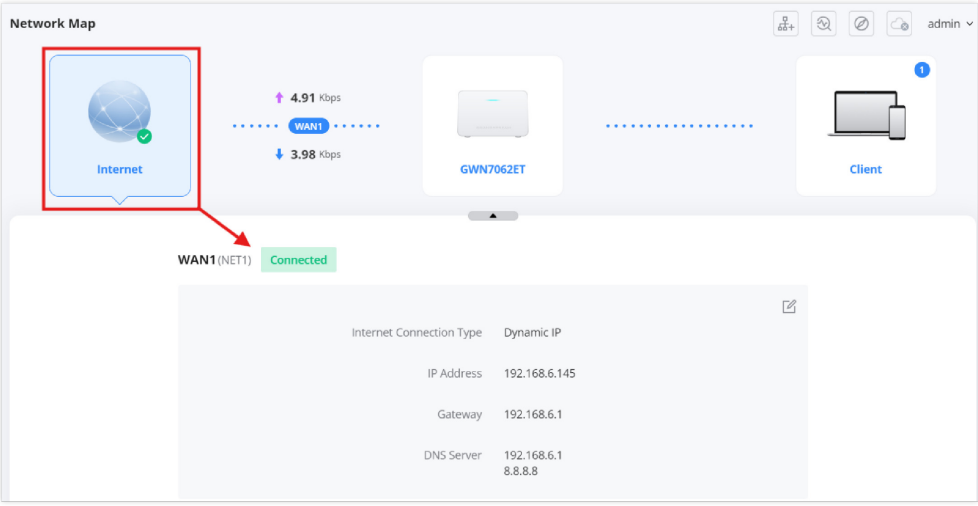
1. **Expand View**:
   - By default, the **Network Map** displays a **visual representation** of the router's connections, including **Internet, primary router, and clients**.
   - The detailed **WAN connection information** is visible below.
2. **Collapse View**:
   - Clicking the **collapse arrow** (▲) at the top of the **WAN details panel** will hide the **connection details**, keeping only the high-level network visualization.
3. **Expand Again**:
   - Clicking the **expand arrow** (▼) will restore the full view of **WAN details**, including **IP address, connection type, gateway, and DNS information**.

This feature helps users **toggle between a detailed and simplified view**, making network monitoring more **user-friendly and space-efficient**.

Internet Connection Details

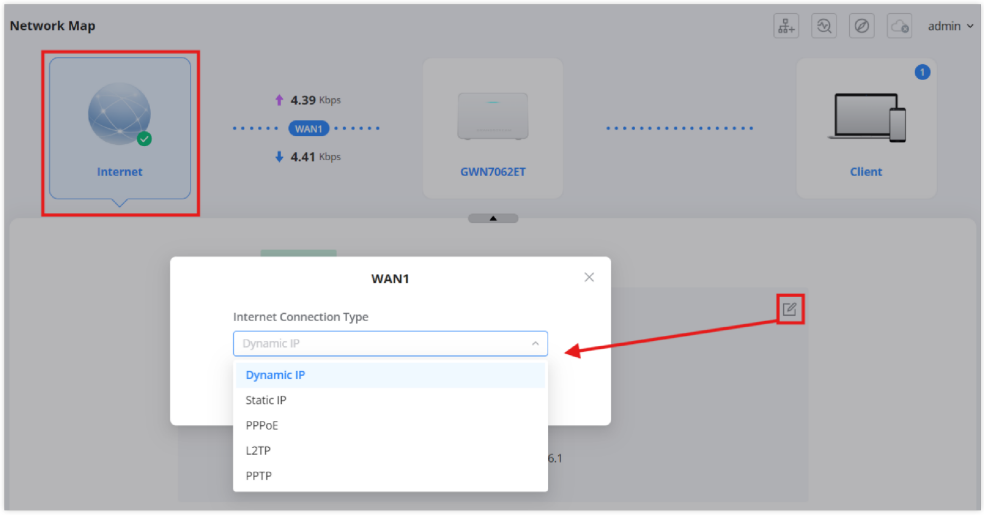
Clicking on the **Internet** icon provides a **detailed view of the WAN connection status**:

- **Internet Connection Type** (e.g., Dynamic IP, Static IP, PPPoE, L2TP, PPTP).
- **IP Address** assigned by the ISP or another Router.
- **Gateway** and **DNS Server** information.



Network Map – Internet

To **edit the WAN settings**, click on the **edit icon** next to the Internet details. A pop-up window will allow selecting the connection type and configuring necessary parameters.



Network Map – Internet – Edit WAN

Internet Connection Types:

When configuring the **WAN (Internet) connection type**, users can select from the following options:

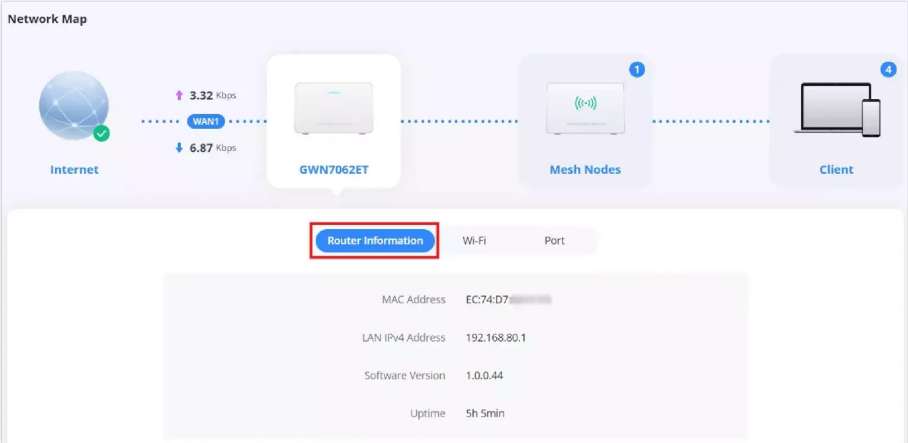
- **Dynamic IP** – The router automatically obtains an IP address from the ISP. This is the most common setting for residential and many business connections.
- **Static IP** – Requires manual entry of an IP address, subnet mask, gateway, and DNS servers. Used for fixed-address internet connections.
- **PPPoE (Point-to-Point Protocol over Ethernet)** – Used for DSL connections where the ISP provides a username and password for authentication.
- **L2TP (Layer 2 Tunneling Protocol)** – A VPN-based internet connection method that requires an L2TP server address, username, and password.
- **PPTP (Point-to-Point Tunneling Protocol)** – An older VPN-based internet connection method, similar to L2TP but generally less secure.

Users should **select the appropriate connection type** based on their ISP's requirements.

Primary Router Information

Displays essential details about the router, including:

- **MAC Address:** The unique identifier assigned to the router.
- **LAN IPv4 Address:** The internal IP address used for local network communication.
- **Software Version:** Indicates the firmware version currently installed.
- **Uptime:** Shows how long the router has been running since the last restart.

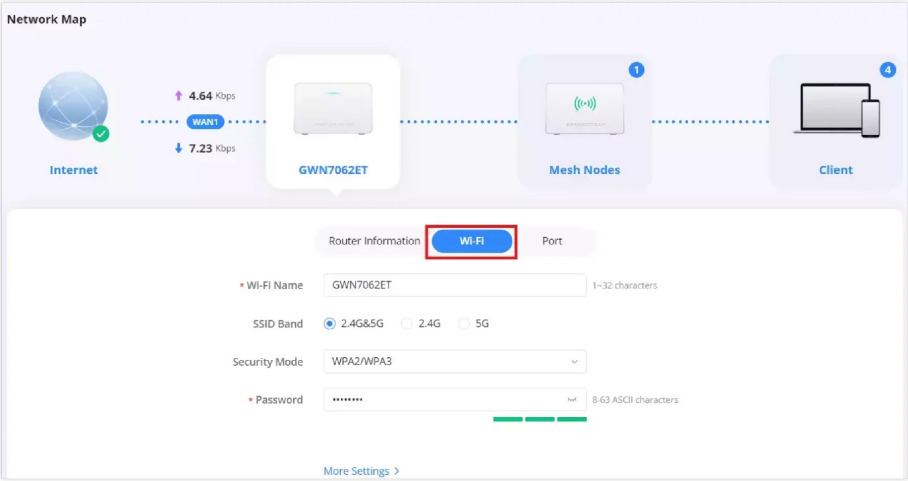


Wi-Fi Settings

Allows users to configure and manage wireless network settings:

- **Wi-Fi Name (SSID):** Set or modify the Wi-Fi network name.
- **SSID Band Selection:** Choose between:
  - **2.4GHz & 5GHz (Dual-band)**
  - **2.4GHz only**
  - **5GHz only**
- **Security Mode:** Select encryption type (e.g. WPA2/WPA3).
- **Wi-Fi Password:** Set or update the wireless password.

To add more SSIDs (Wi-Fi) or more options, click on **More Settings** link.



Network Map – Wi-Fi

Port Status

The **Port tab** in the **Network Map** provides real-time information on the **physical connection status** of each port on the router. This helps users monitor which ports are active and their connection speeds.

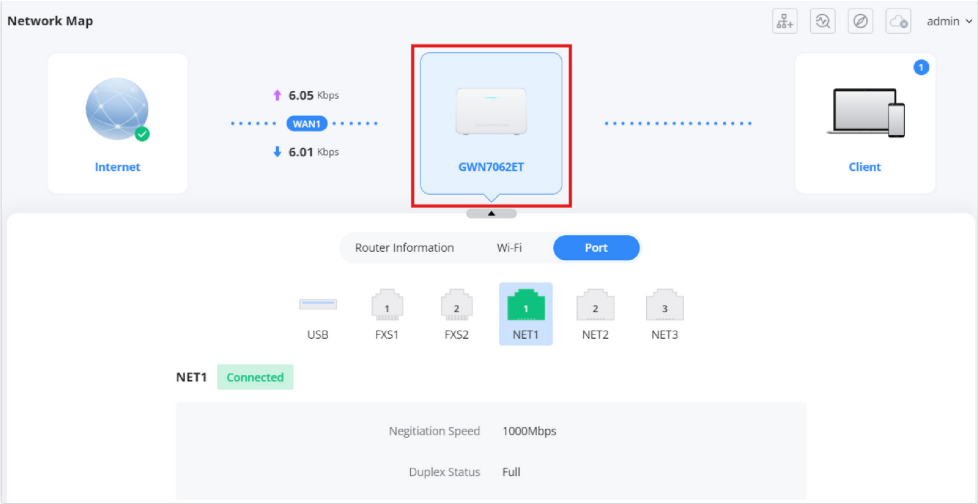
Accessing the Port Status:

1. Click on the **router icon** (e.g., **GWN7062ET**) in the **Network Map**.
2. Navigate to the **Port** tab to view detailed port information.

Port Information Displayed:

- **Connection Status** – Indicates if the port is **Connected** or **Disconnected**.
- **Negotiation Speed** – Displays the current connection speed (e.g., **1000Mbps** for Gigabit connections).
- **Duplex Status** – Shows whether the connection is **Full** or **Half Duplex**.

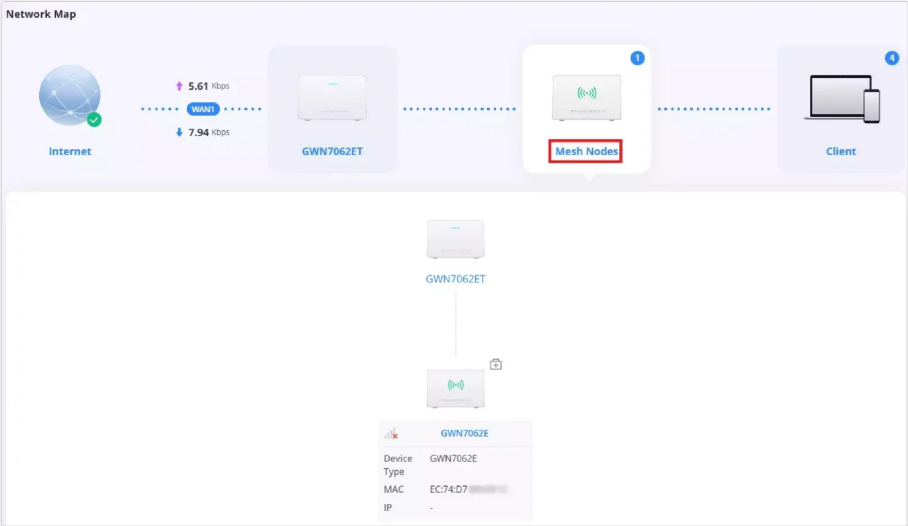
This section helps users **identify active ports, check connectivity issues, and verify speed and duplex settings**.



Network Map – Primary Router – Port

Mesh Nodes

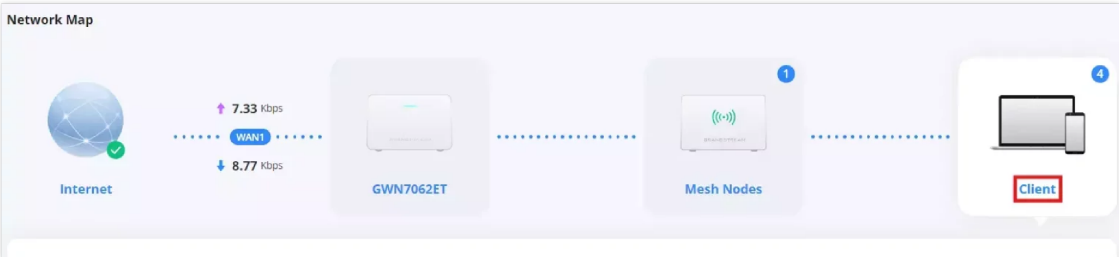
- Displays any **Mesh devices** connected to the network.
- Shows **device type, MAC address, and connection status**.



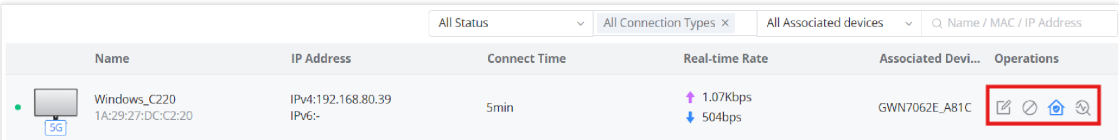
Network Map – Mesh Nodes

Client Devices

- Lists all devices connected to the router.
- Displays **connection type** (2.4GHz, 5GHz, or wired).
- Shows **IP addresses, real-time bandwidth usage, and connection time**.
- Allows **basic device management**, such as renaming, blocking, or prioritizing clients.



Network Map – Clients



Managing Connected Devices:

Users can perform various actions directly from the **Operations** column:

- **Edit (Pencil Icon)** – Modify the device name or other settings.
- **Block (Prohibited Icon)** – Restrict network access for the selected device.
- **Parental Control (House Icon)** – Add the device to the **Parental Control list** for content filtering and time-based access restrictions. For more details refer to Basic → HomeCare → Parental Control.
- **Repair (Circular Arrow Icon)** – If the device has connection issues, clicking this icon redirects the user to Intelligent Detection → Internet Failure for troubleshooting.

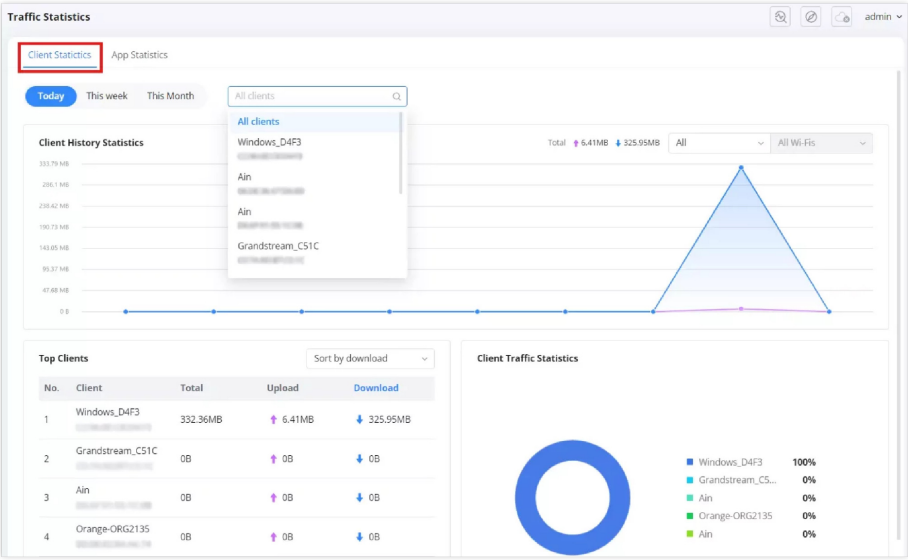
Traffic Statistics

The **Traffic Statistics** page provides real-time insights into network usage, helping users monitor data consumption and optimize bandwidth. This section is divided into two key tabs: **Client Statistics** and **App Statistics**, each offering detailed data on network activity.

Client Statistics

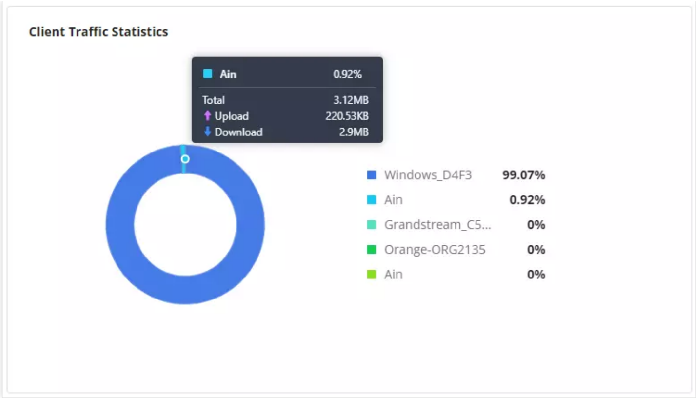
This tab displays **network usage per device**, allowing users to track bandwidth consumption for individual clients.

- **Client History Statistics:** A graphical representation of data usage over time.
- **Top Clients List:** Displays the highest bandwidth-consuming devices, showing:
  - **Device Name & MAC Address**
  - **Total Data Consumption**
  - **Upload & Download Usage**
- **Filtering & Sorting Options:** Users can filter by:
  - Specific clients
  - Time periods (**Today, This Week, This Month**)
  - Sorting methods (**Upload or Download usage**)



Traffic Statistics – Client Statistics part 1

The **Traffic Statistics** page includes interactive visual representations of network usage. Users can **hover over graphs** to view additional details about specific clients or applications.

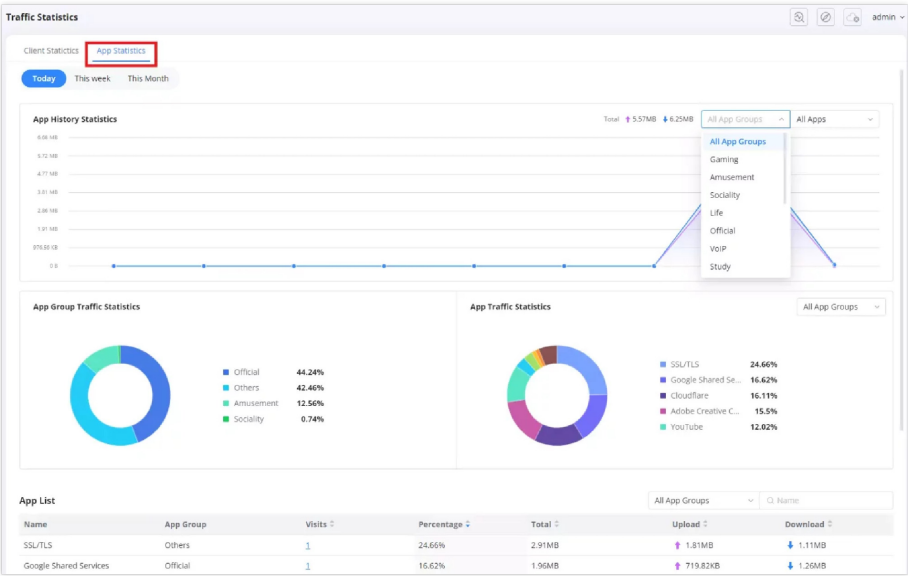


Traffic Statistics – Client Statistics part 2

App Statistics

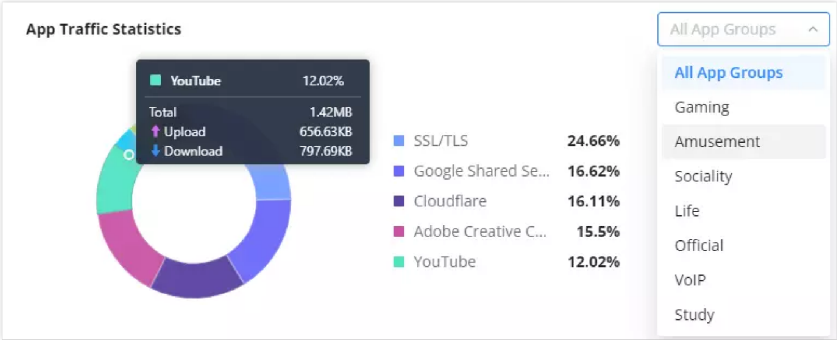
This tab provides a breakdown of network usage based on application types, enabling better traffic management and prioritization.

- **App History Statistics:** Tracks total bandwidth usage over time.
- **App Group Traffic Statistics:** Categorizes network traffic into groups such as:
  - **Gaming, VoIP, Social Media, Streaming, Official Work, and Others**
- **App List:** Displays detailed statistics for each application, including:
  - **Total Usage, Upload, Download, and Visit Count**
  - **Percentage of Total Network Traffic**
- **Filtering Options:** Users can filter by:
  - **Specific application types**
  - **Time periods (Today, This Week, This Month)**



Traffic Statistics – App Statistics part 1

It's also possible in this page too to hover over graphs for more details or more info.



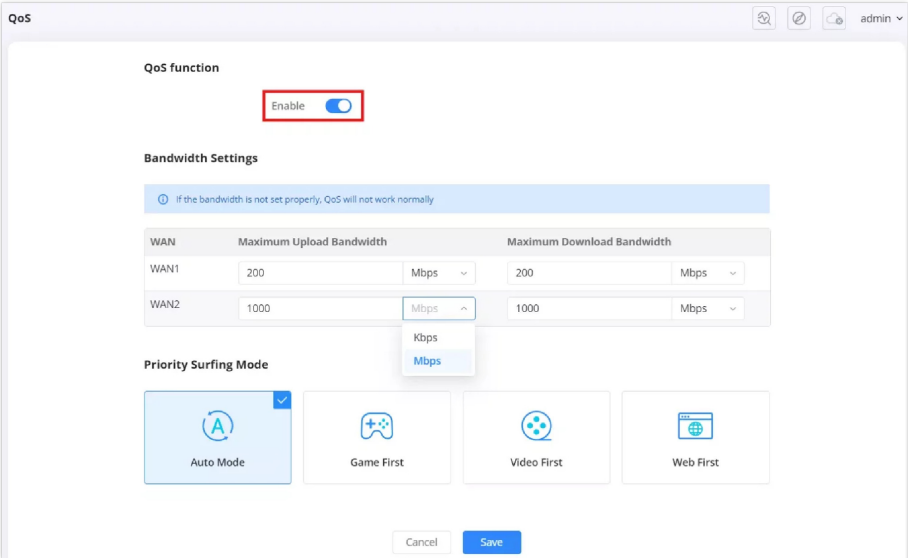
QoS (Quality of Service)

Quality of Service (QoS) is a network feature that prioritizes specific types of internet traffic to ensure optimal performance for critical applications. By enabling QoS, users can allocate bandwidth more efficiently, reducing latency for gaming, streaming, video calls, and other high-priority tasks.

Enabling QoS

To enable QoS on the router, navigate to:
Basic → QoS

- Toggle the **QoS function** switch to **Enable**.
- Ensure that bandwidth settings are properly configured for QoS to function effectively.



QoS

Bandwidth Settings

Users can manually define the **maximum upload and download bandwidth** for each **WAN port** to optimize traffic distribution.

- **WAN Selection:** Displays multiple WAN interfaces (e.g., WAN1, WAN2) to apply QoS settings separately.
- **Maximum Upload Bandwidth:** Define the highest upload speed per WAN connection (Kbps or Mbps).
- **Maximum Download Bandwidth:** Set the maximum download speed for each WAN interface.

Proper configuration of these settings ensures that **QoS operates efficiently** without network congestion.

Priority Surfing Mode

Users can select **traffic prioritization modes** based on their preferred usage:

- **Auto Mode:** The router dynamically manages bandwidth based on network activity.
- **Game First:** Prioritizes gaming traffic to reduce latency and lag.
- **Video First:** Ensures seamless streaming by prioritizing video traffic.
- **Web First:** Allocates bandwidth for smooth web browsing and productivity tasks.

📌 **Note:** After configuring QoS settings, click **Save** to apply the changes.

This feature is highly beneficial for **gamers, remote workers, streamers, and households with multiple users**, ensuring a **balanced and optimized network experience** across different applications.

HomeCare

Parental Control

The **Parental Control** feature under **Basic** → **HomeCare** allows administrators to manage and control internet access for specific devices connected to the network. This feature is particularly useful for parents, schools, or workplaces to enforce internet usage policies.

Key Features of Parental Control:

- **Time-Based Restrictions:** Set internet access schedules to restrict online usage during specific hours, such as school nights or weekends.
- **App & URL Filtering:** Block or allow certain applications or websites to ensure safe browsing.
- **Device-Specific Rules:** Apply different rules for different devices, either by selecting from connected clients or adding devices manually.
- **One-Click Network Disconnection:** Instantly disconnect or schedule internet disconnection for selected devices.
- **General Settings:** Option to block internet access for unmanaged devices that are not subject to parental control rules.

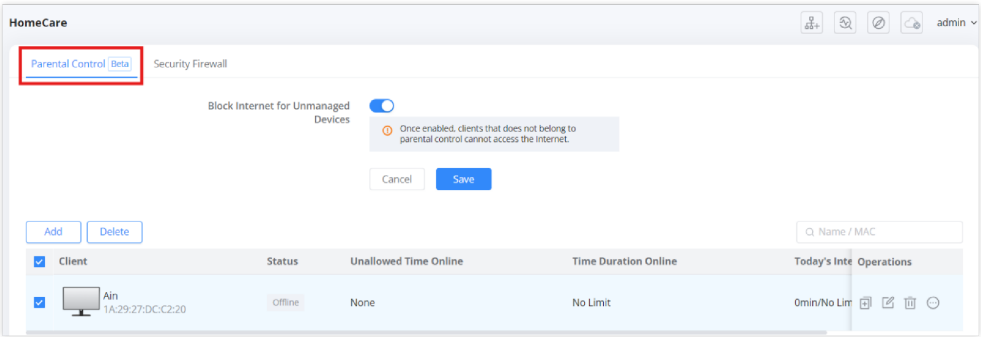
To configure **Parental Control**, navigate to **Basic** → **HomeCare** → **Parental Control** and use the available options to set restrictions, add devices, or customize browsing rules.

Parental Control

The **Parental Control** section allow administrators to define how unmanaged devices connect to the internet. This feature ensures that any device not assigned parental control rules is restricted from accessing the network, enhancing security and ensuring controlled internet usage.

To configure enable Parental Control:

1. Navigate to **Basic** → **HomeCare** → **Parental Control**.
2. Then toggle on **Block Internet for Unmanaged Devices**.



Parental Control page

> **Note:**
>
> When this setting is enabled, all unmanaged devices will be unable to access the internet unless explicitly assigned to parental control rules.

Adding a Client to Parental Control

To apply parental control rules to specific devices, users must add them to the **Parental Control** client list. This allows administrators to set time restrictions, content filters, and other network rules for selected devices.

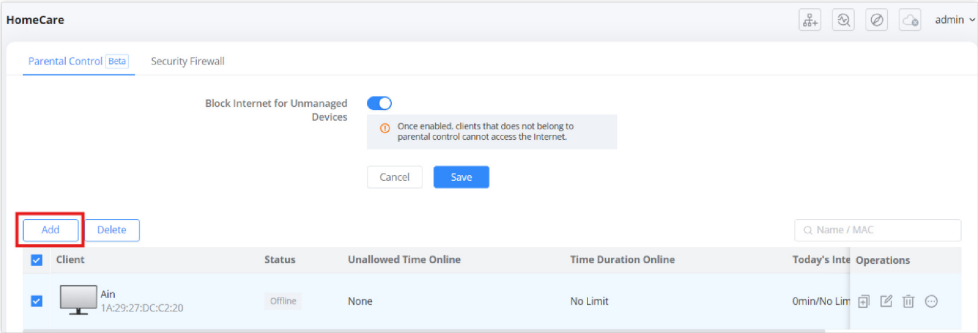
Navigating to Add a Client:

To add a device under Parental Control:

1. Navigate to **Basic** → **HomeCare** → **Parental Control**.

2. Click on the **Add** button at the top-left of the client list.

Once a client is added, administrators can configure various settings such as online time limits, app restrictions, and URL filtering.



Parental Control – add Client/Device

Selecting or Manually Adding a Device

After clicking **Add** in the Parental Control section, users have two options to add a device:

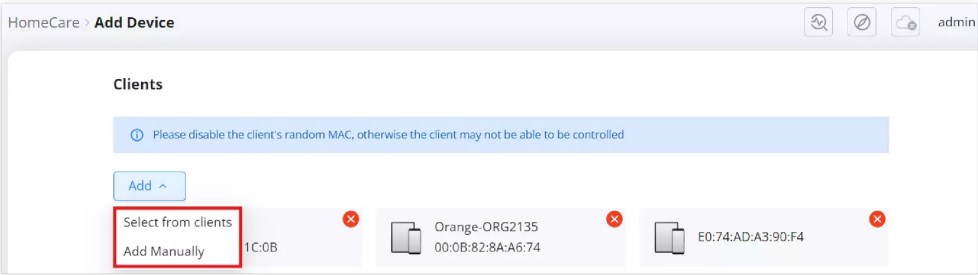
1. **Select from Clients** – Choose a device that is already connected to the router from the available list.
2. **Add Manually** – Enter the MAC address of a device that is not currently connected but needs to be managed under Parental Control.

Important Note:

- Devices with **randomized MAC addresses** may not be properly controlled. It is recommended to **disable MAC randomization** on the client device to ensure proper enforcement of rules.

Steps to Add a Device:

1. Navigate to **Basic** → **HomeCare** → **Parental Control**.
2. Click **Add**, then choose either:
   - **Select from Clients** to pick a device from the connected list.
   - **Add Manually** to enter the MAC address of an offline device.
3. Once added, the device will appear in the list and can be assigned specific Parental Control rules.



Parental Control – add device/client from client lists or manually

Enabling and Configuring Internet Time Limits

The **Internet Time Limit** feature in **Parental Control** allows users to define specific time periods when internet access is blocked for selected devices. This is particularly useful for managing children's online activity by restricting internet usage during school nights or setting time-based limitations.

Steps to Enable Internet Time Limits:

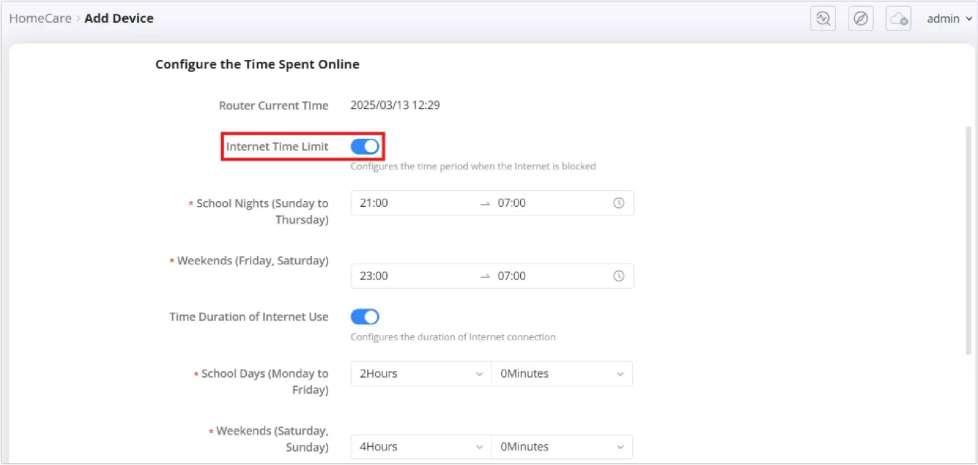
1. Navigate to **Basic** → **HomeCare** → **Parental Control**.
2. Click **Add** to add a client device if not already listed.
3. Enable **Internet Time Limit** by toggling the switch.
4. Configure the **blocked time periods**:
   - Set restricted hours for **school nights (Sunday to Thursday)**.

- Define blocked times for **weekends (Friday and Saturday)**.

5. Enable **Time Duration of Internet Use** to specify the maximum allowed usage time per day:
   - Assign usage limits for **school days (Monday to Friday)**.
   - Configure usage limits for **weekends (Saturday and Sunday)**.

6. Once configured, click **Save** to apply the settings.

These restrictions will automatically disconnect the device from the internet during the specified times.



Parental Control – Configure the time spent online

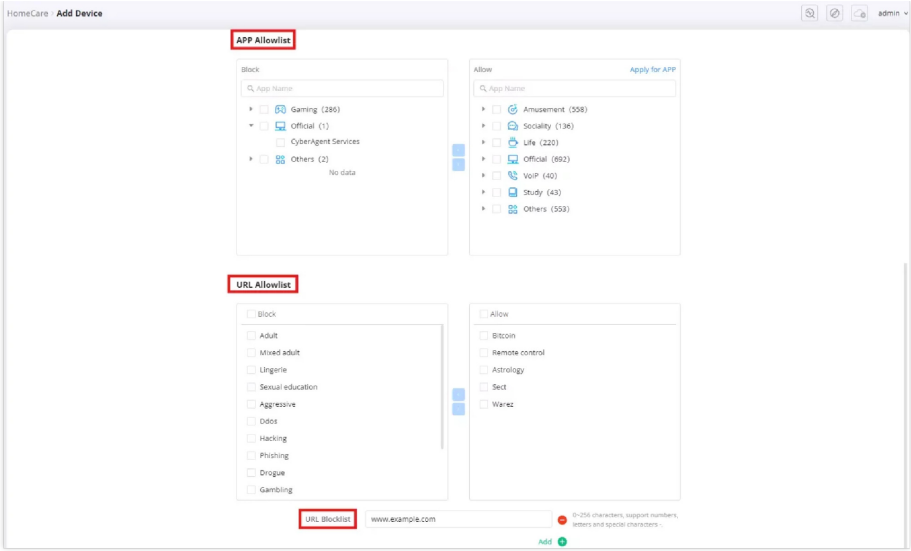
Configuring App and URL Filtering

The App and URL Filtering feature under Parental Control allows users to restrict access to certain applications and websites, ensuring a safer browsing environment.

Steps to Configure App and URL Filtering:

1. Navigate to **Basic** → **HomeCare** → **Parental Control**.
2. Select a device or add a new device.
3. Under the **App Allowlist**, configure application-based restrictions:
   - Use the **Block** section to restrict specific apps or app categories such as gaming or social media.
   - Use the **Allow** section to specify permitted applications.
4. Under the **URL Allowlist**, manage website access:
   - Use the **Block** section to restrict access to specific website categories like adult content, phishing, hacking, and gambling.
   - Add a **custom URL** to block a specific website using the **URL Blocklist** field.
5. Click **Apply** to save the settings.

These settings ensure that only allowed applications and websites are accessible, preventing exposure to inappropriate content.



Parental Control – App/URL allow or block

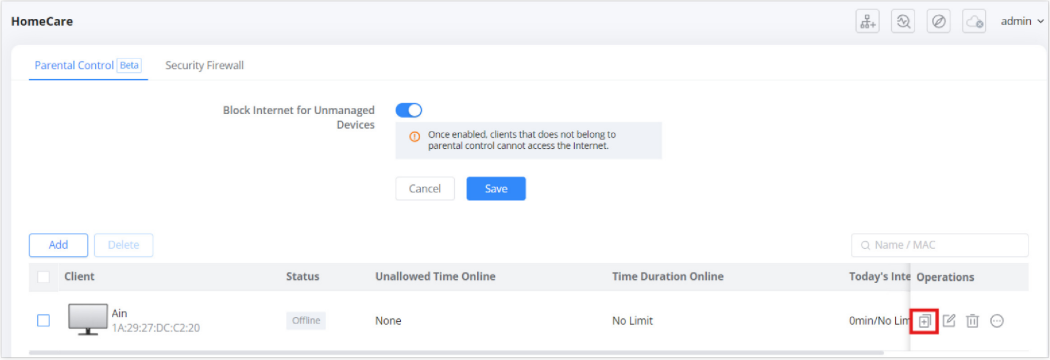
Applying Parental Control Settings to a New Device

The **Parental Control** feature allows users to quickly apply an existing device's settings to a new device, simplifying network management.

Steps to Apply Settings to a New Device:

1. Navigate to **Basic** → **HomeCare** → **Parental Control**.
2. In the list of configured clients, locate the device with the desired settings.
3. Click the **"+"** icon under the **Operations** column.
4. Select the new client to apply the existing settings.
5. Confirm the selection, and the new device will inherit the parental control rules of the original client.

This feature ensures consistency in parental control configurations across multiple devices, streamlining the setup process.



Parental Control – Apply to other devices

One-Click Network Disconnection

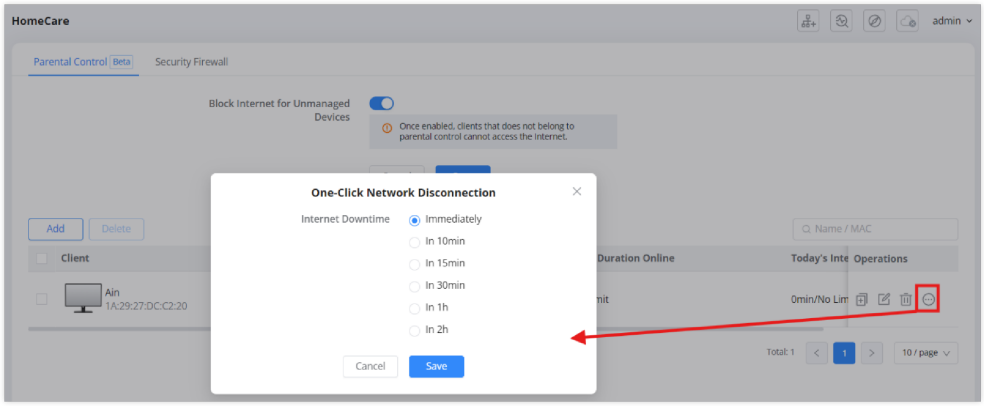
The **One-Click Network Disconnection** feature in **Parental Control** allows administrators to instantly or scheduled disconnect a specific device from the network.

Steps to Disconnect a Device:

1. Navigate to **Basic** → **HomeCare** → **Parental Control**.
2. Locate the device from the list of managed clients.
3. Click on the **three-dot menu (•••) under the Operations column**.
4. Select the **One-Click Network Disconnection** option.
5. Choose one of the following disconnection modes:
   - **Disconnect Immediately** – The device is instantly removed from the network.
   - **Schedule Disconnection** – Set a delay (e.g., 10 min, 15 min, 30 min, 1 hour, 2 hours) before disconnection.

6. Click **Save** to apply the changes.

This feature provides flexibility for managing online time and enforcing parental control policies.



Parental Control – One-Click Network Disconnection

> **Important:**
>
> This feature requires devices to have a static MAC address to function properly. If your device is using a random MAC address, certain functions may not work as expected. To ensure compatibility, follow the steps in Disabling Client Random MAC Address to disable the random MAC feature on your device.

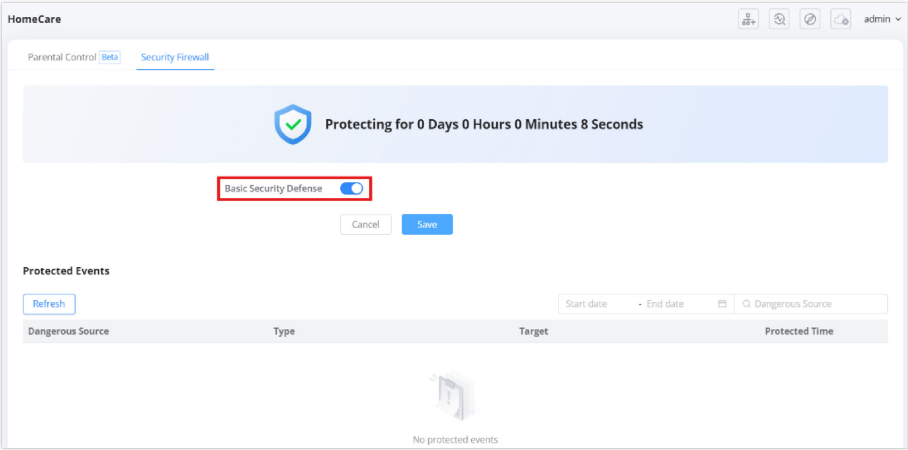
Security Firewall

The **Security Firewall** feature under HomeCare provides **basic network security** by detecting and preventing potential threats, helping to protect connected devices from malicious attacks.

Enabling Security Firewall

To enable the Security Firewall on the router, navigate to:
Basic → HomeCare → Security Firewall

- Toggle **Basic Security Defense** to **Enable**.
- Click **Save** to apply the settings.



HomeCare – Security Firewall

Protected Events

This section logs and displays detected security threats, such as:

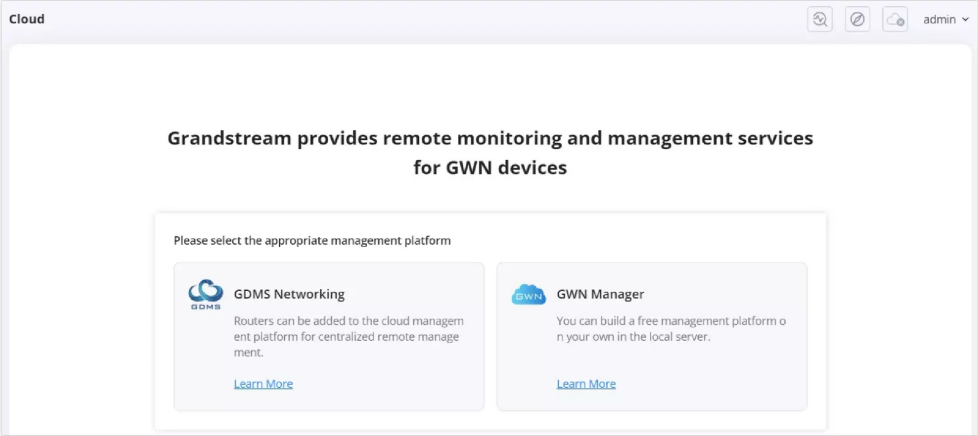
- **Dangerous Sources:** Identifies malicious IP addresses or domains.
- **Threat Type:** Categorizes security risks based on network activity.
- **Target Device:** Specifies which device was affected by the blocked threat.
- **Protected Time:** Logs the date and time of each detected event.

📌 **Note:** Users can click **Refresh** to update the event list and monitor real-time security threats.

This feature enhances **network protection** by proactively identifying and blocking potential cyber threats, ensuring a **safer browsing and internet experience** for all connected devices.

Cloud

The **Cloud** section in the routers allows users to remotely manage and monitor their routers using **Grandstream's cloud-based and on-premise management platforms**. This feature is particularly useful for businesses, IT administrators, and remote workers who require centralized management and control over their network.



Cloud

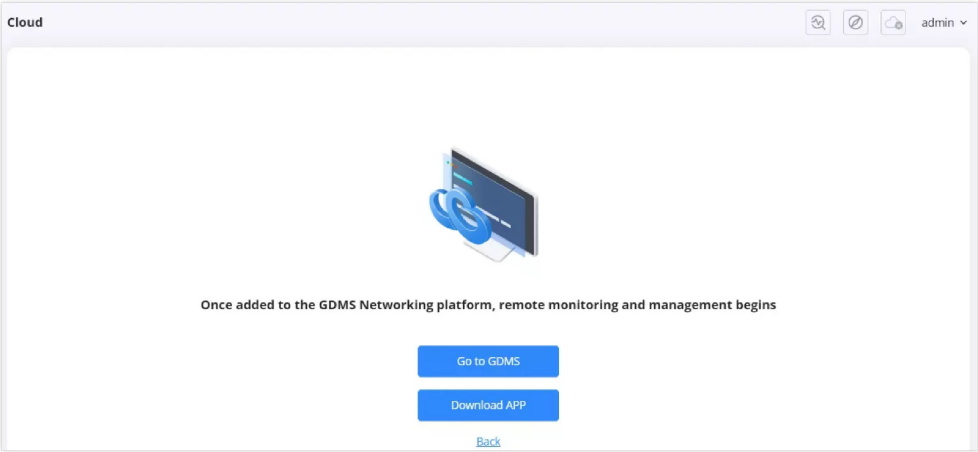
Users can choose between:

1. **GDMS Networking** – A cloud-based platform that allows for centralized remote management.
2. **GWN Manager** – A local, on-premise management solution.

This feature enhances flexibility by offering different deployment options and integration with mobile applications for easy access.

GDMS Networking

The **GDMS Networking** feature enables remote monitoring and centralized management of GWN devices via the **Grandstream Device Management System (GDMS)**. By adding the router to the **GDMS Networking** platform, users can remotely configure, manage, and monitor their network from anywhere.



Cloud – GDMS Networking

Options Available:

- **Go to GDMS**: Clicking this button redirects users to the GDMS web portal, where they can sign in and manage their connected GWN devices.
- **Download APP**: This option provides access to the GDMS mobile application, available for download on both iOS and Android, for on-the-go network monitoring.

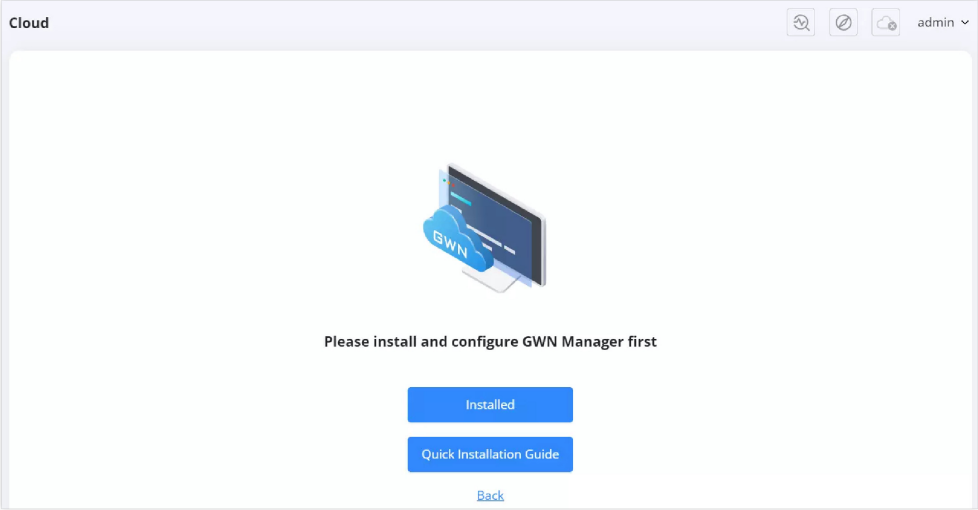
This integration allows network administrators to efficiently manage multiple devices remotely while ensuring real-time monitoring and configuration capabilities.

GWN Manager

For users who prefer a local management platform, **GWN Manager** can be installed and configured.

Installing GWN Manager

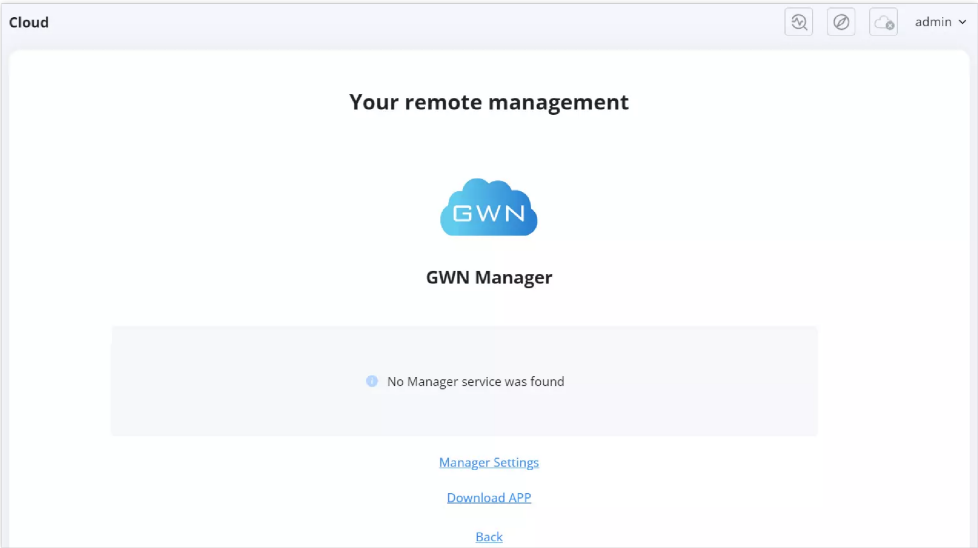
1. Click **Quick Installation Guide** to access the online installation manual.
2. Follow the setup instructions to install GWN Manager on a local server.
3. Click **Installed** once the setup is complete



Cloud – GWN Manager

Accessing GWN Manager

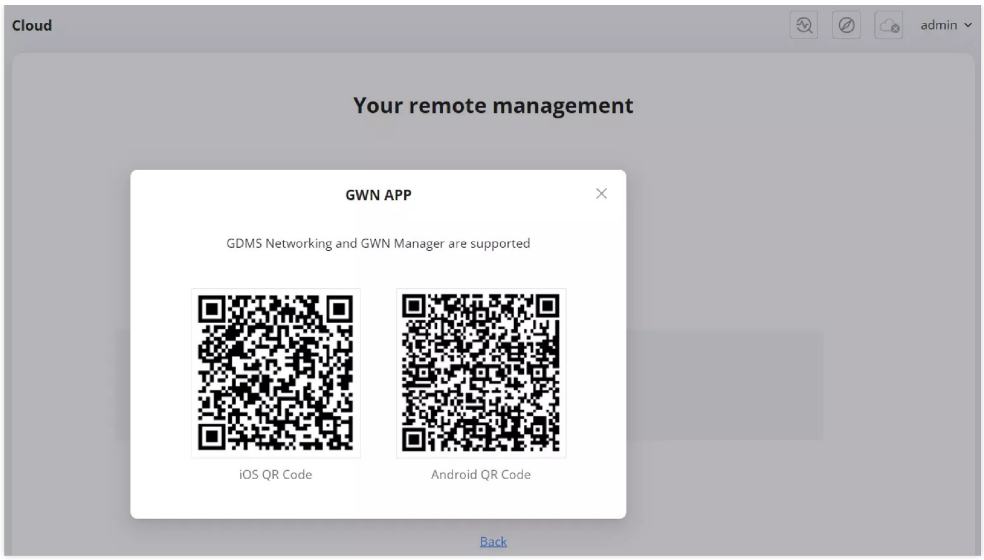
1. After installation, if no **GWN Manager service** is detected, an error message appears.
2. Options available:
   - **Manager Settings** – Configure a local GWN Manager instance.
   - **Download APP** – Install the mobile app for GWN Manager.



Cloud – GWN Manager – page

Downloading the GWN App

1. Clicking **Download APP** opens a **QR Code** scanner.
2. Users can scan the code to download the **GWN App** for **iOS or Android**.

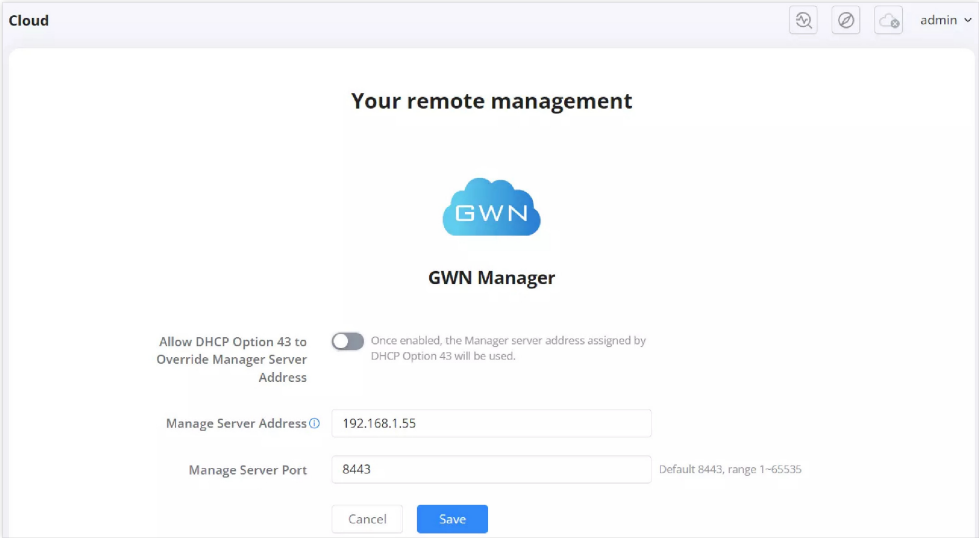


Cloud – GWN Manager – GWN App QR code

Configuring GWN Manager

Users can connect to **GWN Manager** manually or automatically:

- **Automatic Configuration**: Uses **DHCP Option 43** to detect and assign the manager's server.
- **Manual Configuration**: Users input the **Manage Server Address** and **Port** manually.



Cloud – GWN Manager Settings

ADVANCED

Advanced mode unlocks more detailed and sophisticated network settings, suitable for IT professionals and advanced users who require granular control over their network. Key features include:

- **Overview:** A detailed dashboard of the router's performance and status.
- **Internet Settings:** WAN/LAN configurations, DHCP, static IP, and PPPoE settings.
- **Telephony (GWN7062ET only):** Configuration of the **2x RJ11 FXS ports** for VoIP communication.
- **Wi-Fi Settings:** Customization of SSIDs, encryption types, security protocols, and band selection.
- **Clients Management:** Monitoring and managing connected devices.
- **Traffic Management:** Advanced QoS, bandwidth control, and traffic shaping.
- **NAT & Security:** Port forwarding, DMZ, firewall, URL filtering, and DoS protection.
- **VPN:** Secure remote access with multiple VPN protocols (L2TP, PPTP, OpenVPN, WireGuard).
- **IPv6 Support:** Configuration options for next-generation internet protocol.
- **Captive Portal:** Guest network setup and authentication.

- **System & Maintenance:** Firmware upgrades, logs, and backup configurations.

This mode is recommended for **network administrators, power users, and businesses** needing fine-tuned security, performance, and network segmentation.

By switching between these modes, users can **balance ease of use with advanced functionality**, ensuring an optimized experience for both novice and expert users.

Overview

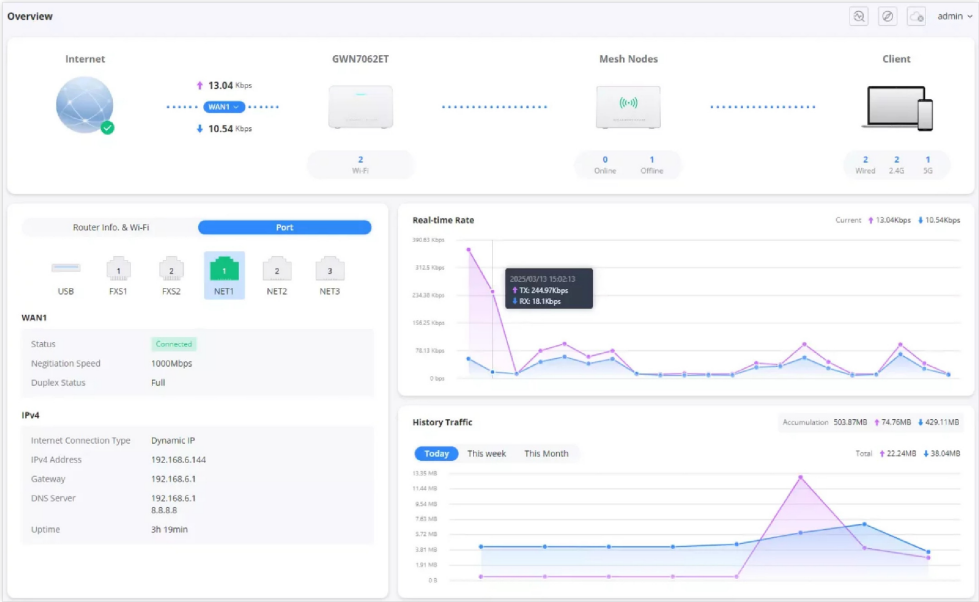
The **Overview Page** provides a real-time snapshot of the router's status, connected devices, and network performance. This page is **dynamic**, meaning users can interact with different sections for detailed insights and navigation to other settings.

Interactive & Navigation Features

- Clicking on **Router, Mesh Nodes, or Client Devices** leads to their respective configuration pages.
- Hovering over graphs provides more detailed network activity.
- Statistics can be toggled between **Today, This Week, or This Month** to analyze trends over time.

This page serves as the **primary dashboard** for monitoring and managing network activity efficiently.

Key Features of the Overview Page



Overview – part 1

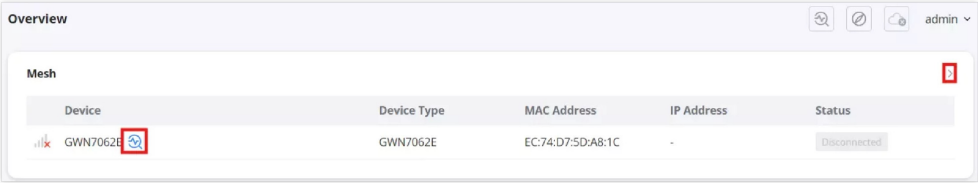
1. **Network Status**:
   - Displays the current upload and download speeds.
   - Clicking on the **router icon** navigates to the **Wi-Fi settings page**.
   - Clicking on the **Mesh Nodes** section directs users to the **Mesh Page**.
   - Clicking on the **Client Devices** (laptop and phone icons) leads to the **Clients Page**.

2. **Router Information & Wi-Fi**:
   - Users can switch between **Port** and **Wi-Fi** views.
   - Shows the status of different ports including **USB, FXS1, FXS2, NET1, NET2, and NET3**.
   - Displays **WAN status**, including:
     - Connection status (e.g., **Connected**).
     - Negotiation speed.
     - Duplex status.

3. **IP & DNS Information**:
   - Displays **IPv4 Address, Gateway, DNS Server**, and **Uptime**.

4. **Real-time Rate Graph**:
   - Shows **current network activity** in an interactive graph.
   - Hovering over the graph reveals precise details of upload and download speeds at specific times.

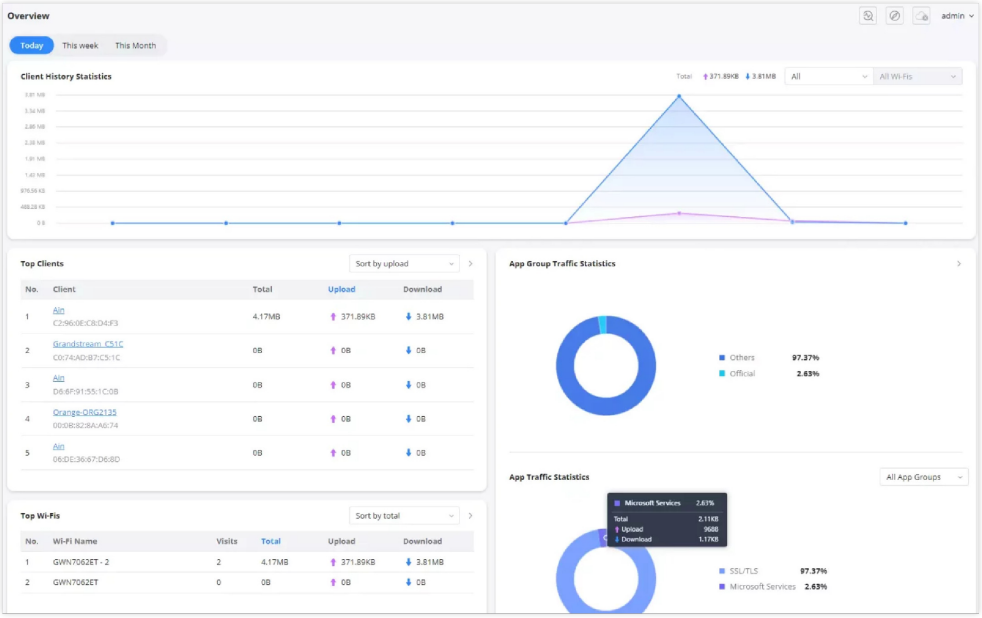
5. **History Traffic Graph**:
   - Users can **filter data** by **Today, This Week, or This Month**.
   - Displays total data usage with **upload and download statistics**.



Overview – part 2

6. **Mesh Network Section**:

- Shows **connected mesh devices**.
- Clicking on the **diagnostic icon** next to a mesh device directs users to the **Intelligent Detection → Mesh Node Connection** settings.
- Clicking on the **arrow icon** leads to the **Mesh Page**.



Overview – part 3

7. **Client & Wi-Fi Statistics**:

- Displays **top clients** based on data usage.
- Allows users to **sort by upload, download, or total usage**.
- Shows **Wi-Fi usage statistics**, including:
  - Number of visits per Wi-Fi network.
  - Upload and download data usage.

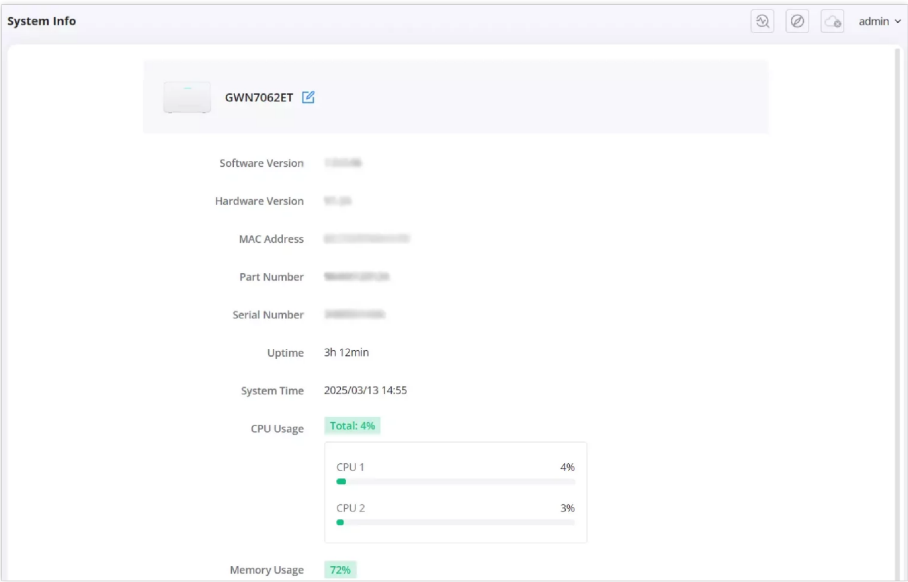
- **App Group Traffic Statistics**:
  - Displays **percentage usage of different app categories**.

- **App Traffic Statistics**:
  - Shows **detailed breakdown of app traffic**, such as Microsoft Services, SSL/TLS, etc.
  - Hovering over **app sections** reveals additional details about upload/download usage.

System Info

The following details are displayed on this page:

- **Device Model**: Identifies the router model, e.g., **GWN7062ET**.
- **Software Version**: Displays the installed firmware version.
- **Hardware Version**: Indicates the router's hardware revision.
- **MAC Address**: The unique network identifier assigned to the router.
- **Part Number**: Manufacturer's part number for the device.
- **Serial Number**: A unique identifier for tracking the device.
- **Uptime**: Displays the total time the router has been running since the last reboot.
- **System Time**: Shows the current time configured on the router.



Overview – System Info

Resource Monitoring

The **System Info** page also provides real-time monitoring of CPU and memory usage:

- **CPU Usage**:
  - Displays the total CPU utilization.
  - Shows individual core usage (e.g., **CPU 1 and CPU 2**).
- **Memory Usage**:
  - Displays the percentage of **RAM utilization**.

Use Case

This page is useful for:

- **Monitoring system performance** to check for resource bottlenecks.
- **Diagnosing issues** related to high CPU or memory usage.
- **Tracking uptime** to determine router stability.

Internet Settings

Internet Setting

The **Internet Settings** page allows users to configure the WAN (Wide Area Network) and LAN (Local Area Network) settings of the GWN7062E and GWN7062ET routers. This page provides options for defining the network roles of available Ethernet ports, setting up different internet connection types, customizing MAC addresses, and configuring Dual-WAN policies for enhanced connectivity and failover mechanisms.

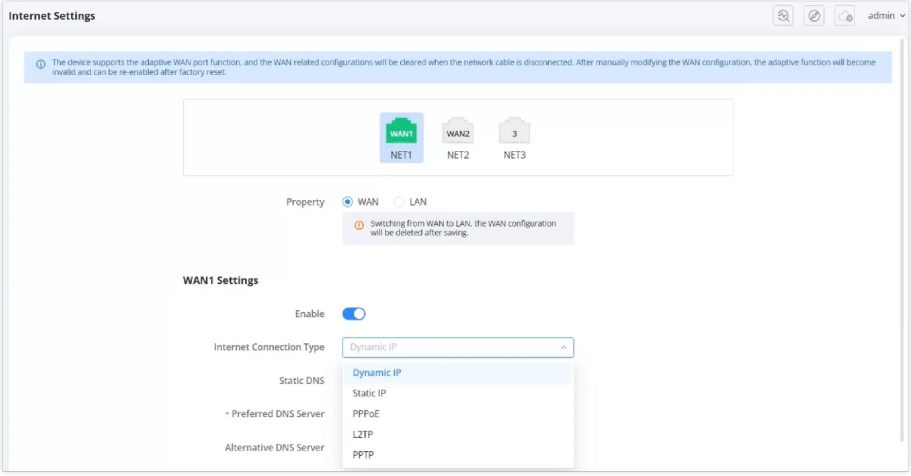
Each Ethernet port on the router is adaptive and can function as either a **WAN** or **LAN** port based on user configuration. This allows flexible network setups to suit various use cases. Users can select the preferred **Internet Connection Type** (e.g., **Dynamic IP, Static IP, PPPoE, L2TP, or PPTP**) and modify additional settings such as DNS configuration and MAC address cloning.

For routers with multiple WAN ports, **Load Balancing** and **Failover** options appear, enabling users to optimize network performance by distributing network traffic across multiple WAN connections or setting up automatic failover in case one connection drops.

- **WAN and LAN Configuration**

The **WAN/LAN Property** section allows users to designate ports as either **WAN** or **LAN**. When switching a port from **WAN to LAN**, all WAN configurations for that port will be cleared.

- **Enable:** Toggle to enable or disable WAN connectivity.
- **Internet Connection Type:** Choose the type of internet connection:
  - **Dynamic IP** – Automatically obtain an IP from the ISP.
  - **Static IP** – Manually configure an IP address, subnet mask, and gateway.
  - **PPPoE** – Authenticate with a username and password provided by the ISP.
  - **L2TP** – Use a Layer 2 Tunneling Protocol for VPN-based internet access.
  - **PPTP** – Configure a Point-to-Point Tunneling Protocol for VPN access.
- **Preferred DNS Server & Alternative DNS Server:** Configure custom DNS servers for better security and speed.

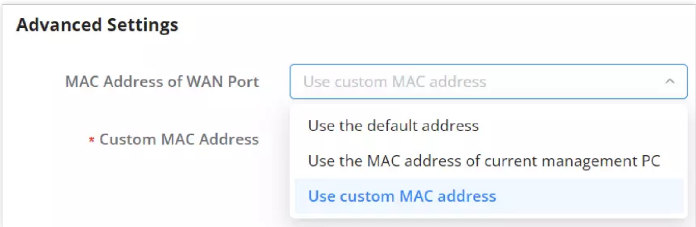


Internet Setting – WAN Settings

- **Advanced WAN Settings**

Users can modify the **MAC Address of the WAN Port** to:

1. **Use the default MAC address** assigned to the router.
2. **Use the MAC address of the current management PC** (useful for ISP authentication).
3. **Enter a custom MAC address** if required.



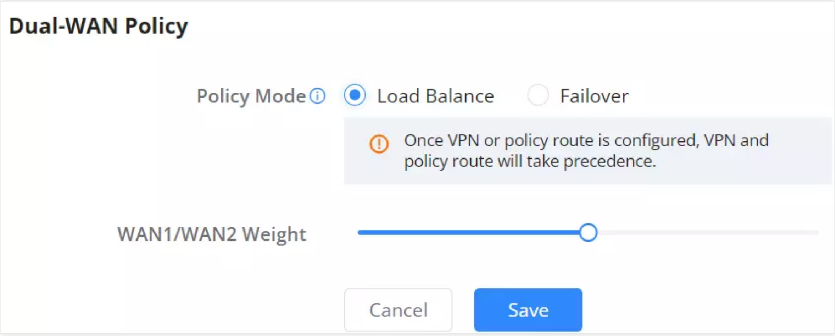
Internet Setting – Advanced Settings

- **Dual-WAN Policy**

If multiple WAN ports are enabled, the router provides options for **Load Balancing** and **Failover** modes:

1. **Load Balancing Mode**

- Balances network traffic between multiple WAN ports.
- Users can adjust the **WAN1/WAN2 Weight** slider to control the distribution of data traffic.

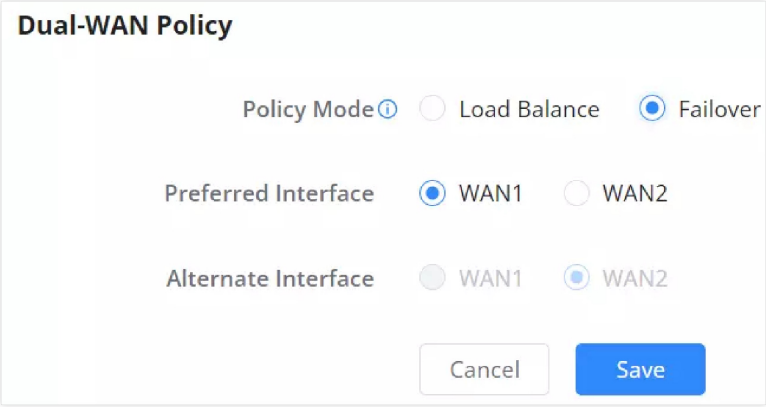


Internet Setting – Load Balance

2. **Failover Mode**

- Sets one WAN interface as the **Primary (Preferred Interface)** and another as a **Backup (Alternate Interface)**.
- If the primary WAN connection fails, the router automatically switches to the backup connection to ensure continuous internet access.

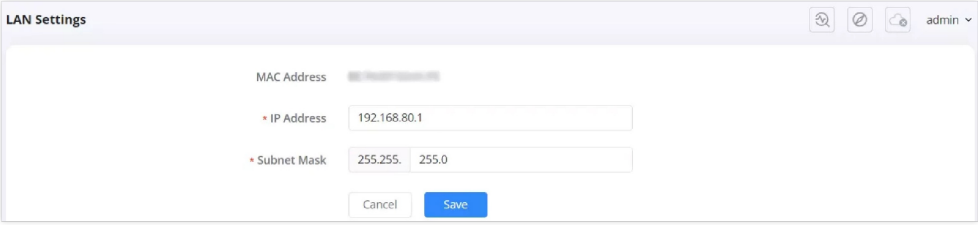
> **Note:**
>
> If VPN or policy routing is configured, those settings take precedence over the Dual-WAN policy.



Internet Setting – Failover

LAN Settings

The **LAN Settings** page allows users to configure the **Local Area Network (LAN)** parameters of the GWN7062E and GWN7062ET routers. This section is essential for defining how devices on the local network communicate with the router and each other. Users can assign a **Gateway IP address** to the router, configure the **subnet mask**, and manage local network connectivity.



LAN Settings

LAN Configuration Options

1. **MAC Address:** Displays the unique MAC address assigned to the LAN interface of the router.
2. **IP Address:** Users can define the router's **LAN IP address**, which serves as the default gateway for devices connected to the local network.
   - Default: `192.168.80.1`
   - This can be customized based on the user's network design.
3. **Subnet Mask:** Defines the network segment by specifying how many IP addresses are available for connected devices.
   - Default: `255.255.255.0`
   - Users can modify the subnet mask to adjust the network size.

Usage Notes

- Changing the **LAN IP address** may require re-accessing the router's web interface using the new IP.
- If the **subnet mask** is modified, ensure that all network devices are configured accordingly to maintain connectivity.
- After making changes, click **Save** to apply the settings.

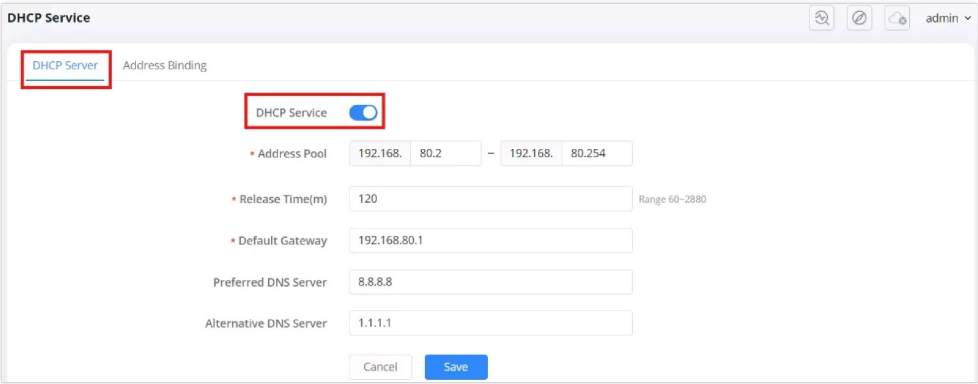
This page is critical for setting up the internal network structure, ensuring efficient communication between connected devices, and defining the router's role in local network management.

DHCP Service

- **DHCP Server**

The **DHCP (Dynamic Host Configuration Protocol) Server** automatically assigns IP addresses to devices on the local network. This ensures seamless connectivity without requiring manual IP configurations for each connected device.

To access the **DHCP Server** settings, navigate to:
Advanced → Internet Settings → DHCP Service → DHCP Server tab



DHCP Server

DHCP Server Settings

1. **DHCP Service**
   - Toggle the switch **ON/OFF** to enable or disable the **DHCP server**.
   - When enabled, the router will dynamically assign IP addresses to connected devices.
2. **Address Pool**
   - Specifies the range of IP addresses available for assignment.
   - Example: `192.168.80.2` – `192.168.80.254`
   - Ensure the range does not conflict with statically assigned IPs.
3. **Release Time (m)**
   - Defines the lease duration for an assigned IP address.
   - Range: **60 – 2880** minutes.
   - After expiration, the DHCP server may reassign the IP if the device disconnects.

4. **Default Gateway**
   - Sets the router's LAN IP address as the gateway for connected devices.
   - Default: `192.168.80.1`

5. **Preferred DNS Server**
   - Specifies the primary **DNS server** used for domain name resolution.
   - Example: `8.8.8.8` (Google Public DNS)

6. **Alternative DNS Server**
   - Specifies a secondary DNS server in case the primary is unavailable.
   - Example: `1.1.1.1` (Cloudflare DNS)

Notes:

- Ensure that the **address pool range** is within the same subnet as the router's LAN IP.
- If DHCP is disabled, **manual IP assignment** is required for all network devices.
- DNS settings affect how devices resolve domain names and access the internet.

Click **Save** to apply changes.

- **Address Binding**

To manage and assign static IP addresses to specific clients on the network, the **Address Binding** feature under DHCP Service allows the administrator to bind a MAC address to a specific IP address. This ensures that the assigned IP address does not change when the device reconnects to the network.

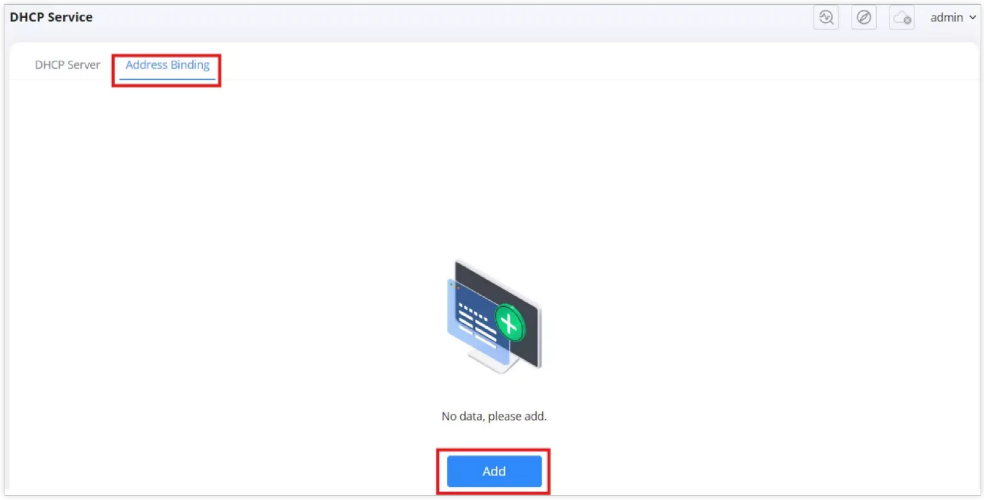
Navigating to the Address Binding Page

1. Go to **Advanced** > **Internet Settings** > **DHCP Service**.
2. Click on the **Address Binding** tab

Adding an Address Binding

If no address bindings are configured, the page will display **"No data, please add."** Follow the steps below to add a new binding.

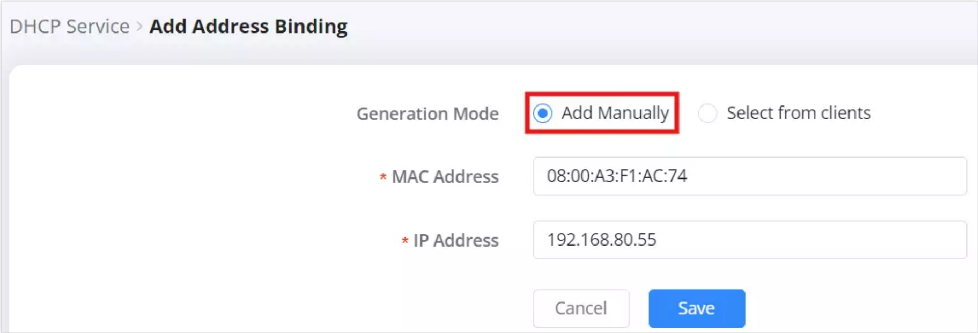
1. Click on **Add** to create a new address binding.
2. A new window appears with two configuration options:
   - **Add Manually** – Enter the **MAC address** and **IP address** manually.
   - **Select from Clients** – Choose a device from the **list of connected clients**, and the system will auto-fill its MAC address and assign an IP.



Address Binding – Add

Option 1: Add Manually

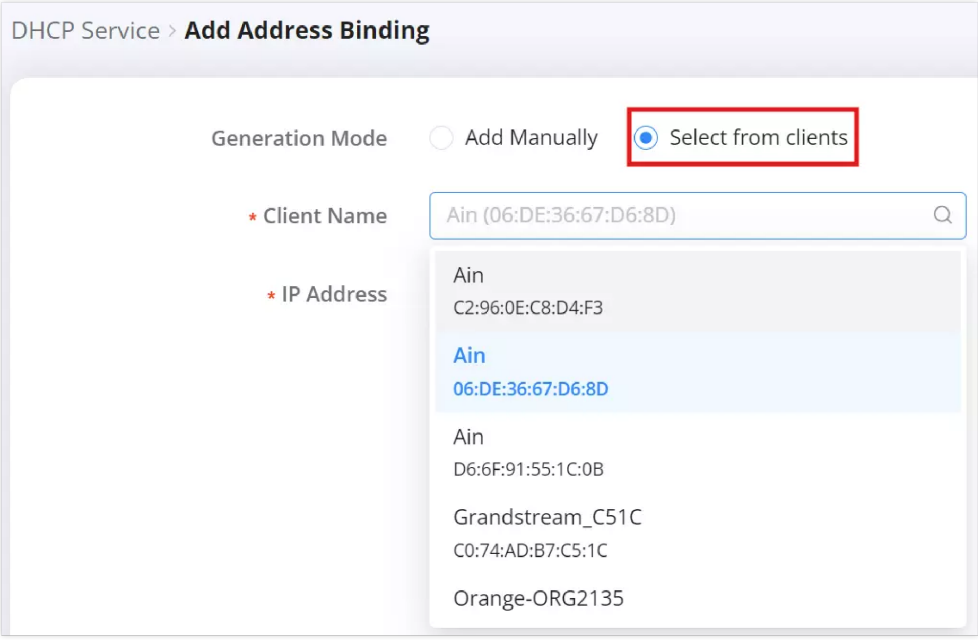
1. Select **Add Manually**.
2. Enter the **MAC Address** of the client.
3. Enter the **IP Address** you want to bind to the MAC address.
4. Click **Save** to confirm.



Address Binding – Add Manually

Option 2: Select from Clients

1. Select **Select from Clients**.
2. Choose a device from the list of connected clients.
3. The system will automatically retrieve its MAC address.
4. Enter the desired **IP Address** for the selected client.
5. Click **Save** to apply the binding



Address Binding – Select from clients

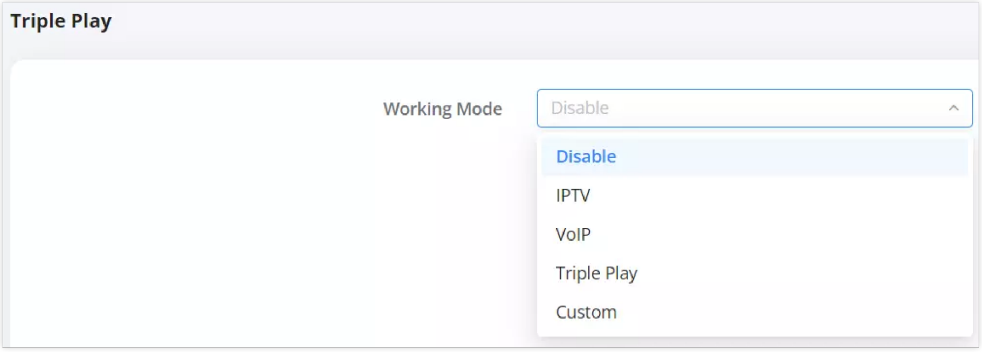
Important:

This feature requires devices to have a static MAC address to function properly. If your device is using a random MAC address, certain functions may not work as expected. To ensure compatibility, follow the steps in Disabling Client Random MAC Address to disable the random MAC feature on your device.

Triple Play

The **Triple Play** feature on the GWN7062E/ET allows users to configure and optimize network settings for multiple services such as **IPTV, VoIP, and Internet**. This function is essential for ISPs and users who need dedicated VLANs (Virtual Local Area Networks) for different types of data traffic. The router provides multiple working modes to ensure efficient handling of IPTV streaming, voice communication, and regular internet usage.

Users can navigate to **Advanced** → **Internet Settings** → **Triple Play** to configure the settings.



Triple Play – Working mode

Selecting a Working Mode

In the **Triple Play** settings, users can select a **Working Mode** from the dropdown menu. The available options are:

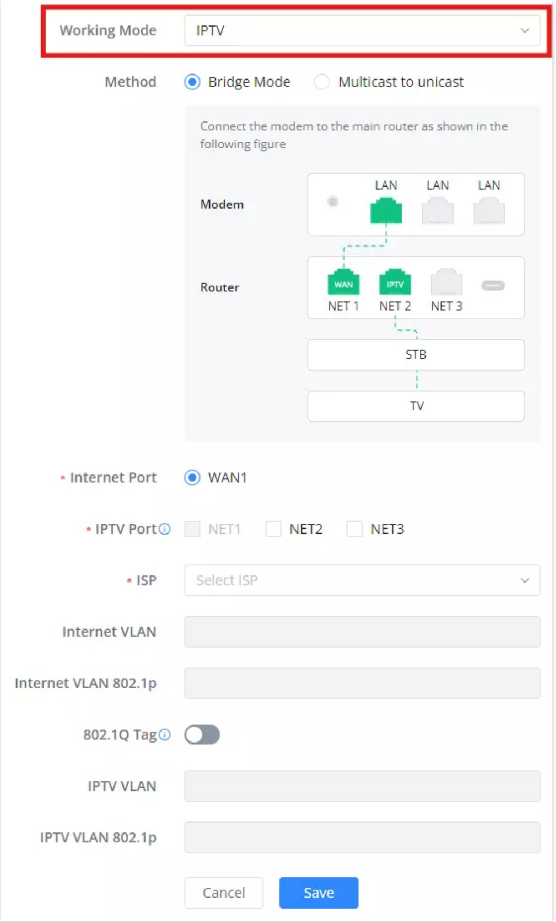
- **Disable**: Triple Play is turned off, and all traffic is treated as general internet traffic.
- **IPTV**: Configures specific settings for IPTV services, ensuring optimal video streaming performance.
- **VoIP**: Prioritizes voice communication traffic, reducing latency and jitter for clear phone calls.
- **Triple Play**: Enables both IPTV and VoIP services while maintaining a separate configuration for regular internet traffic.
- **Custom**: Allows manual configuration of VLAN (Virtual Local Area Network) settings for tailored network segmentation.

To proceed with configuring a specific mode, select the desired option and click **Save**. The corresponding settings for each mode will appear for further customization.

1. **IPTV Mode Overview**

The **IPTV Mode** allows users to configure the router for optimized IPTV service. This setting enables a dedicated IPTV connection while keeping regular internet traffic separate. Users can choose from two different modes:

- **Bridge Mode**: Directly passes IPTV traffic to the connected device, such as a Set-Top Box (STB) or TV.
- **Multicast to Unicast**: Converts multicast IPTV traffic to unicast to improve compatibility with certain networks and devices.



Triple Play – IPTV – Bridge Mode

IPTV Configuration Options:

1. **Selecting the Internet Port**
   - Choose which **WAN port** will handle IPTV traffic.

2. **Assigning an IPTV Port**
   - Select a LAN port (e.g., **NET2, NET3**) to be designated for IPTV service.

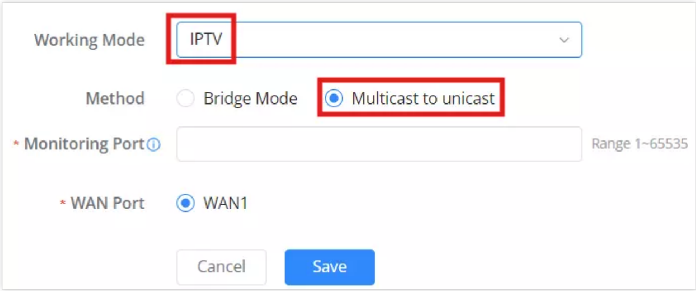
3. **Choosing an ISP**
   - If required, select the Internet Service Provider (ISP) profile for IPTV settings.

4. **VLAN Configuration (Optional)**
   - Users can configure **Internet VLAN**, **IPTV VLAN**, and **802.1Q tagging** to prioritize IPTV traffic.

5. **Multicast to Unicast Conversion**
   - If **Multicast to Unicast** is selected, specify a **Monitoring Port** to track multicast data conversion.

6. **Saving the Configuration**
   - Once the settings are configured, click **Save** to apply the changes.

This setup ensures smooth IPTV streaming by properly isolating and optimizing IPTV traffic within the network.



Triple Play – IPTV – Multicast to Unicast

2. **VoIP Mode**

The **VoIP Mode** is designed to prioritize and optimize Voice over IP (VoIP) traffic, ensuring high-quality voice communication. This mode dedicates a LAN port for VoIP services while maintaining separate network traffic for other internet activities.

VoIP Configuration Options:

1. **Selecting the Internet Port**
   - Choose which **WAN port** will handle VoIP traffic.

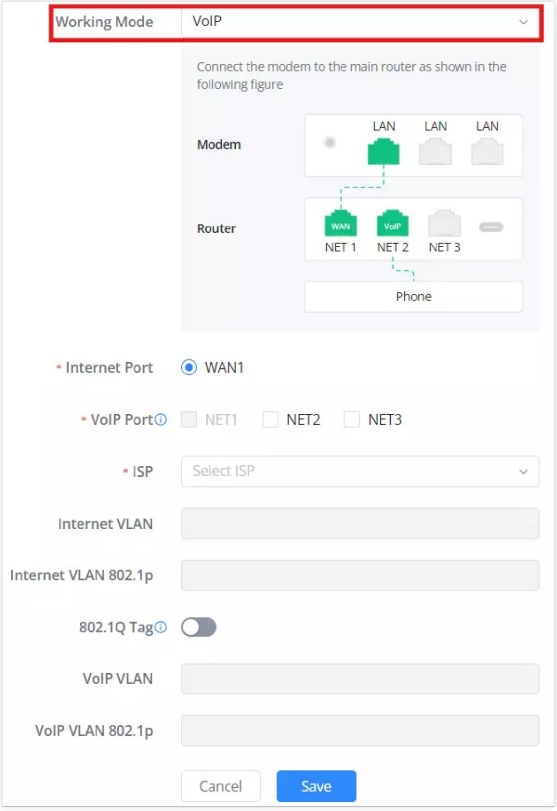
2. **Assigning a VoIP Port**
   - Select a LAN port (e.g., **NET2, NET3**) to be dedicated to VoIP service.

3. **Choosing an ISP**
   - If required, select the **Internet Service Provider (ISP)** profile that provides VoIP service.

4. **VLAN Configuration (Optional)**
   - Users can configure **Internet VLAN**, **VoIP VLAN**, and **802.1Q tagging** to prioritize VoIP traffic and ensure smooth communication.

5. **Saving the Configuration**
   - After setting the VoIP parameters, click **Save** to apply the changes.

By enabling VoIP mode, users ensure that voice traffic is properly isolated and prioritized, reducing latency and packet loss, which is crucial for high-quality VoIP calls.



Triple Play – VoIP

3. **Triple Play Mode**

The **Triple Play Mode** is designed for networks that require separate VLANs for **Internet, IPTV, and VoIP services**. This mode ensures that different types of traffic are managed efficiently, reducing interference and optimizing bandwidth allocation.

Triple Play Configuration Options:

1. **Selecting the Internet Port**
   - Choose which WAN/LAN port will handle general internet traffic.

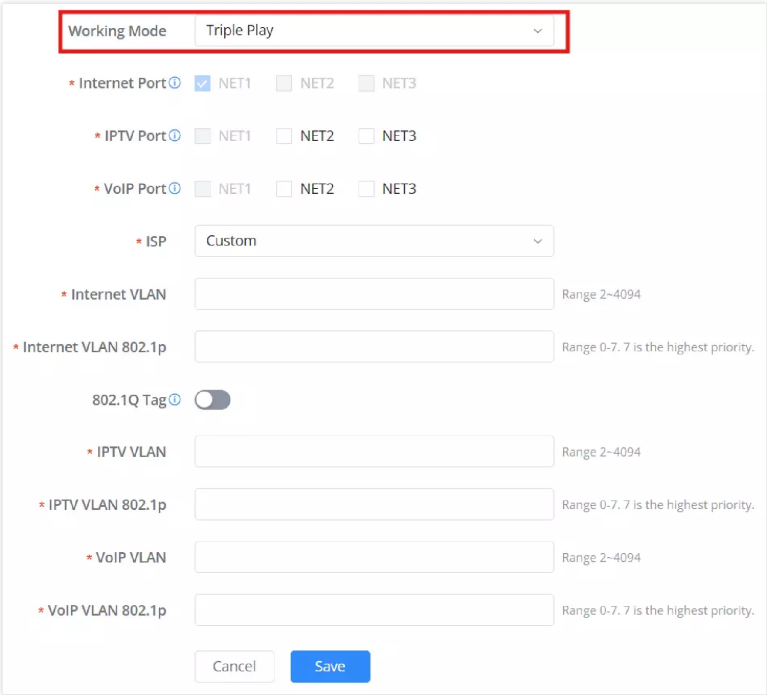
2. **Assigning IPTV and VoIP Ports**
   - Select the dedicated LAN ports (**NET1, NET2, NET3**) for IPTV and VoIP traffic.
   - This ensures that IPTV traffic does not interfere with internet browsing or VoIP calls.

3. **Choosing an ISP Profile**
   - Select an ISP profile from the dropdown list or set it to **Custom** for manual configuration.

4. **VLAN Configuration for Different Services**
   - **Internet VLAN:** Assigns a VLAN ID to the general internet traffic.
   - **IPTV VLAN:** Assigns a VLAN ID specifically for IPTV services.
   - **VoIP VLAN:** Assigns a VLAN ID to prioritize voice traffic.
   - **802.1Q Tagging:** Enables VLAN tagging to manage traffic priority across the network.

5. **Saving the Configuration**
   - After configuring the VLAN and port settings, click **Save** to apply the changes.

By using Triple Play mode, users can separate and prioritize network traffic efficiently, ensuring high performance for streaming services, VoIP calls, and general internet usage.



Triple Play

4. **Custom Mode**

Custom Mode is designed for **advanced users and network administrators** who require granular control over VLAN and traffic segmentation. Unlike the predefined IPTV, VoIP, or Triple Play modes, **Custom Mode** allows users to manually define VLAN IDs, traffic priorities, and network bridges, making it useful in environments with complex network policies, multi-ISP setups, or unique service requirements.

Custom Mode Configuration Options:

1. **Selecting the Internet Port**
   - Choose which WAN/LAN port will handle general internet traffic.

2. **Enabling 802.1Q Tagging**
   - 802.1Q tagging allows VLANs to be assigned to network traffic, helping with network segmentation.

3. **WAN VLAN and Priority Configuration**
   - **WAN VLAN ID:** Assigns a VLAN ID to internet traffic (Range: 2-4094).
   - **WAN VLAN 802.1p Priority:** Defines traffic priority (Range: 0-7, where 7 is the highest priority).
   - These settings ensure that different types of traffic (e.g., voice, video, and data) are handled efficiently.

4. **Configuring NET Bridge**
   - The **NET Bridge** function allows LAN ports to be grouped together under a specific VLAN.
   - Users can assign a VLAN ID to a specific LAN port (**NET1, NET2, NET3**) to control traffic flow.

- The **802.1p value** determines the priority of traffic within that VLAN.

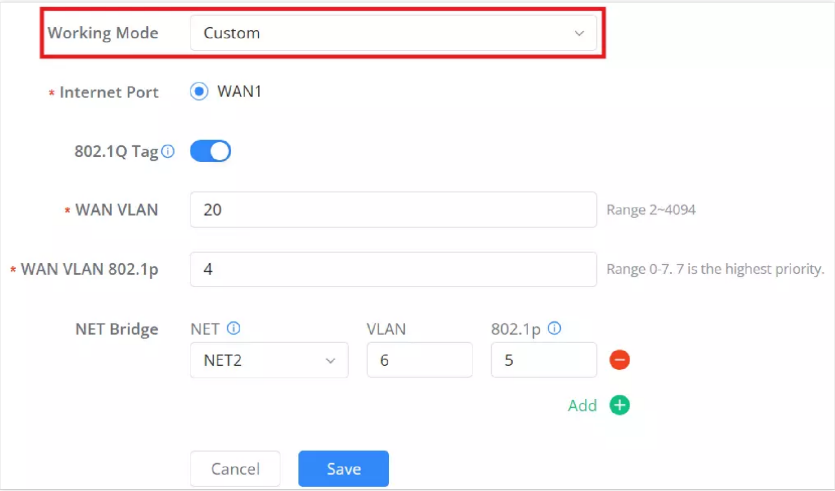
5. **Adding Multiple VLANs**
   - Users can configure multiple VLANs with different priority levels and traffic types to optimize network performance.

6. **Saving the Configuration**
   - Once all settings are configured, click **Save** to apply the changes.

When to Use Custom Mode:

- **Enterprises with multiple VLANs** for security and traffic isolation.
- **Networks requiring specific traffic shaping** based on applications or departments.
- **Multi-ISP environments** where VLAN mapping is required for different services.
- **Advanced IPTV or VoIP configurations** with unique ISP tagging requirements.

By using **Custom Mode**, administrators gain **full control over VLAN assignments**, ensuring efficient **network segmentation, security, and traffic prioritization**.



Triple Play – Custom

Policy Routes

Policy routes allow network administrators to define custom routing rules based on either domain names or client devices. This feature enables precise control over internet traffic, directing specific services or devices through designated WAN interfaces for optimized performance and load balancing.

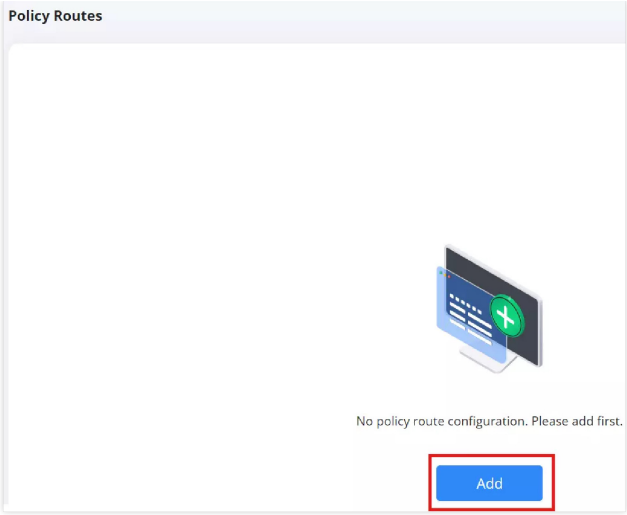
Users can create policy routes based on:

1. **Domain-Based Routing** – Routes specific domains (e.g., youtube.com) through a chosen WAN interface.
2. **Client-Based Routing** – Routes traffic from specific client devices through a designated WAN interface. Clients can be selected from the list of connected devices or added manually by MAC address.

This configuration is accessible via: **Advanced** → **Internet Settings** → **Policy Routes**.

Adding a Policy Route

1. Navigate to **Advanced** → **Internet Settings** → **Policy Routes**.
2. Click the **"Add"** button to create a new policy route.

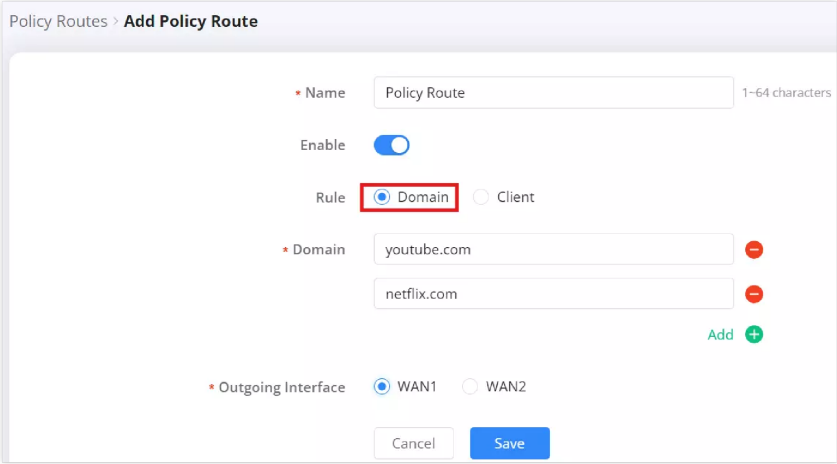


Policy Routes – Add

Configuring a Domain-Based Policy Route:

1. In the **Add Policy Route** window:
   - Enter a **Name** for the policy route.
   - Enable the policy by toggling the **Enable** switch.
   - Select **Domain** as the rule type.
   - Enter one or more domain names (e.g., youtube.com, netflix.com).
   - Choose the **Outgoing Interface** (WAN1 or WAN2).
2. Click **Save** to apply the settings.

This method ensures that all traffic directed to the specified domains is routed through the selected WAN interface.



Policy Routes – Domain

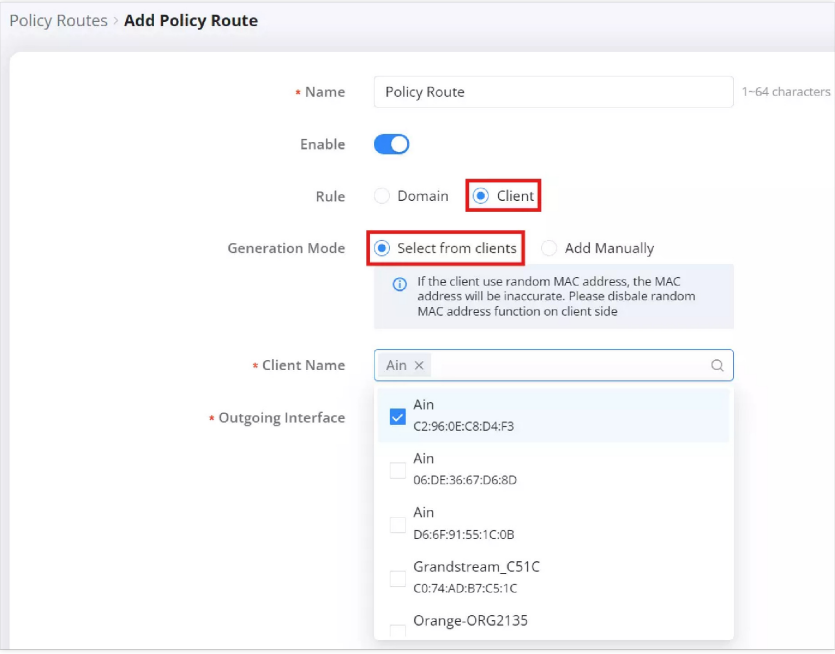
Configuring a Client-Based Policy Route:

1. In the **Add Policy Route** window:
   - Enter a **Name** for the policy route.
   - Enable the policy by toggling the **Enable** switch.
   - Select **Client** as the rule type.

Selecting a Client from the Connected Devices List:

- Choose **Select from clients** under **Generation Mode**.
- Select the **Client Name** from the available list.
- Choose the **Outgoing Interface** (WAN1 or WAN2).
- Click **Save** to apply the settings.

This method allows predefined devices to be routed through specific WAN connections.

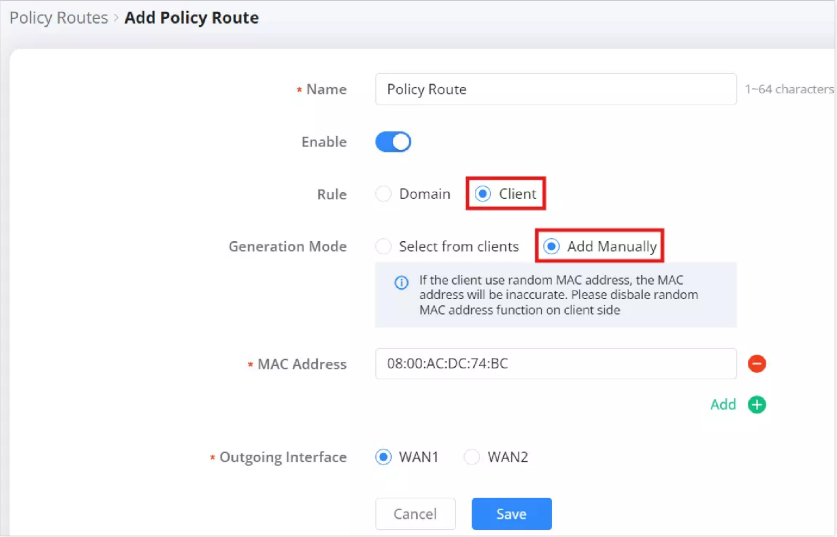


Policy Routes – Select from Clients

Adding a Client Manually (MAC Address):

- Choose **Add Manually** under **Generation Mode**.
- Enter the **MAC Address** of the client device.
- Select the **Outgoing Interface** (WAN1 or WAN2).
- Click **Save** to confirm the settings.

This approach is useful for devices that do not appear in the client list but require specific routing rules.



Policy Routes – Add Manually

Important:

This feature requires devices to have a static MAC address to function properly. If your device is using a random MAC address, certain functions may not work as expected. To ensure compatibility, follow the steps in Disabling Client Random MAC Address to disable the random MAC feature on your device.

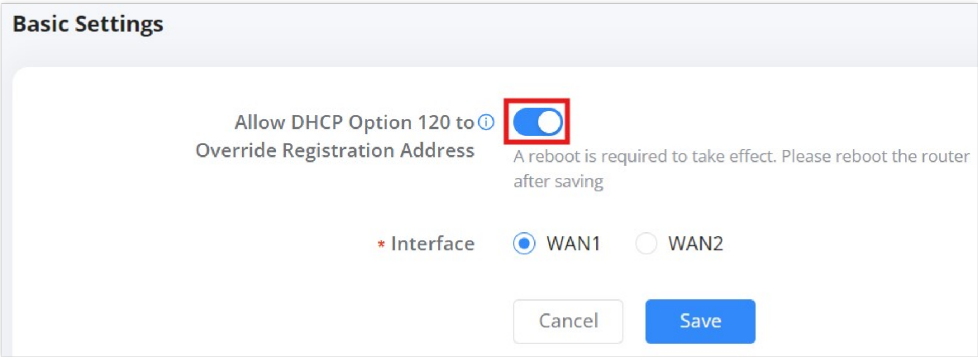
Telephony

The **Telephony** section is available exclusively for the **GWN7062ET** model, as it includes **two FXS ports** for analog telephone connections. These settings allow users to configure VoIP services, enable DHCP Option 120 for SIP registration, and manage FXS ports.

To access **Telephony settings**, navigate to:
Advanced → Telephony → Basic Settings / FXS Settings

Basic Settings

The **Basic Settings** page includes an option to allow **DHCP Option 120**, which helps SIP phones automatically obtain the **VoIP server registration address**.



Telephony – Basic Settings

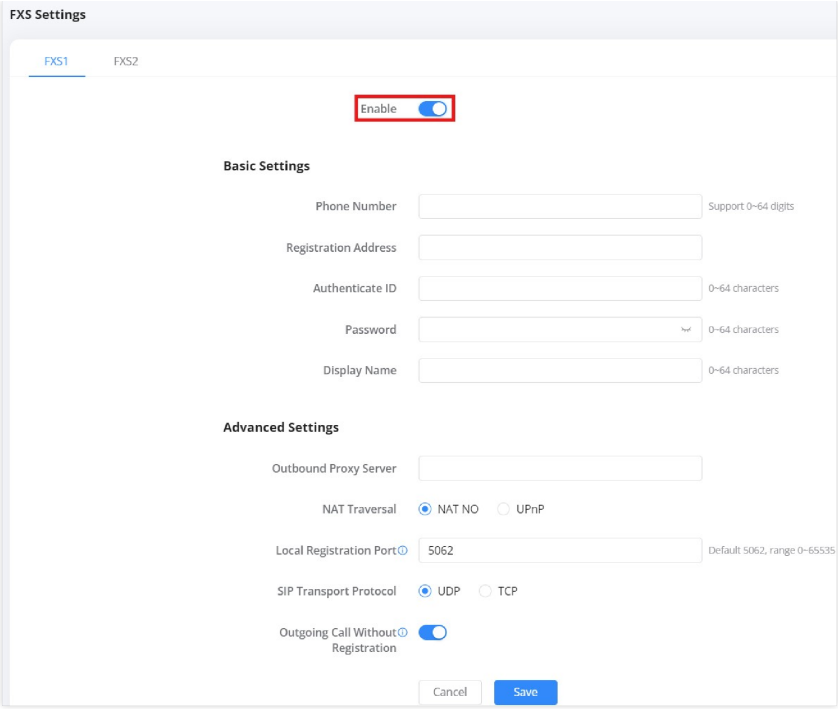
Steps to Enable DHCP Option 120:

1. **Navigate to**: **Advanced → Telephony → Basic Settings**
2. Toggle **Allow DHCP Option 120** to **ON**
3. Select the desired **WAN interface** (**WAN1 or WAN2**) for SIP registration.
4. Click **Save** to apply changes.
5. **Reboot the router** for the settings to take effect.

This feature is useful for automatic VoIP service registration when multiple WAN interfaces are available.

FXS Settings

The **FXS Settings** page allows users to configure the two **FXS ports** for analog telephone connections, enabling **VoIP services** over traditional phones.



Telephony – FXS Settings

Steps to Enable FXS Ports:

1. **Navigate to**: **Advanced** → **Telephony** → **FXS Settings**
2. Select **FXS1** or **FXS2** from the tabs at the top.
3. Toggle **Enable** to **ON**.
4. Fill in the following required fields:
   - **Phone Number**: Assign a number to the FXS line.
   - **Registration Address**: Enter the SIP server address provided by your VoIP provider.
   - **Authenticate ID & Password**: Enter the credentials from your VoIP service provider.
   - **Display Name**: Set the name displayed for outgoing calls.
5. Configure **Advanced Settings** as needed:
   - **Outbound Proxy Server**: If required by your VoIP provider, enter the outbound proxy server address.
   - **NAT Traversal**: Select **NAT NO** or **UPnP** based on network requirements.
   - **Local Registration Port**: Default is **5062**, but can be changed if necessary.
   - **SIP Transport Protocol**: Choose between **UDP or TCP** based on provider recommendations.
   - **Outgoing Call Without Registration**: Enable or disable this option as needed.
6. Click **Save** to apply changes.

This configuration ensures that the **FXS ports** function correctly, allowing users to make and receive calls over their VoIP service.

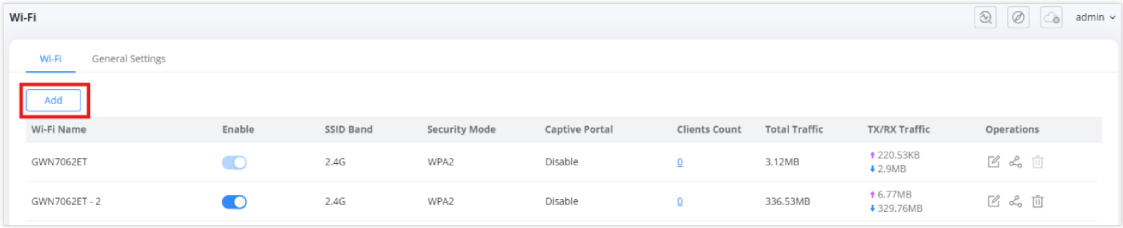
Wi-Fi Settings

Wi-Fi

The **Wi-Fi Settings** section allows users to configure wireless networks, manage SSIDs, apply security settings, and enable advanced features such as **captive portals, scheduled Wi-Fi disabling, and QR code sharing**. This section is essential for optimizing the router's wireless performance, ensuring secure network access, and providing seamless connectivity for multiple devices.

Navigating to Wi-Fi Settings

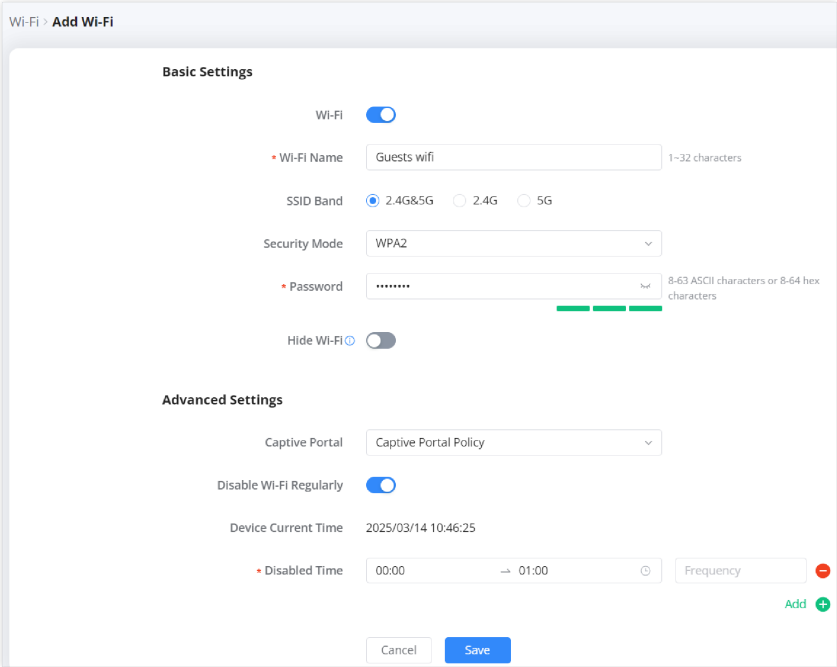
1. Log in to the router's **Web UI**.
2. Navigate to **Advanced** → **Wi-Fi Settings** → **Wi-Fi**.



Wi-Fi page

Adding a New Wi-Fi Network:

1. Click the **"Add"** button to create a new Wi-Fi network.
2. In the **Basic Settings** section:
   - Toggle **Wi-Fi** to **enable**.
   - Enter the **Wi-Fi Name (SSID)**.
   - Select the **SSID Band** (2.4GHz, 5GHz, or both).
   - Choose the **Security Mode** (e.g, WPA2, WPA3).
   - Set a **password** (8-64 ASCII characters or hex format).
   - (Optional) Enable **Hide Wi-Fi** to prevent SSID broadcasting.
3. In the **Advanced Settings** section:
   - Choose a **Captive Portal Policy** (if applicable).
   - Enable **Disable Wi-Fi Regularly** to schedule automatic network disabling.
   - Configure the **Disabled Time** range and frequency.
4. Click **Save** to apply changes.



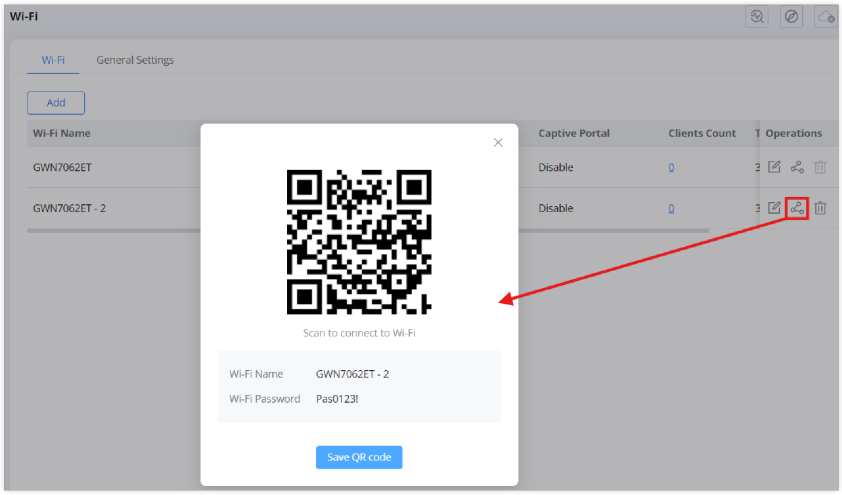
Add Wi-Fi

Managing Existing Wi-Fi Networks:

The **Wi-Fi Settings** page displays the list of existing Wi-Fi networks. Users can:

- **Enable/Disable** SSIDs with the toggle switch.
- **Edit** SSID settings by clicking the **edit icon**.
- **Delete** an SSID with the **trash icon**.

- **Monitor Traffic** statistics for each Wi-Fi network.



Share Wi-Fi

Sharing Wi-Fi via QR Code:

Users can generate a QR code to allow guests to quickly connect to the Wi-Fi network.

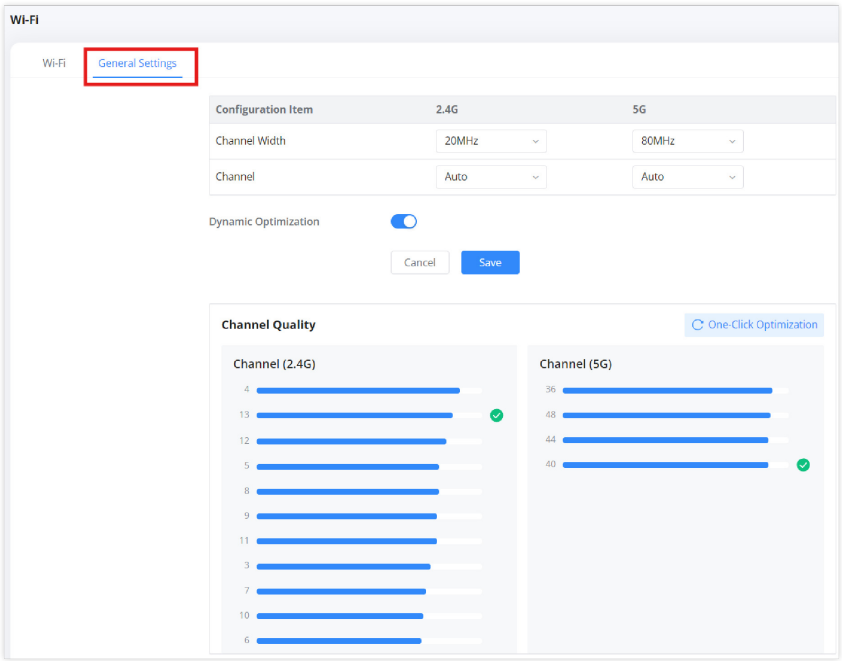
1. Click the **"Share"** icon next to an SSID.
2. A QR code containing the SSID and password will be displayed.
3. Click **"Save QR Code"** to download it as an image.
4. Users can scan the QR code with their mobile device to connect instantly.

Wi-Fi General Settings

The **General Settings** tab under **Wi-Fi Settings** provides users with advanced controls for optimizing Wi-Fi performance. This section allows for configuring **channel width, channel selection, and dynamic optimization** for both the **2.4GHz and 5GHz bands**, ensuring a stable and interference-free wireless environment.

Navigating to General Settings

1. Log in to the router's **Web UI**.
2. Navigate to **Advanced** → **Wi-Fi Settings** → **Wi-Fi** → **General Settings**.



Wi-Fi General Settings

Available Configuration Options:

1. **Channel Width**:
   - Adjust the **channel width** for both **2.4GHz** and **5GHz** bands.
   - Options:
     - **2.4GHz**: 20MHz (recommended for stability).
     - **5GHz**: 40MHz, 80MHz (wider channels for higher speeds).
2. **Channel Selection**:
   - Select **Auto** to allow the router to choose the best available channel dynamically.
   - Manually specify a channel if needed to avoid interference.
3. **Dynamic Optimization**:
   - When enabled, the router automatically **optimizes Wi-Fi channels** to reduce congestion and interference.
4. **One-Click Optimization**:
   - Click this button to manually trigger **Wi-Fi optimization**, allowing the router to scan and apply the best wireless settings.
5. **Channel Quality Monitoring**:
   - Displays the **current channel quality** for both **2.4GHz and 5GHz bands**, helping users identify interference and adjust settings accordingly.

Mesh

The **Mesh Networking** feature on the **GWN7062E/T** routers enables users to expand their network coverage by wirelessly connecting multiple routers. This feature is ideal for homes and small businesses, providing seamless internet access across a larger area without the need for additional cabling. Mesh networking allows for automatic route optimization and enhances network reliability, ensuring uninterrupted connectivity even if one of the routers in the mesh experiences issues.

With Mesh Networking, users can:

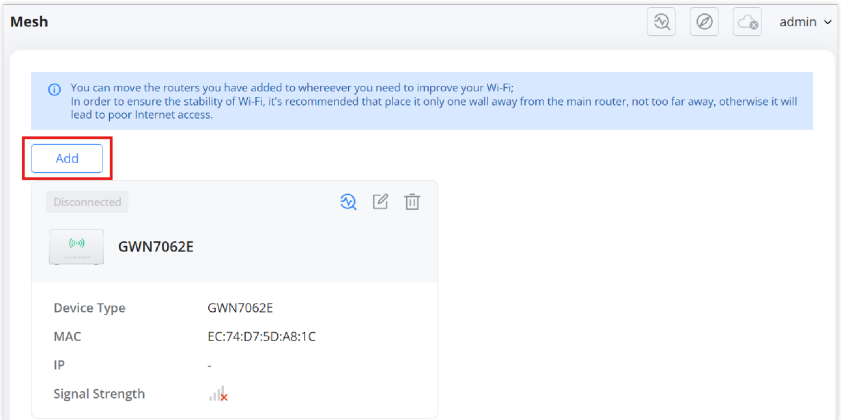
- Extend Wi-Fi coverage seamlessly by adding more routers.
- Optimize signal strength and network stability using intelligent routing.
- Avoid the need for additional Ethernet cables.
- Ensure a self-healing network where traffic automatically reroutes in case of link failure.

1. Accessing the Mesh Networking Feature

Navigate to **Advanced** → **Wi-Fi Settings** → **Mesh** to access the Mesh configuration page.

2. Adding a New Router to the Mesh Network

- Click on the **"Add"** button to begin the process of adding a new node router to the mesh.
- A prompt will appear detailing the **preparations required** before adding the new router.



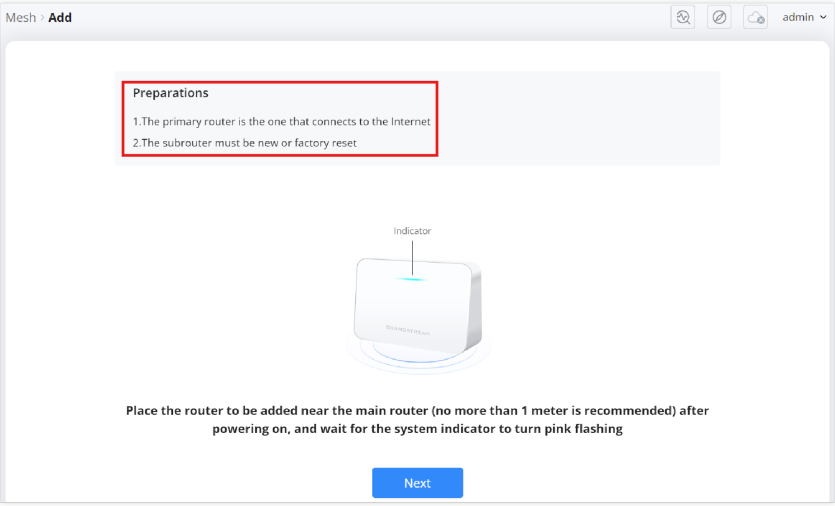
Mesh – Add sub router

3. Preparing the Router for Mesh Connection

Before proceeding with the setup:

- The **primary router** should already be connected to the internet.
- The **new router (node router)** must be **new or factory reset** to be properly detected.

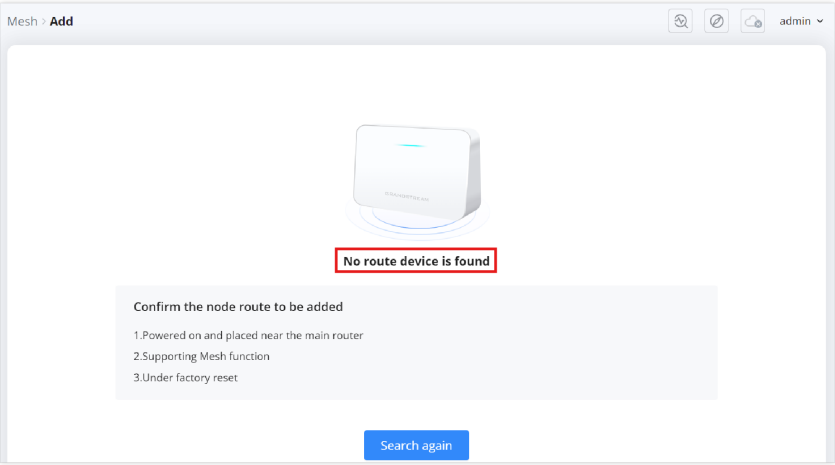
Once these conditions are met, click **"Next"** to proceed.



Preparing the Router for Mesh Connection

4. Searching for Available Node Routers

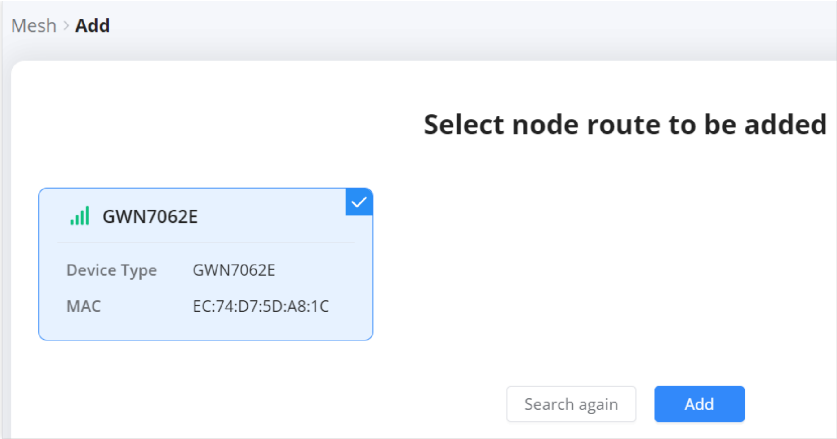
- The system will search for available routers that can be added to the Mesh.
- If no routers are found, users should:
  - Ensure the node router is powered on.
  - Confirm that the router supports Mesh functionality.
  - Reset the router to factory settings if necessary.
  - Click **"Search Again"** to retry detection.



Mesh – no router is found

5. Selecting the Router to Add

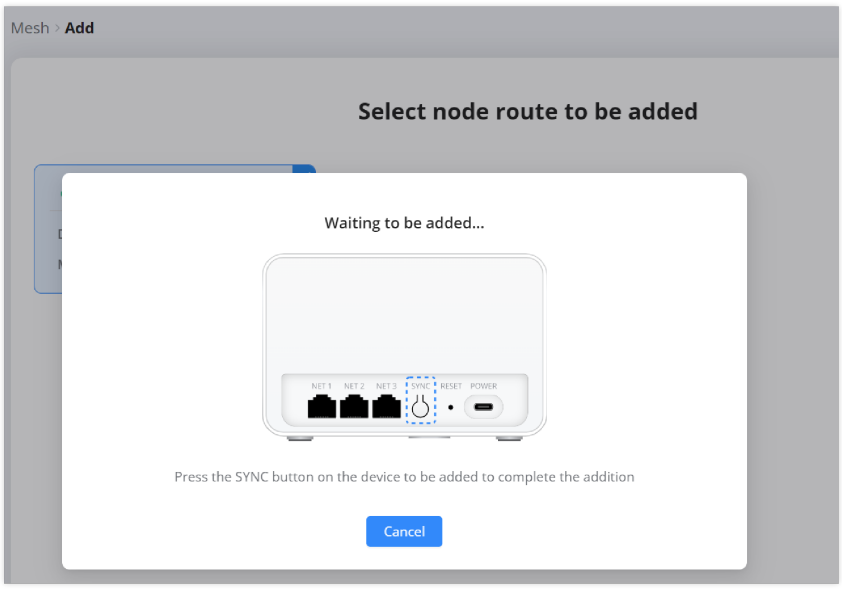
- Once a node router is detected, it will be displayed on the screen.
- Select the router and click **"Add"** to initiate the connection process.



Mesh – sub router is found

6. Synchronizing the Node Router

- After clicking "Add," the system will prompt users to **press the "SYNC" button** on the node router.
- Locate the **SYNC button** on the device and press it to complete the pairing process.



Mesh – Synchronizing the Node Router

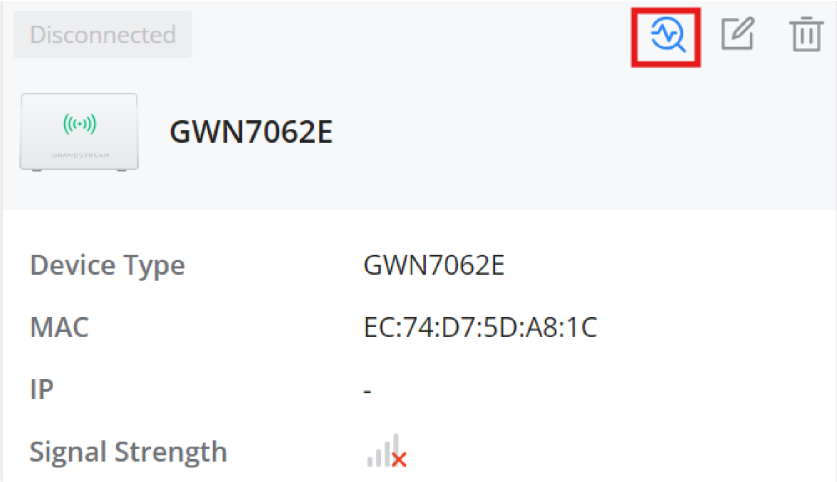
7. Confirmation of Successful Connection

- If the pairing is successful, the node router will appear in the **Mesh list** as **"Connected"**, displaying its **MAC address, IP address, and signal strength**.

Mesh – Confirmation of Successful Connection

8. Diagnosing Connection Issues

- If the node router appears as **"Disconnected"**, users can troubleshoot the connection by clicking on the **diagnostic icon**.
- This will open the **Intelligent Detection Page**, where further tests can be run to identify the issue.



Mesh – Diagnosing Connection Issues

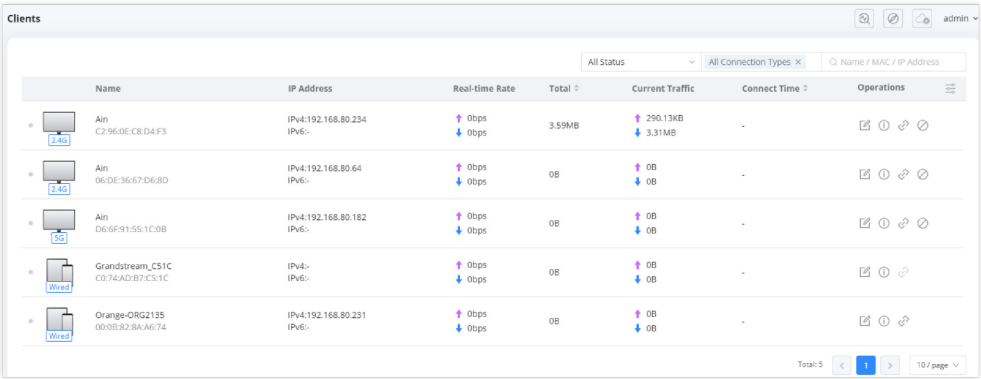
For instructions on using the physical **Sync Button** and understanding the system indicator lights, please refer to this guide: GWN7062E(T) – Setting Up Mesh Using the SYNC Button

Clients

The **Clients** page on the GWN7062E/T router provides an overview of all connected devices, including both wired and wireless clients. This section allows users to monitor connected clients, view real-time traffic statistics, and manage client access. Users can rename devices, assign static IPs, analyze traffic statistics, and block unwanted clients.

Accessing the Clients Page

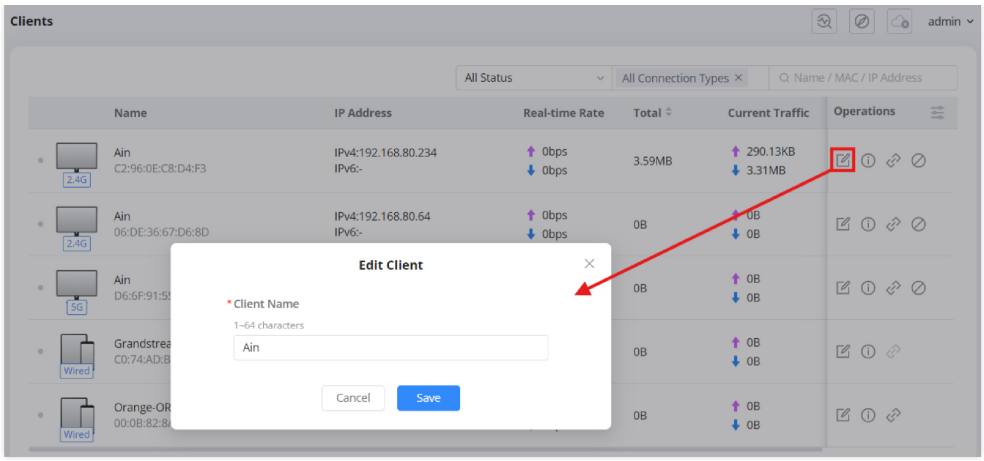
1. Navigate to **Advanced** → **Clients** in the left sidebar.
2. The Clients page will display a list of all connected devices, including:
   - Device Name
   - IP Address (IPv4/IPv6)
   - Connection Type (2.4G, 5G, or Wired)
   - Real-Time Data Rate
   - Total Data Usage
   - Current Traffic
   - Available operations for each client



Clients page

Modifying a Client Name

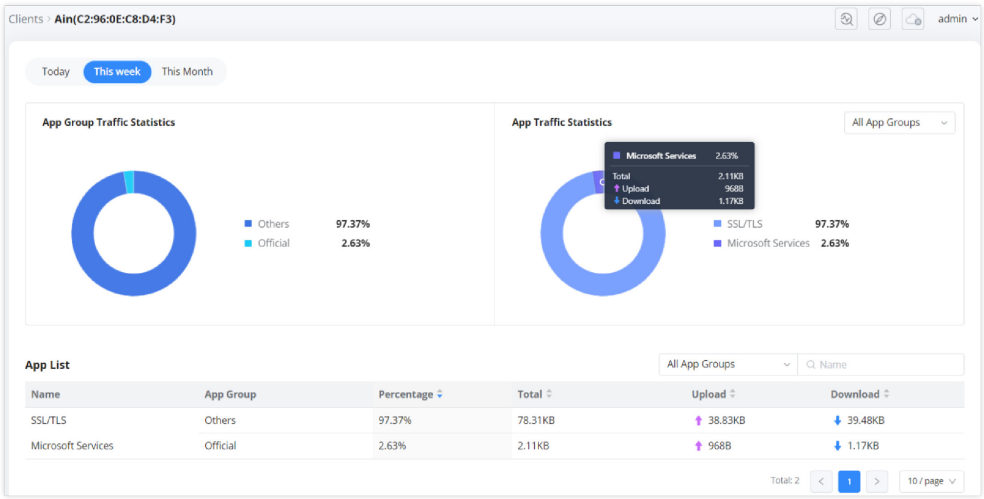
1. Click on the **Edit (pencil) icon** next to the client name.
2. Enter a new name in the pop-up window.
3. Click **Save** to apply the changes.



Clients – edit name

Viewing Client Traffic Details

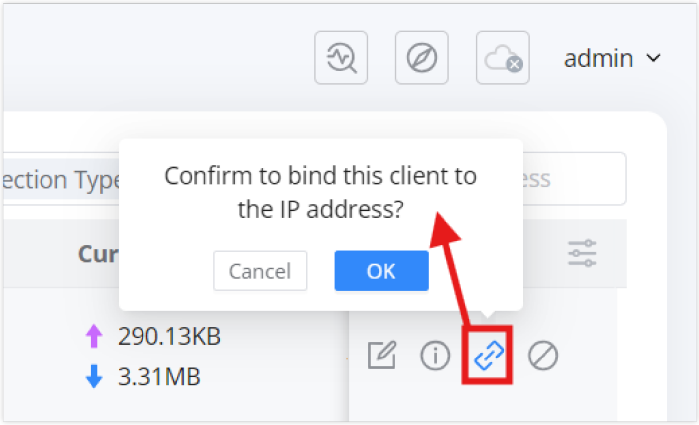
1. Click on the **Exclamation mark icon** next to a client entry.
2. This opens a **Client Traffic Overview** page with:
   - **Traffic statistics by app group**
   - **Data usage trends over time** (Today, This Week, or This Month)
   - **Breakdown of applications consuming network resources**



Clients – View details

Binding a Static IP to a Client

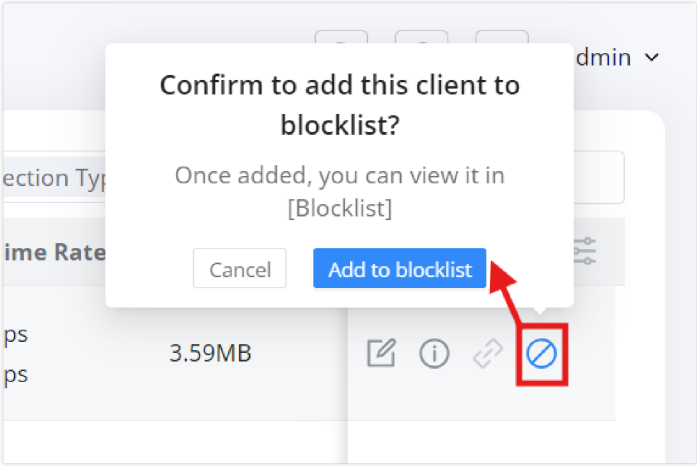
1. Click on the **Link (chain) icon** next to the client.
2. A confirmation prompt will appear: *"Confirm to bind this client to the IP address?"*
3. Click **OK** to assign a static IP to the client.



Clients – set a static IP address for the client

Blocking a Wireless Client

1. Click on the **Block (circle with a slash) icon** next to the client.
2. A confirmation prompt will appear: *"Confirm to add this client to blocklist?"*
3. Click **Add to blocklist** to prevent the device from reconnecting to the network.
   - **Note:** Blocking is only effective for **wireless clients**.



Clients – Add Client to Blocklist

Disabling Client Random MAC Address

Many modern operating systems use **random MAC addresses** as a privacy feature. However, for certain router functions such as **Parental Control, Address Binding, Policy Routes, and Blocklist**, a **static MAC address** is required.

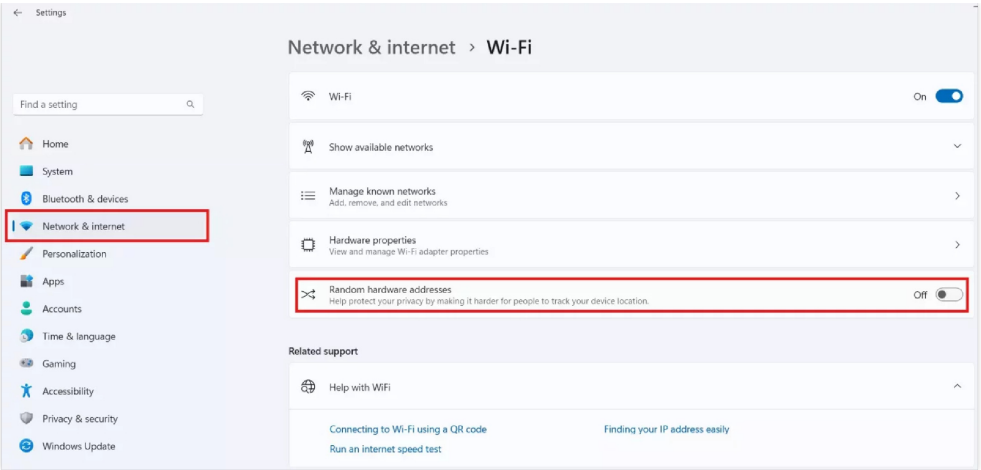
To ensure proper operation, users should **disable random MAC addresses** for their specific Wi-Fi network. Below is a general method to do so, followed by examples for **Windows®, iOS®, and Android®**.

General Steps to Disable Random MAC Address:

1. **Navigate to Wi-Fi settings** on your device.
2. **Locate the network** you are connected to.
3. **Open network properties** or advanced settings.
4. Find the **MAC Address Type / Privacy Settings** option.
5. Select **Use Device MAC / Phone MAC / Fixed MAC** instead of **Randomized MAC**.
6. Save and reconnect to the network.

- **Windows® (Example: Windows® 10/11)**

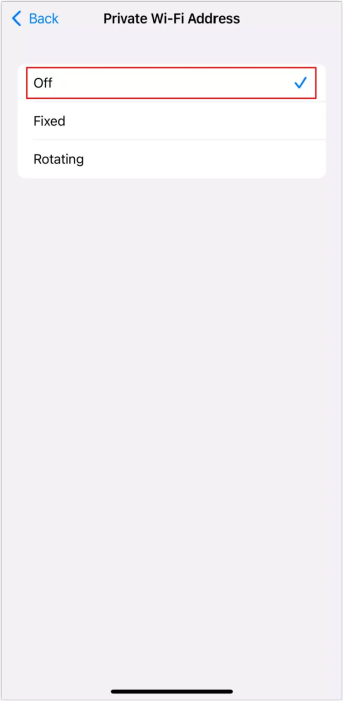
1. **Go to** `Settings` > `Network & Internet` > `Wi-Fi`.
2. Click on `Manage known networks`.
3. Select your Wi-Fi network and click `Properties`.
4. Scroll down to `Random hardware addresses`.
5. Toggle the option **Off**.



Disable Random MAC Address – Windows® (Example: Windows® 10/11)

- **iOS® (Example: iOS® 14 and later)**

1. **Open** `Settings` > `Wi-Fi` .
2. Tap on the (i) **information icon** next to your Wi-Fi network.
3. Tap `Private Wi-Fi Address` .
4. Select **Off**.

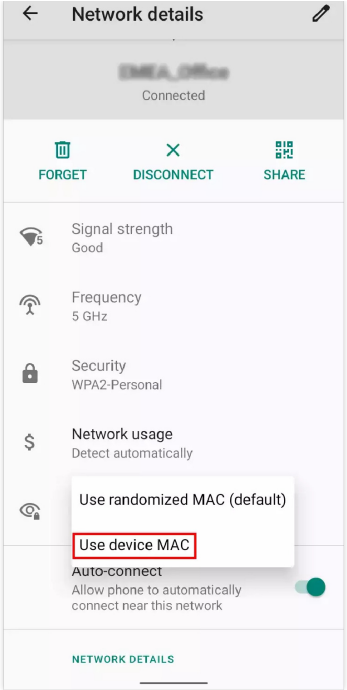


Disable Random MAC Address – iOS®
(Example: iOS® 14 and later)

- **Android® (Examples: Stock Android, Samsung®, Xiaomi)**

Stock Android:

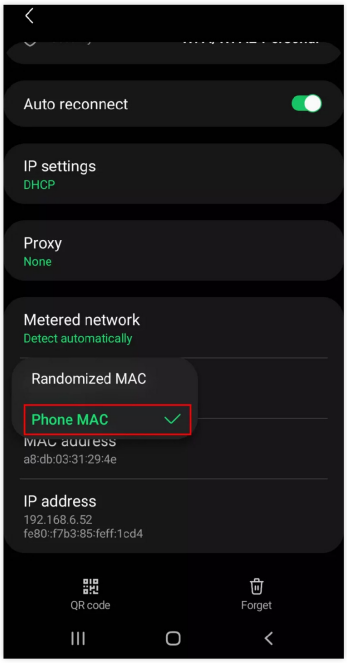
1. **Go to** `Settings` > `Network & Internet` > `Wi-Fi` .
2. Tap on your **connected network**.
3. Tap `Privacy` or `MAC Address Type` .
4. Select **Use device MAC** instead of `Use randomized MAC` .



Disable Random MAC Address – Stock Android

Samsung® Devices:

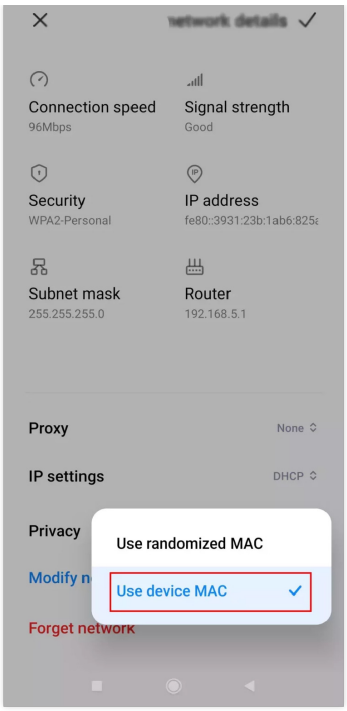
1. **Go to** `Settings` > `Connections` > `Wi-Fi` .
2. Tap on your **connected network**.
3. Scroll to `MAC Address Type` .
4. Select **Phone MAC** instead of `Randomized MAC` .



Disable Random MAC Address – Samsung® Devices:

Xiaomi Devices:

1. **Go to** `Settings` > `Wi-Fi` .
2. Tap on your **connected network**.
3. Scroll down to `Privacy` .
4. Select **Use device MAC** instead of `Use randomized MAC` .

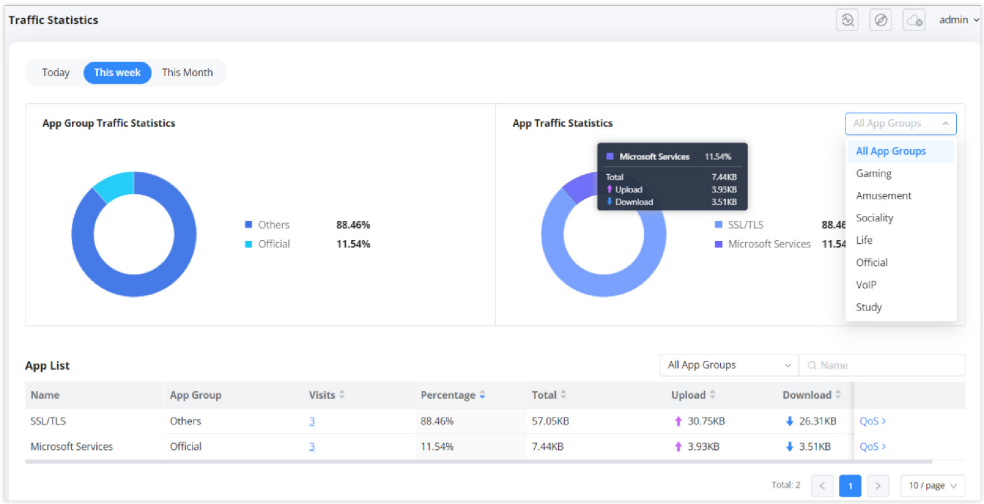


Disable Random MAC Address – Xiaomi Devices:

Traffic Management

Traffic Statistics

The **Traffic Statistics** page on the GWN7062E/T router provides detailed insights into network traffic usage. This section helps users monitor bandwidth consumption by different applications and categorize traffic usage over time. Users can filter traffic by application groups, review real-time data usage, and set QoS rules based on traffic patterns.



Traffic Statistics page

Accessing the Traffic Statistics Page:

1. Navigate to **Advanced** → **Traffic Management** → **Traffic Statistics** in the left sidebar.
2. The page displays two main charts:
   - **App Group Traffic Statistics**: A pie chart showing traffic distribution across different application categories.
   - **App Traffic Statistics**: A breakdown of specific applications contributing to network usage.

Filtering Traffic Data:

- Users can filter traffic data based on **time periods**:
  - **Today**
  - **This Week**

    - **This Month**
- The right-side drop-down menu allows filtering by **App Groups**, including:
    - Gaming
    - Amusement
    - Sociality
    - Life
    - Official
    - VoIP
    - Study

Viewing Application Traffic Details:

- Hovering over the **App Traffic Statistics** chart reveals detailed upload and download statistics for each application.
- The **App List** table provides:
    - Application Name
    - Traffic Category (App Group)
    - Number of Visits
    - Percentage of Total Traffic
    - Total Data Usage (Upload & Download)

Accessing QoS Settings:

- Each application entry includes a **QoS** link that allows users to configure Quality of Service rules for better traffic management.

QoS

The **QoS (Quality of Service) feature** on the GWN7062E(T) router enables users to optimize and control network traffic based on priority settings. It allows for the allocation of bandwidth to specific applications, clients, or traffic types, ensuring better performance for critical services like gaming, VoIP, and streaming. Users can configure QoS rules based on traffic type, application, or device priority.

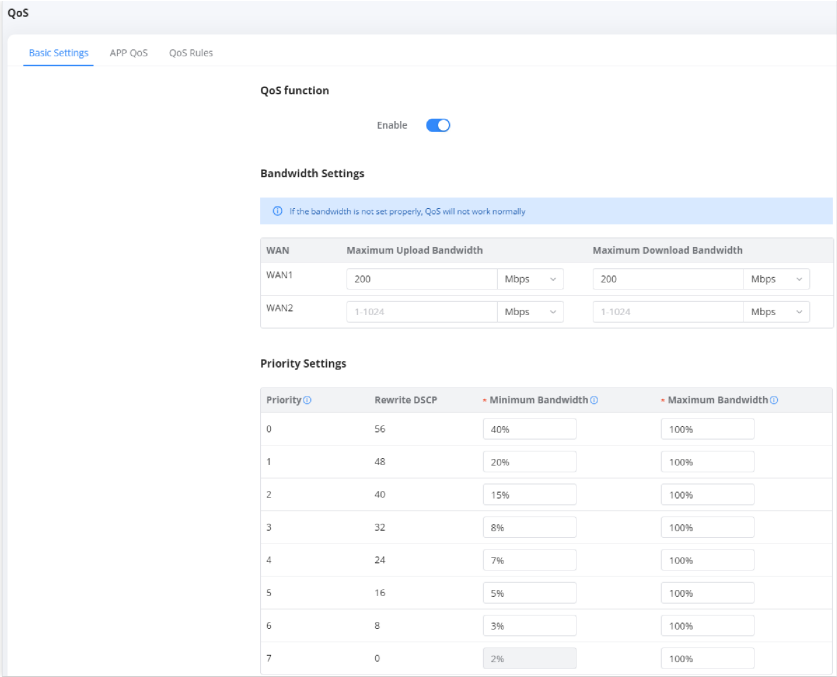
Accessing the QoS Settings:

- Navigate to **Advanced > Traffic Management > QoS** to access the QoS settings.
- The QoS page consists of three main tabs:
    - **Basic Settings** – Enables QoS and sets bandwidth limits.
    - **APP QoS** – Allows setting priority levels for application categories.
    - **QoS Rules** – Defines custom rules for prioritizing specific clients, applications, or domains

Enabling QoS and Setting Bandwidth (Basic Settings):

- **Enable QoS:** Toggle the switch to activate QoS.
- **Set Maximum Bandwidth:**
    - Users can define upload and download speed limits for WAN1 and WAN2 connections.
- **Configure Priority Settings:**
    - Assign priority levels (0 to 7), minimum bandwidth, and rewrite **DSCP (Differentiated Services Code Point)** values to optimize traffic flow.

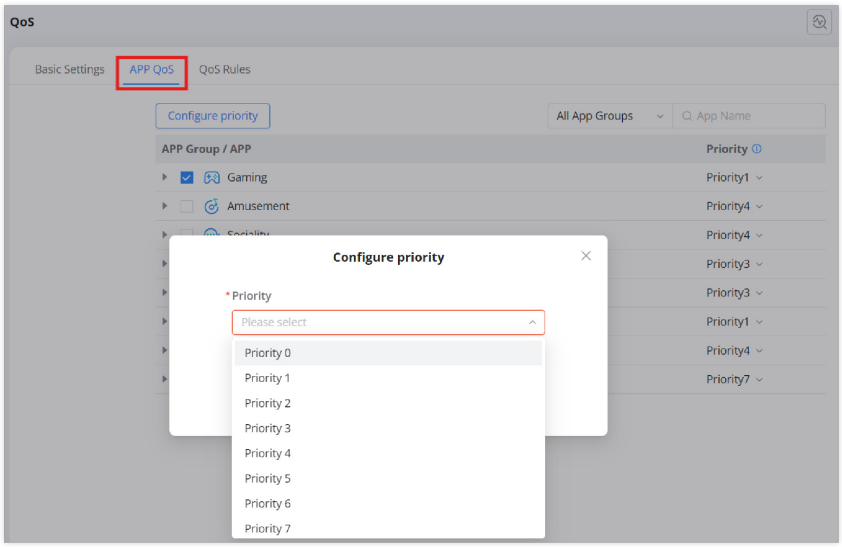
Important Note: If bandwidth settings are not configured properly, QoS will not function as expected.



QoS – Basic Settings

Configuring APP QoS:

- Navigate to the **APP QoS** tab.
- Click **"Configure Priority"** to assign a priority level to different application groups or individual applications.
- The available priority levels range from **Priority 0 (highest) to Priority 7 (lowest)**.
- Users can classify traffic based on categories such as:
  - **Gaming**
  - **VoIP**
  - **Social Media**
  - **Streaming**
  - **Work & Study**
- Selecting a higher priority ensures better bandwidth allocation for critical applications.



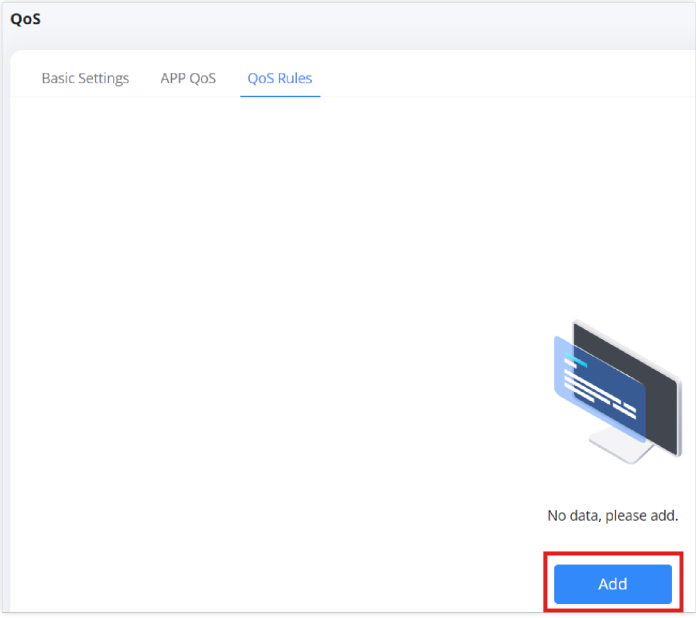
QoS – App QoS

Adding a Custom QoS Rule:

- Go to the **QoS Rules** tab.
- Click **"Add"** to create a new QoS rule.
- Configure the following parameters:
  - **Name:** Enter a descriptive rule name.

- **Source:** Choose between **all clients**, **specific clients**, or an **IP address**.
- **Destination:** Select **All Traffic**, **Applications**, or **Domain**.
- **Apps:** If applicable, select the app or app category to prioritize.
- **Priority:** Assign a priority level from **0 (highest) to 7 (lowest)**.
- **Rewrite DSCP:** Adjust DSCP settings if necessary.

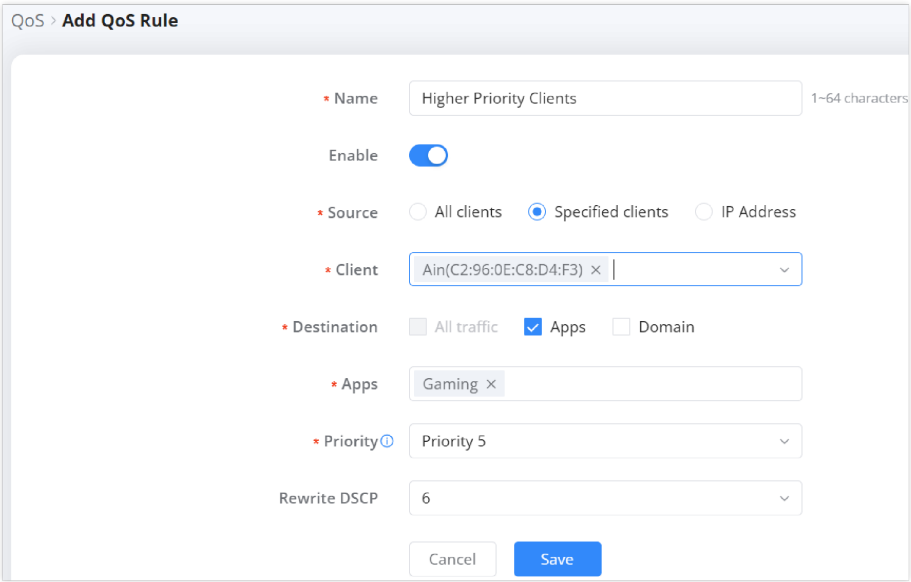
- Click **"Save"** to apply the rule.



QoS Rules page

- Configure the following parameters:
  - **Name:** Enter a descriptive rule name.
  - **Source:** Choose between **all clients**, **specific clients**, or an **IP address**.
  - **Destination:** Select **All Traffic**, **Applications**, or **Domain**.
  - **Apps:** If applicable, select the app or app category to prioritize.
  - **Priority:** Assign a priority level from **0 (highest) to 7 (lowest)**.
  - **Rewrite DSCP:** Adjust DSCP settings if necessary.

- Click **"Save"** to apply the rule.



QoS – Add QoS Rule

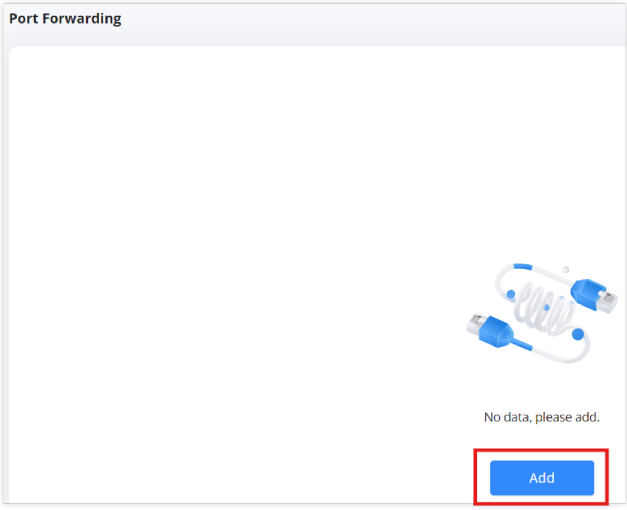
NAT

Port Forwarding

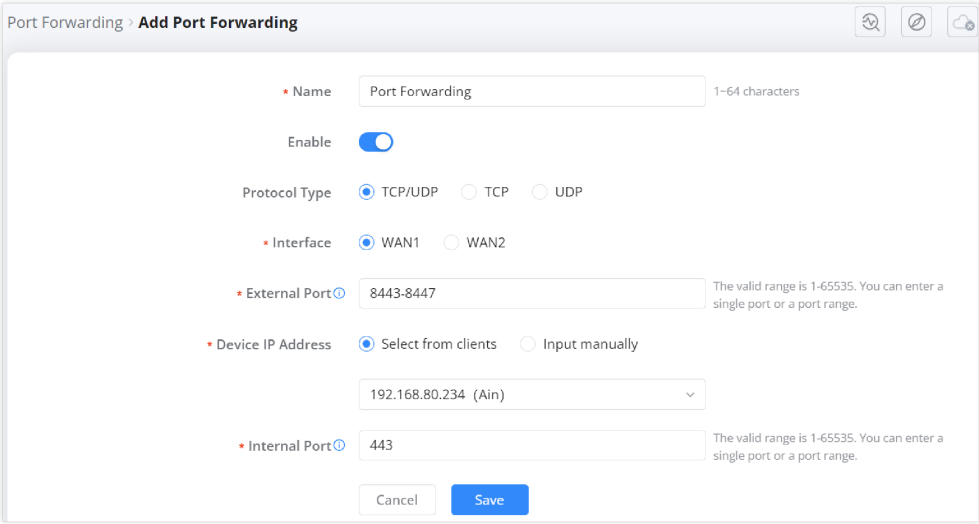
Port forwarding is a feature that allows external devices to communicate with devices on a local network through a specific port or range of ports. This is essential for hosting services such as web servers, gaming servers, or remote access applications. By configuring port forwarding, users can direct incoming network traffic from the WAN (Wide Area Network) to a designated IP address within the LAN (Local Area Network).

Accessing the Port Forwarding Page:

1. **Navigate to the Router's Web Interface**
   - Log in to the **GWN7062E(T) Web UI**.
   - From the **left-side menu**, expand the **NAT** section.
   - Click on **Port Forwarding**.
2. **Adding a New Port Forwarding Rule**
   - On the **Port Forwarding page**, click the **"Add"** button to create a new forwarding rule.



Port Forwarding page



Add Port Forwarding

Configuring the Port Forwarding Rule:

- **Name:** Enter a descriptive name for the rule (e.g., "Web Server").
- **Enable:** Toggle the switch to enable or disable the rule.
- **Protocol Type:** Select the desired protocol:
  - **TCP/UDP** (both protocols)

    - **TCP only**
    - **UDP only**
- **Interface:** Choose the WAN interface for this rule (**WAN1 or WAN2**).
- **External Port:** Specify the external port(s) that will receive incoming traffic.
  Note: The external port should be within the valid range of **1-65535**.
- **Device IP Address:** Select a target device from the list of connected clients or manually enter the IP address of the internal device.
- **Internal Port:** Specify the internal port(s) where traffic should be forwarded.
  Note: If a range of ports is used, the internal and external port ranges must match.

Understanding the Port Forwarding Notes:

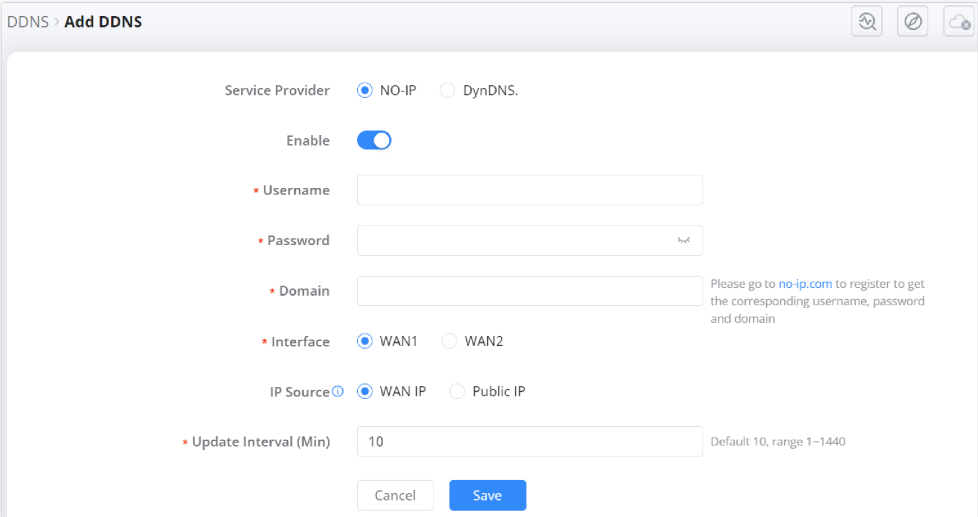
- **External Port Note:** This port is open to the internet, allowing external users to send requests.
- **Internal Port Note:** This is the destination port inside the local network. If a port range is specified, the difference between the starting and ending ports must remain consistent.

DDNS

Dynamic DNS (DDNS) allows users to associate a domain name with a changing dynamic IP address. This feature is useful for users who host services at home or in environments where the public IP address frequently changes. By enabling DDNS, users can access their network remotely using a domain name instead of remembering a changing IP address.

Accessing the DDNS Settings:

1. **Login to the Router Web UI.**
2. **Navigate to NAT → DDNS.**
3. Click on **"Add"** to configure a new DDNS entry.



DDNS

Configuring DDNS:

1. **Service Provider:**
   - Select a supported DDNS service provider:
     - **NO-IP**
     - **DynDNS**
   - Users must have an account with the chosen provider.
2. **Enable DDNS:**
   - Toggle the **Enable** switch to activate DDNS.
3. **Account Credentials:**
   - **Username:** Enter the registered username from the DDNS provider.

- **Password:** Enter the corresponding password.
- **Domain:** Input the registered DDNS domain (e.g., `myrouter.no-ip.com`).

4. **Interface Selection:**
   - Choose the WAN interface to associate with the DDNS:
     - **WAN1**
     - **WAN2**

5. **IP Source:**
   - Choose how the IP address should be obtained:
     - **WAN IP** (Default) – Uses the router's WAN IP.
     - **Public IP** – Uses the detected public-facing IP.

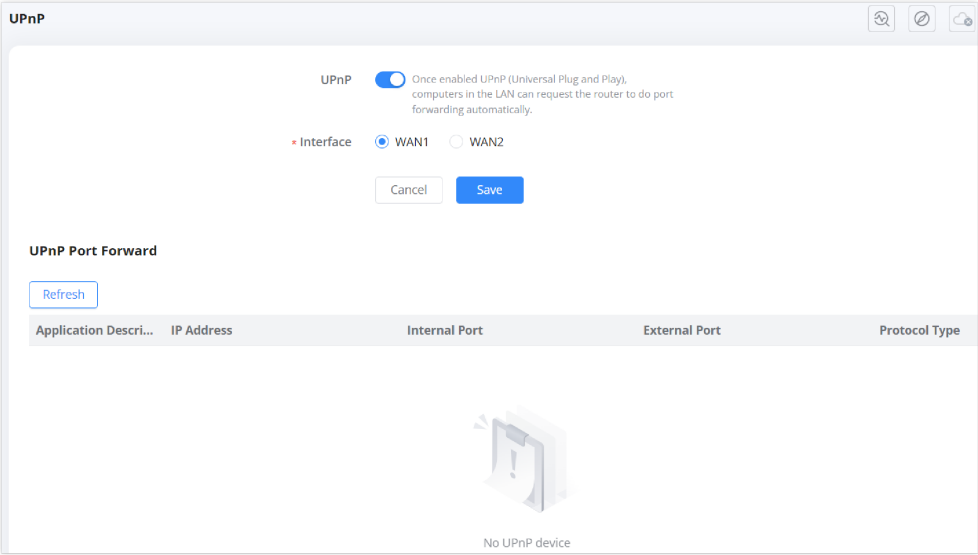
6. **Update Interval:**
   - Set the frequency for updating the DDNS record.
   - Default: **10 minutes** (Range: **1 – 1440 minutes**).

UPnP

Universal Plug and Play (UPnP) is a feature that allows devices on a local network to automatically configure port forwarding on the router. This is useful for applications such as online gaming, video conferencing, and peer-to-peer connections, where port forwarding is required for seamless communication.

Accessing the UPnP Settings:

1. **Login to the Router Web UI.**
2. **Navigate to NAT → UPnP.**
3. The UPnP settings page will be displayed.



UPnP

Configuring UPnP:

1. **Enable UPnP:**
   - Toggle the **UPnP** switch to activate the feature.
   - Once enabled, devices on the LAN can request the router to handle port forwarding automatically.

2. **Select the Interface:**
   - **WAN1** (default) or **WAN2** can be chosen for UPnP operation.

3. **Saving the Configuration:**
   - Click **"Save"** to apply the changes.

Security Considerations:

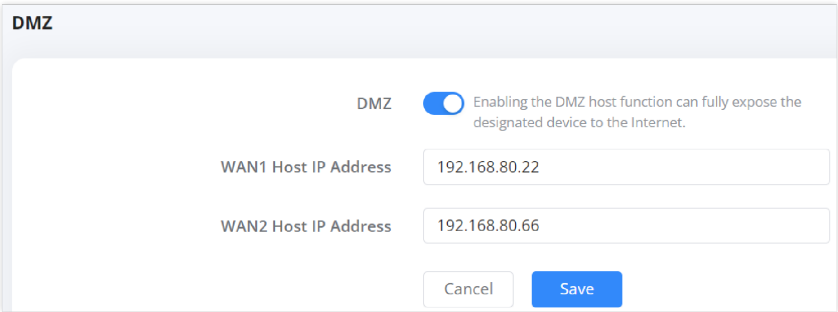
- While UPnP simplifies port forwarding, it may pose security risks if enabled without proper monitoring.
- It is recommended to **disable UPnP** if not actively used to prevent unauthorized applications from opening ports.
- Users can manually configure port forwarding for more control over network security.

DMZ

The **DMZ (Demilitarized Zone)** feature allows a device on the local network to be fully exposed to the internet, bypassing firewall protection. This is typically used for applications that require unrestricted access, such as gaming consoles, web servers, or VoIP devices.

Accessing the DMZ Settings:

1. **Login to the Router Web UI.**
2. **Navigate to NAT → DMZ.**
3. The DMZ settings page will be displayed.



DMZ

Configuring the DMZ:

1. **Enable the DMZ Function:**
   - Toggle the **DMZ** switch to activate this feature.
   - Once enabled, the specified device will be fully exposed to the internet.
2. **Enter the DMZ Host IP Address:**
   - For **WAN1**, enter the internal IP address of the device you wish to expose.
   - If using **WAN2**, enter the corresponding IP address for that network.

Security Considerations:

- The **DMZ host is vulnerable** to external attacks since it is directly exposed to the internet.
- It is **recommended to use DMZ only when necessary** and for trusted devices.
- For enhanced security, consider **using Port Forwarding** instead of DMZ for specific applications.
- Ensure the DMZ host has a **strong firewall and security measures** in place.

Security

Security Firewall

The **Security Firewall** section allows users to configure and monitor security settings to protect the router and connected devices from potential threats. This section is divided into two key areas:

- **Defense Settings**
- **Defense Statistics**

To access the Security Firewall settings:

1. Navigate to **Security** from the left-side menu.

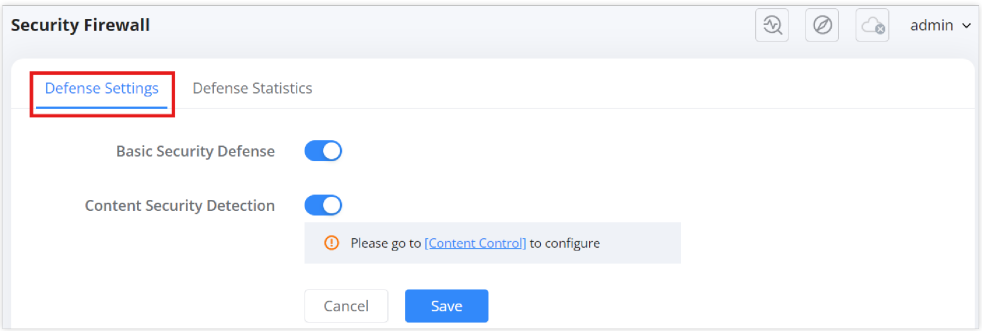
2. Click on **Security Firewall**.

Defense Settings:

The **Defense Settings** tab allows users to enable or disable core security features.

- **Basic Security Defense**: This feature enhances network security by providing fundamental protection against common threats.
- **Content Security Detection**: When enabled, this feature allows users to configure content filtering and security settings via the **Content Control** section.

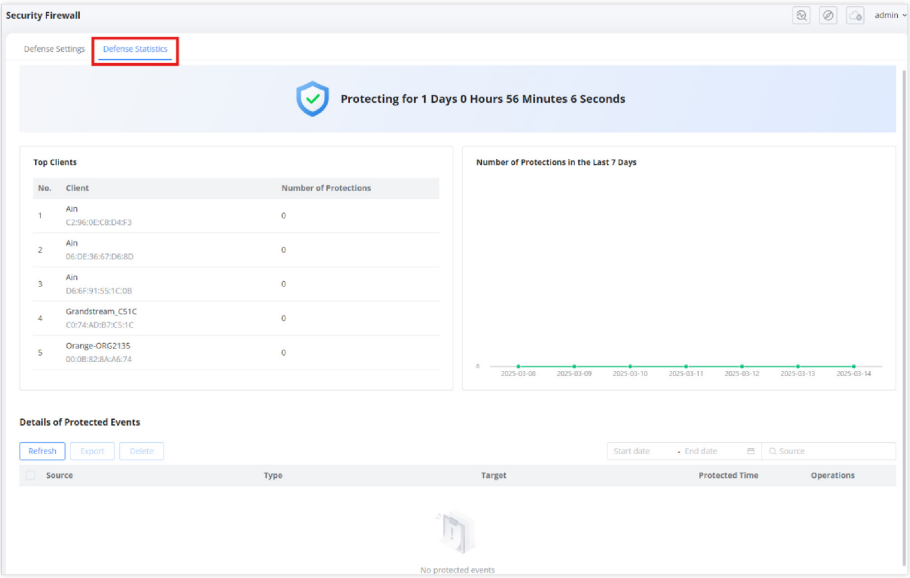
> **Note:**
>
> If Content Security Detection is enabled, users must configure content control settings separately by navigating to Security > Content Control.



Security Firewall – Defense Settings

Defense Statistics

The **Defense Statistics** tab provides real-time data on the router's security protections.



Security Firewall – Defense Statistics

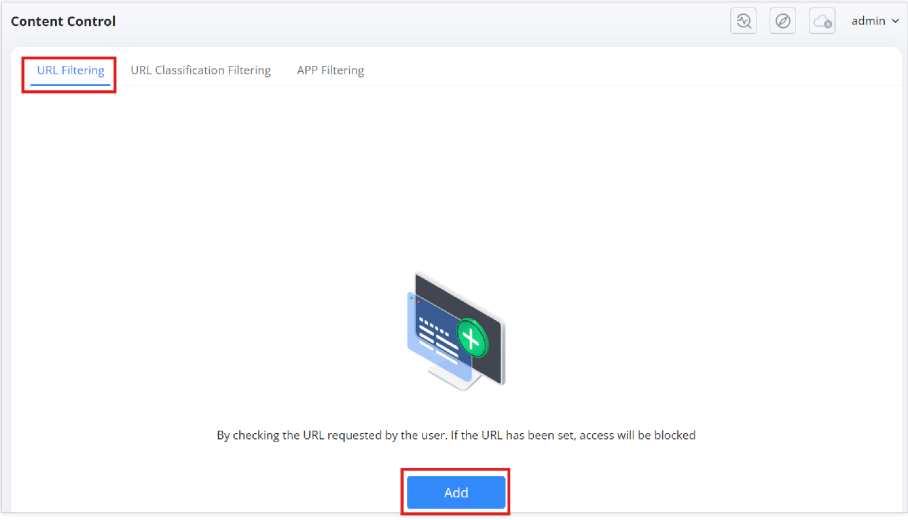
Key Metrics in Defense Statistics:

- **Protection Duration**: Displays how long the security system has been actively protecting the network.
- **Top Clients**: Lists connected clients along with the number of security protections applied.
- **Number of Protections in the Last 7 Days**: A graphical representation of security events over the past week.
- **Details of Protected Events**: Displays a log of security events, including source, type, target, and protection time.

Content Control

The **Content Control** section allows administrators to manage and restrict network access to websites and applications based on predefined filters and categories. This feature is useful for network security, parental controls, and workplace productivity.

To access the **Content Control** page, navigate to: **Security** → **Content Control**



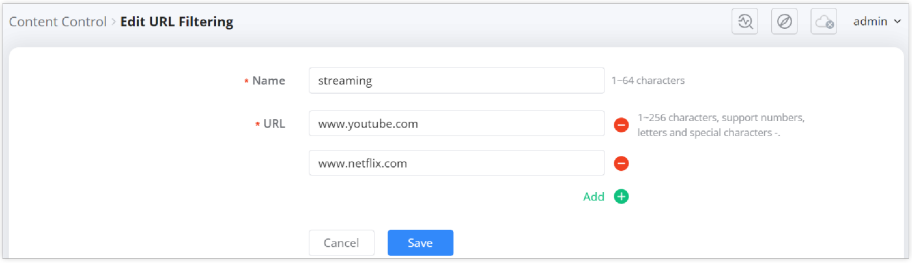
Content Control page

URL Filtering

URL Filtering enables administrators to manually specify websites that should be blocked on the network.

1. Click on the **"Add"** button.
2. Enter a **Name** for the filter rule.
3. Specify one or more URLs (e.g., `www.youtube.com`, `www.netflix.com`).
4. Click **"Save"** to apply the rule.

Once added, all clients connected to the network will be restricted from accessing the specified websites.



Content Control – Add URL Filtering

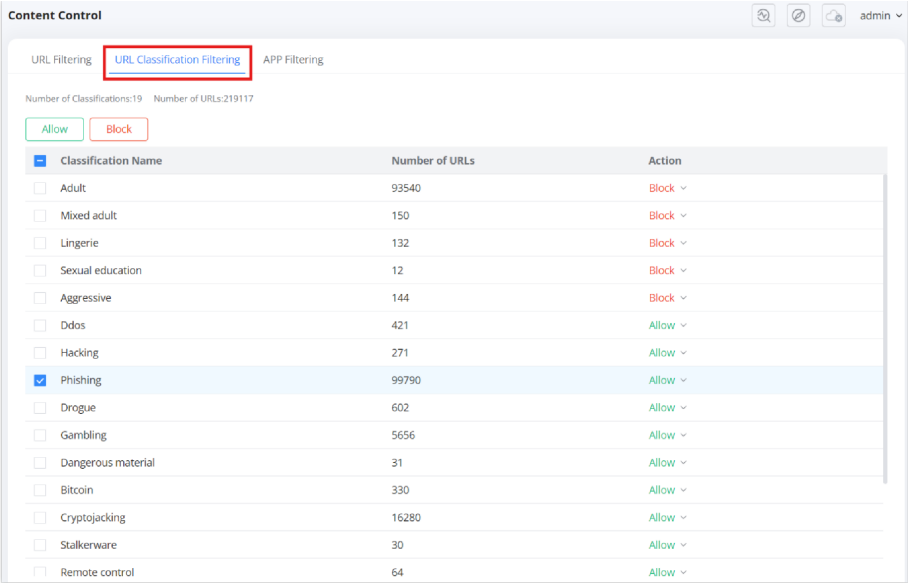
URL Classification Filtering

This feature provides category-based website filtering, allowing administrators to block or allow predefined groups of websites.

Blocking or Allowing Categories

1. Navigate to the **URL Classification Filtering** tab.
2. A list of categories such as **Adult, Phishing, Gambling, Hacking, Cryptojacking, etc.** will be displayed.
3. To block a category, select **"Block"** in the action column.
4. To allow access to a category, select **"Allow"**.

This method is efficient for restricting entire categories instead of entering URLs manually.



Content Control – URL Classification Filtering

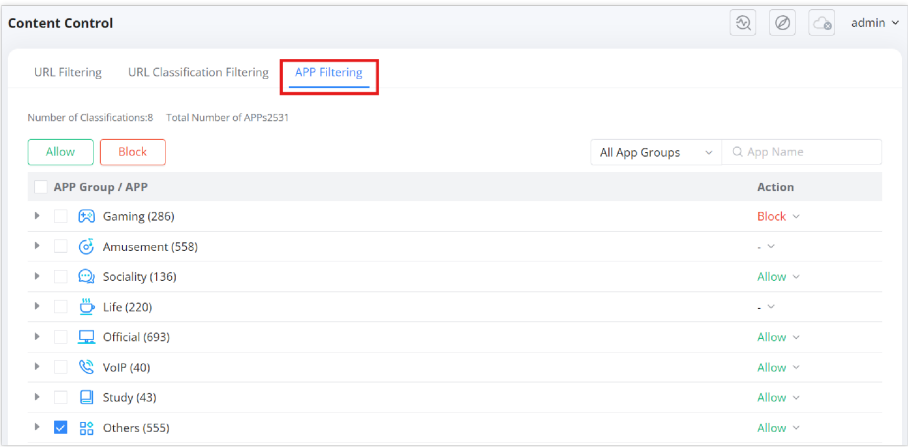
App Filtering

App Filtering allows administrators to control access to applications based on their category or specific application names.

Blocking or Allowing Applications:

1. Navigate to the **App Filtering** tab.
2. A list of categories such as **Gaming, Sociality, VoIP, Study, Official, etc.** will be displayed.
3. Expand a category to view specific applications.
4. Choose **"Block"** or **"Allow"** for each application or entire category.

This feature is useful for blocking non-work-related applications such as gaming, streaming, or social media.

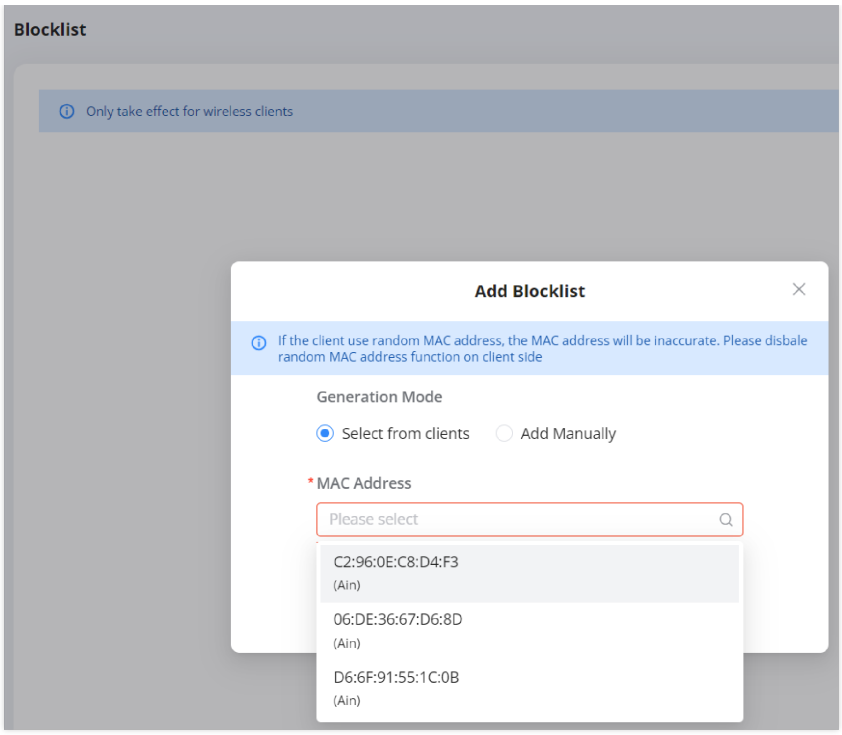


Content Control – App Filtering

Blocklist

The **Blocklist** feature allows administrators to block specific wireless clients from connecting to the network. This is useful for restricting access to unauthorized devices or managing network security.

To access the **Blocklist** page, navigate to: **Security** → **Blocklist**



blocklist

Adding a Device to the Blocklist:

1. Click on the **"Add"** button.
2. Choose a **Generation Mode**:
   - **Select from clients** – Choose a MAC address from a list of currently connected devices.
   - **Add Manually** – Enter the MAC address of the device manually.
3. Select or enter the **MAC Address** of the client device.
4. Click **"Save"** to block the selected device.

Note: This feature **only affects wireless clients**. Wired clients will not be blocked.

> **Important:**
>
> This feature requires devices to have a static MAC address to function properly. If your device is using a random MAC address, certain functions may not work as expected. To ensure compatibility, follow the steps in Disabling Client Random MAC Address to disable the random MAC feature on your device.

VPN

The **VPN (Virtual Private Network)** feature on the GWN7062E(T) router allows users to create secure connections between remote locations or clients over the internet. The router supports multiple VPN protocols, providing flexibility and security based on network requirements.

Supported VPN Protocols

The GWN7062E(T) router supports the following VPN protocols:

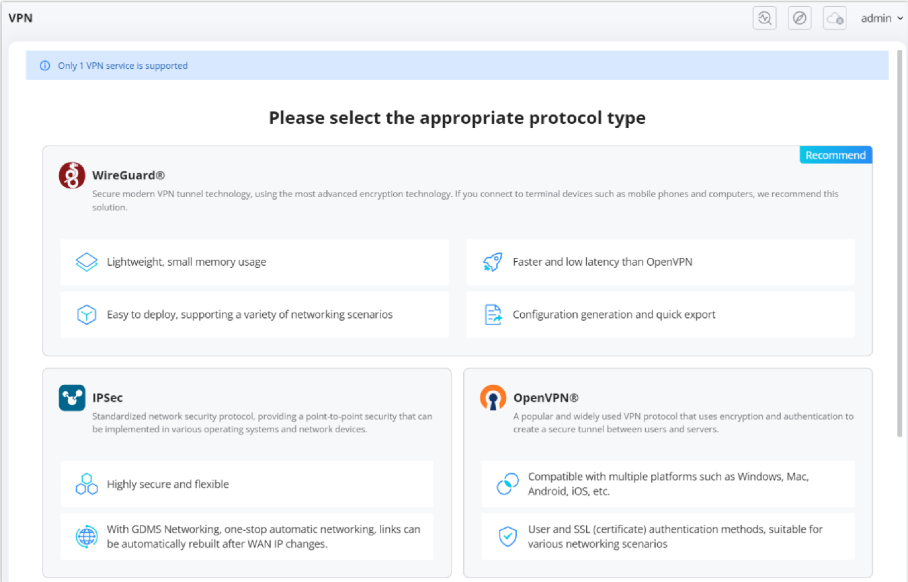
1. **WireGuard® (Recommended)**
   - Secure and modern VPN technology using advanced encryption.
   - Faster and lower latency compared to OpenVPN.
   - Lightweight with minimal memory usage.
   - Easy configuration with quick export options.
2. **IPSec**

- Standardized network security protocol for point-to-point security.
- Highly secure and flexible.
- Integrates with GDMS Networking for automatic WAN IP updates.

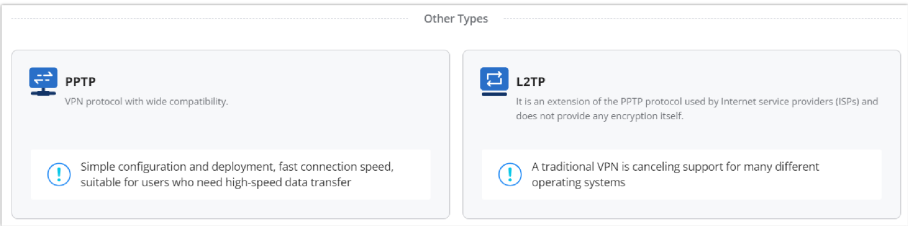
3. **OpenVPN®**
   - A widely used VPN protocol with encryption and authentication features.
   - Compatible with multiple platforms (Windows, Mac, Android, iOS).
   - Supports user authentication via SSL certificates.

4. **PPTP**
   - Simple and easy-to-deploy VPN solution.
   - Fast connection speeds suitable for high-speed data transfer.
   - Broad compatibility with older systems.

5. **L2TP**
   - Extension of PPTP, often used by ISPs.
   - Does not provide encryption itself.
   - Less commonly supported by modern VPN setups.



VPN Setup Wizard – part 1



VPN Setup Wizard – part 2

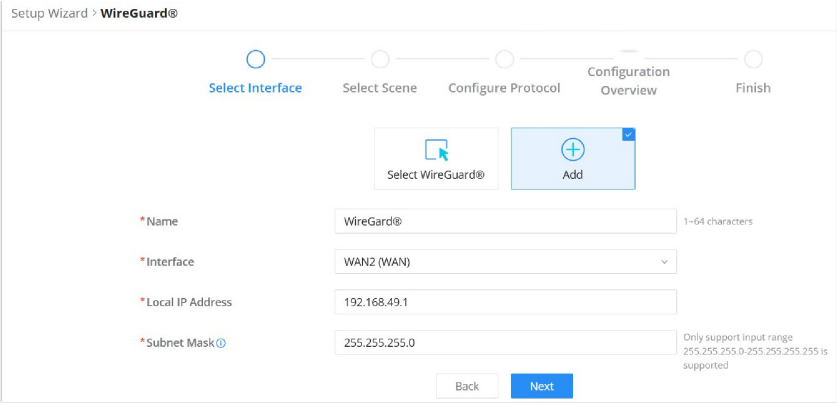
VPN-Type Specific:

The wizard is tailored for each VPN type. For instance:

- **WireGuard®**: Prioritizes fast, low-latency connections with a simple and secure setup.
- **IPSec**: Provides robust encryption and secure communication for both site-to-site and client-to-site scenarios.
- **OpenVPN®**: Allows more customizable security options, such as user-based certificate management and SSL encryption.
- **PPTP/L2TP**: While legacy protocols, these are supported for backward compatibility with older devices and systems.

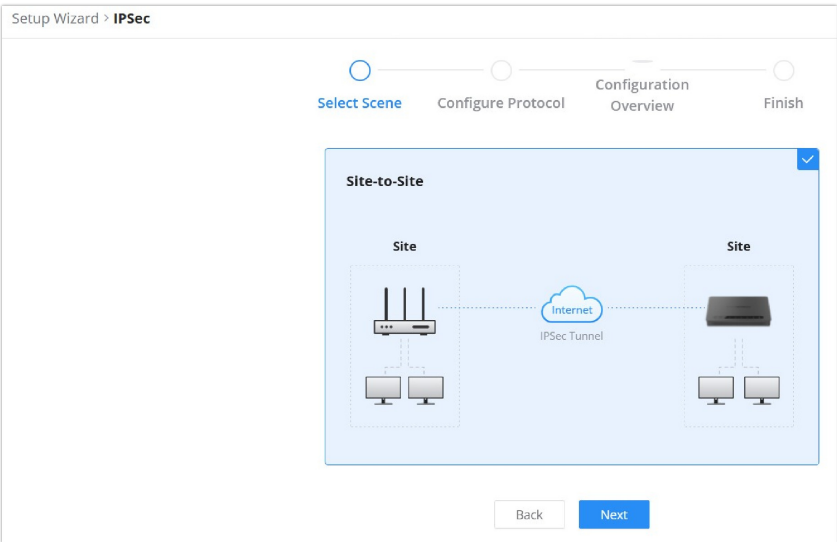
By following this wizard, users can rapidly configure the required VPN connections without needing to navigate complex settings manually, making it an ideal solution for businesses looking to enhance security without complexity.

- **WireGuard® Setup Wizard**



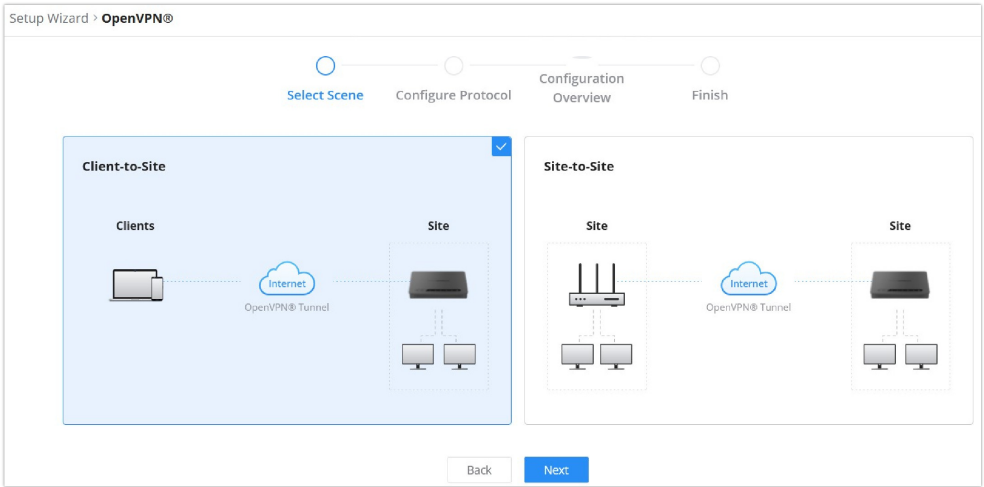
WireGuard® Example

- **IPSec Setup Wizard**



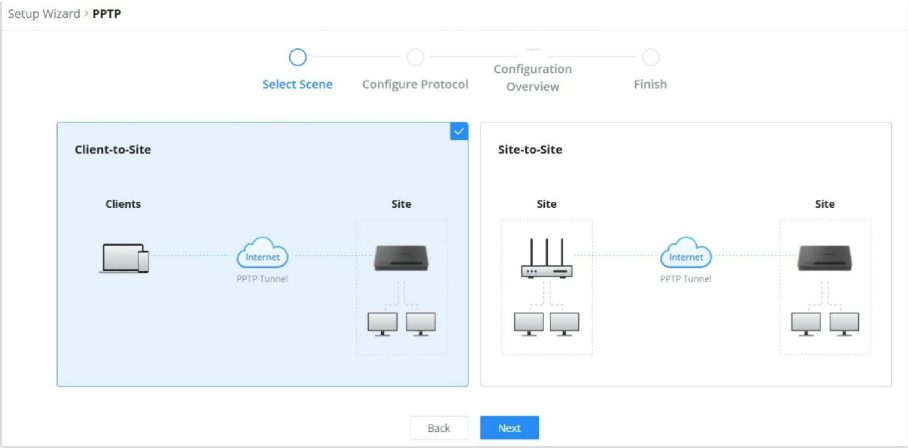
IPSec Example

- **OpenVPN® Setup Wizard**



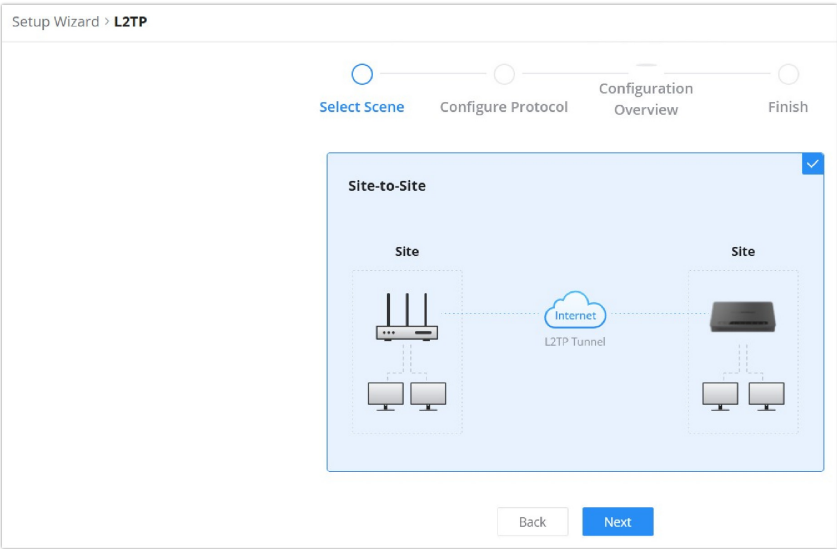
OpenVPN® Example

- **PPTP Setup Wizard**



PPTP Example

- **L2TP Setup Wizard**



L2TP Example

For more details on how to configure VPN, please refer to this guide: VPN Guide

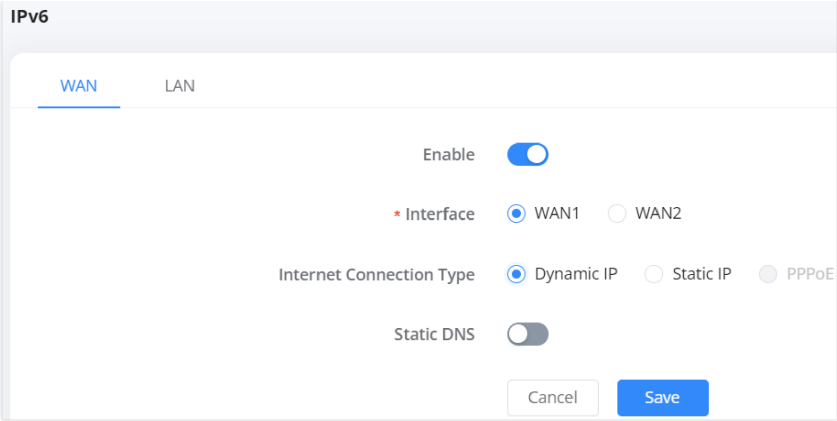
IPv6

The GWN7062E(T) router supports IPv6 networking, allowing users to configure WAN and LAN settings for next-generation Internet Protocol connectivity. IPv6 provides a larger address space, improved security, and better support for modern networking needs. The configuration interface for IPv6 is accessible via the router's web UI under **Advanced** → **IPv6**.

WAN

The **WAN IPv6 settings** control how the router connects to the Internet using IPv6. This section includes the following options:

- **Enable** – Toggle to enable or disable IPv6 for the WAN interface.
- **Interface Selection** – Choose WAN port (e.g, **WAN1** or **WAN2**) to specify which WAN port should use IPv6.
- **Internet Connection Type**:
  - **Dynamic IP (Default)**: The router automatically obtains an IPv6 address from the ISP.
  - **Static IP**: Manually configure a fixed IPv6 address.
  - **PPPoE**: Used if the ISP requires PPPoE authentication for IPv6.
- **Static DNS** – If enabled, allows users to specify custom IPv6 DNS servers for name resolution.
- **Save** – Click to apply changes.

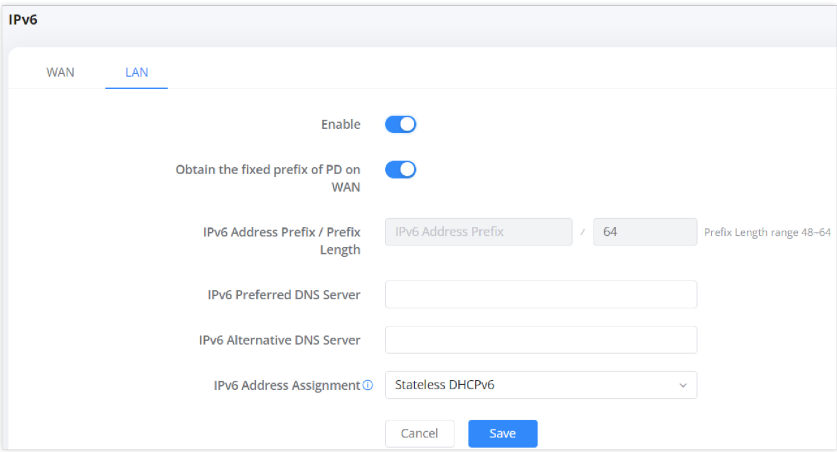


IPv6 – WAN

LAN

The **LAN IPv6 settings** determine how IPv6 addresses are assigned to devices within the local network. This section includes:

- **Enable** – Toggle to enable IPv6 on the LAN network.
- **Obtain the Fixed Prefix of PD on WAN** – If enabled, the router will automatically use the IPv6 prefix assigned by the ISP.
- **IPv6 Address Prefix / Prefix Length** – Defines the IPv6 network prefix for LAN devices.
  - The prefix length can be set between **48 and 64 bits**.
- **IPv6 Preferred DNS Server** – Manually specify the primary IPv6 DNS server.
- **IPv6 Alternative DNS Server** – Set a secondary DNS server for redundancy.
- **IPv6 Address Assignment**:
  - **Stateless DHCPv6** (Default) – The router assigns IPv6 addresses without requiring a DHCP server.
  - Other options may include **Stateful DHCPv6** or **SLAAC**, depending on network requirements.
- **Save** – Click to apply changes.



IPv6 – LAN

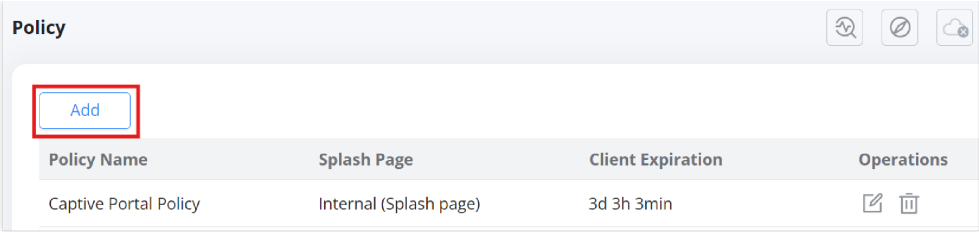
Captive Portal

Policy

The **Captive Portal Policy** feature allows administrators to define access policies for users connecting to the network via a captive portal. These policies can be applied to SSIDs when setting up Wi-Fi access, ensuring that users are prompted with a login or terms acceptance page before gaining internet access.

Located under **Advanced** → **Captive Portal** → **Policy**, this section displays existing captive portal policies and allows the creation of new ones.

To create a new policy, click the **"Add"** button.



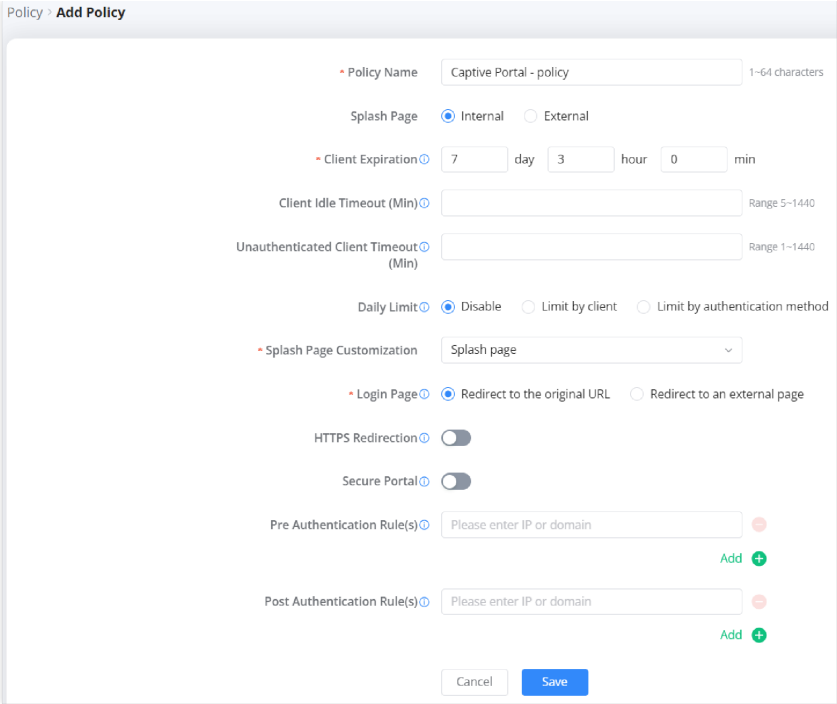
Add a Policy rule

Creating a New Captive Portal Policy:

After clicking **"Add"**, the configuration page appears with several customizable settings:

1. **Policy Name**: Define a unique name for the captive portal policy.
2. **Splash Page**: Choose between:
   - **Internal**: Uses the built-in splash page.
   - **External**: Redirects users to an external captive portal.
3. **Client Expiration**: Set the duration for which users remain authenticated before requiring re-authentication.
4. **Client Idle Timeout (Optional)**: Defines the time (in minutes) after which inactive clients are disconnected.
5. **Unauthenticated Client Timeout (Optional)**: Specifies how long an unauthenticated client can remain connected before being disconnected.
6. **Daily Limit**:
   - **Disable**: No limits are applied.
   - **Limit by client**: Restricts access per client.
   - **Limit by authentication method**: Restricts access based on authentication type.
7. **Splash Page Customization**: Select the type of splash page to display.
8. **Login Page Redirection**:
   - **Redirect to the original URL**: After authentication, users are redirected to the page they initially requested.
   - **Redirect to an external page**: After authentication, users are redirected to a specified URL.
9. **HTTPS Redirection**: If enabled, all HTTP traffic will be redirected to HTTPS.
10. **Secure Portal**: Enabling this ensures encrypted connections for the captive portal.
11. **Pre-Authentication Rules**: Allows defining specific IPs or domains that users can access before authentication.
12. **Post-Authentication Rules**: Defines accessible resources after authentication.

Once configured, click **"Save"** to apply the policy.



Add/Edit Policy Rule

Applying a Captive Portal Policy:

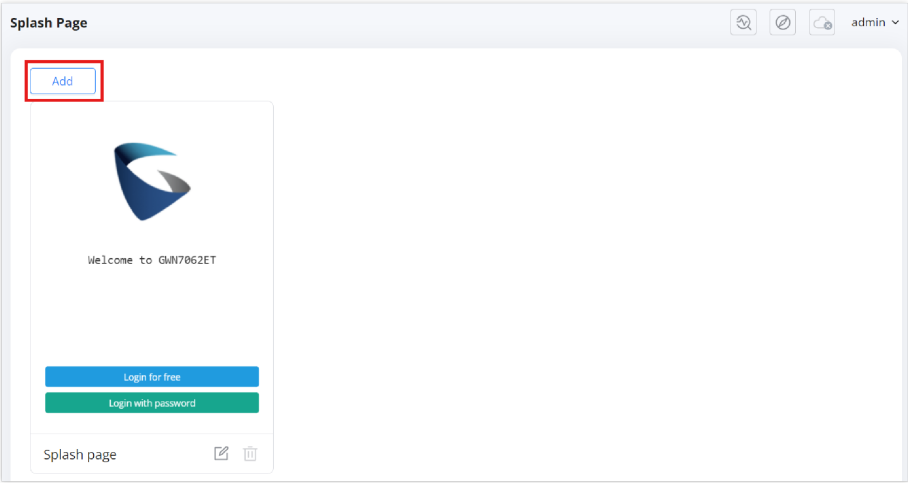
After creating a captive portal policy, it can be assigned to an SSID in the **Wi-Fi Settings** section. Users connecting to this SSID will be required to authenticate via the defined captive portal policy before accessing the network.

This feature helps administrators enforce security and access controls effectively, ensuring compliance with network policies.

Splash Page

The **Splash Page** is a customizable web-based login interface that appears when users connect to a Wi-Fi network using a **Captive Portal Policy**. This page is used for authentication and can be configured with different login methods.

Go to **Advanced** → **Captive Portal** → **Splash Page** in the router's Web UI.



Splash page

Splash Page Components:

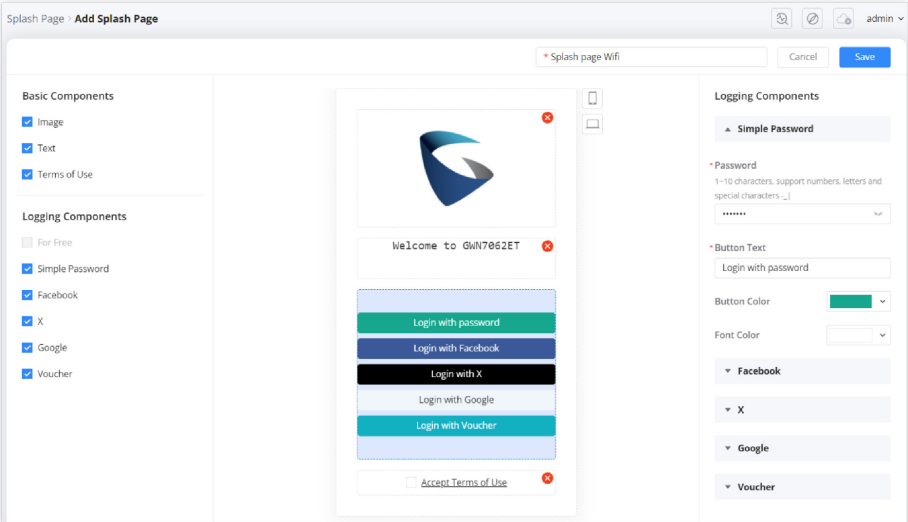
When adding a splash page, users can customize various elements, including:

- **Basic Components**
  - **Image**: Upload a custom logo or branding.
  - **Text**: Display a welcome message.
  - **Terms of Use**: Optionally require users to accept terms before accessing the network.

- **Login Components**
  - **For Free**: Allows open access without authentication.
  - **Simple Password**: Users enter a pre-configured password.
  - **Facebook Login**: Authenticate using a Facebook account.
  - **X (formerly Twitter) Login**: Authenticate using an X (Twitter) account.
  - **Google Login**: Authenticate using a Google account.
  - **Voucher Login**: Users enter a generated voucher code.

Customization Options:

- **Button Text & Colors**: Customize login button text, colors, and styles.
- **HTTPS Redirection**: Enable/disable HTTPS redirection for security.
- **Secure Portal**: Enhances security for the login page.



Add splash page

Using Splash Page with Captive Portal Policy:

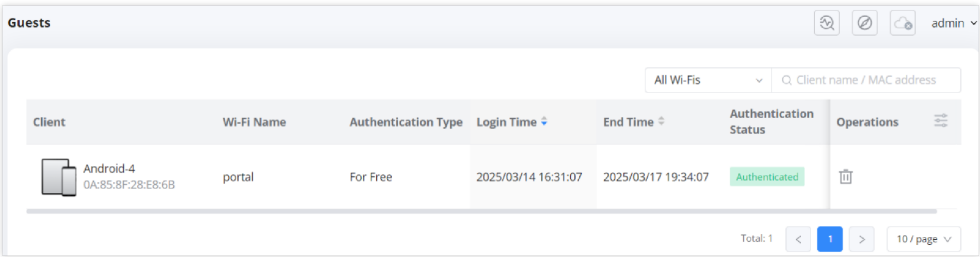
Once created, a splash page can be assigned to a **Captive Portal Policy**, which is then linked to an SSID in **Wi-Fi Settings**. This ensures that users connecting to the Wi-Fi network will be redirected to the splash page for authentication.

Guests

The **Guests Page** provides an overview of all users who have connected to the network using a **Captive Portal Policy**. This page displays authentication details for clients who accessed Wi-Fi SSIDs configured with a captive portal.

Navigating to the Guests Page:

- Go to **Advanced** → **Captive Portal** → **Guests** in the router's Web UI.



Guests

Guest Information Displayed:

The **Guests Page** lists details of connected clients, including:

- **Client**: The device name and MAC address.

- **Wi-Fi Name**: The SSID (Wi-Fi network) the client connected to.
- **Authentication Type**: The method used to authenticate (e.g., “For Free,” “Simple Password,” “Facebook,” etc.).
- **Login Time**: The timestamp when the client successfully authenticated.
- **End Time**: The expiration time of the authentication session.
- **Authentication Status**: Indicates whether the client is currently authenticated or not.

Filtering and Managing Guests:

- Use the search bar to filter guests by **Wi-Fi SSID** or **Client Name/MAC Address**.
- Click the **Trash Bin** icon under “Operations” to remove or disconnect a guest from the network.

Use Case:

This page is useful for administrators to:

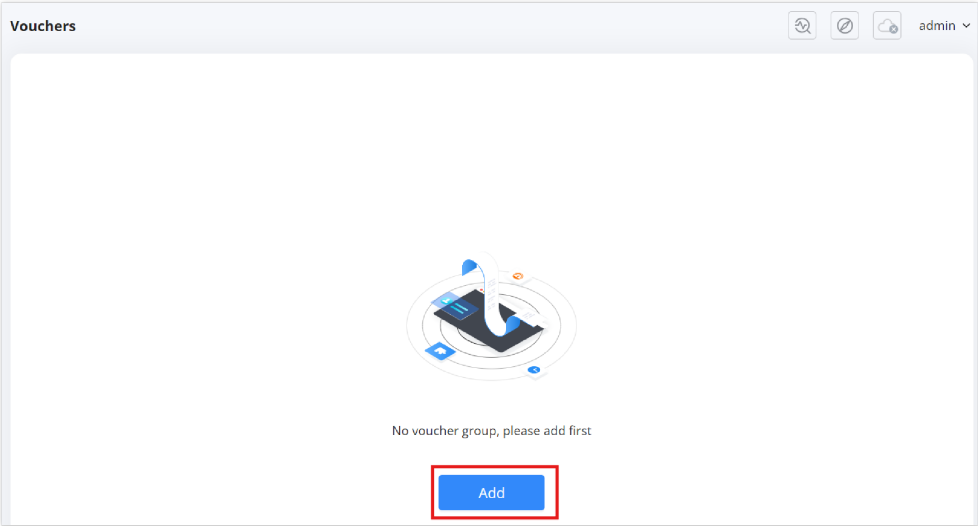
- Monitor guest connections in real-time.
- Manage authentication sessions for different users.
- Identify and troubleshoot access issues.

Vouchers

The **Vouchers** feature is part of the **Captive Portal** system. Vouchers allow administrators to generate access codes that can be distributed to users for temporary or controlled internet access. These vouchers can be linked to a **Splash Page**, which in turn is applied to a **Captive Portal Policy** and assigned to a Wi-Fi SSID.

Navigating to the Vouchers Page:

To configure vouchers, go to: **Advanced** → **Captive Portal** → **Vouchers**
This page displays the list of generated voucher groups and provides options to create, manage, and distribute them.



Voucher page

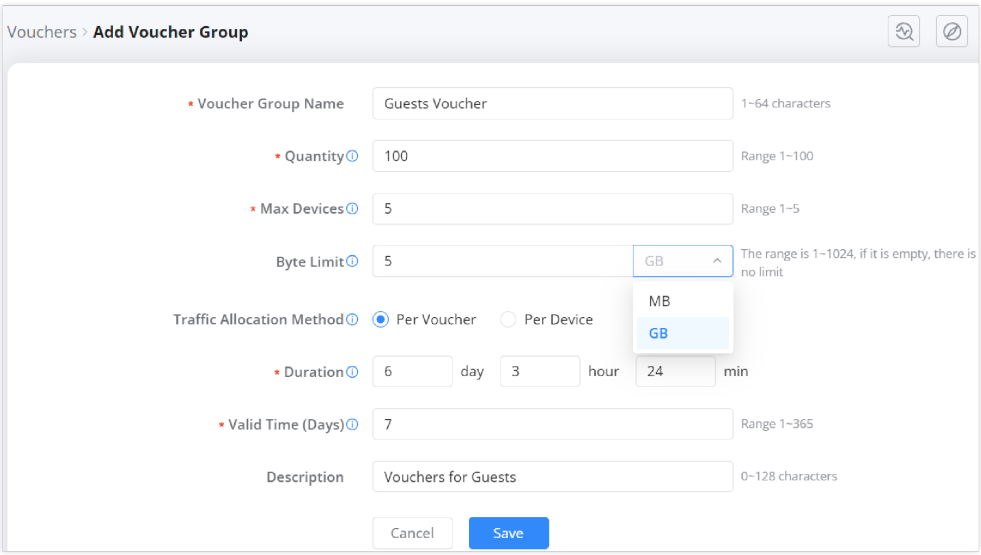
Adding a Voucher Group:

To create a new voucher group:

1. Click the **Add** button on the **Vouchers** page.
2. Fill in the required details:
   - **Voucher Group Name**: A label to identify the voucher group.
   - **Quantity**: Number of vouchers to generate (1-100).
   - **Max Devices**: Maximum number of devices per voucher (1-5).
   - **Byte Limit**: Set a data limit per voucher or per device (MB/GB).

- **Traffic Allocation Method**:
  - **Per Voucher**: The total data limit applies to all devices using the same voucher.
  - **Per Device**: Each device gets an independent data limit.
- **Duration**: Defines how long the voucher remains active (days/hours/minutes).
- **Valid Time**: The period before the voucher expires (1-365 days).
- **Description**: Optional text to describe the voucher usage.

3. Click **Save** to generate the vouchers.



Add/Edit voucher

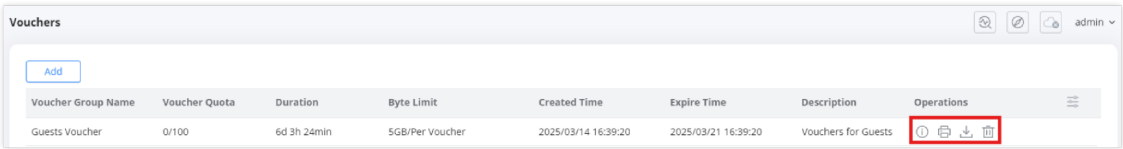
Managing Vouchers:

Once created, the voucher group will be listed on the **Vouchers** page. Each entry includes:

- **Voucher Quota**: Displays used vs. available vouchers.
- **Duration**: The validity period of the vouchers.
- **Byte Limit**: The data allocation per voucher.
- **Created Time & Expiry Time**: When the vouchers were generated and when they will expire.
- **Description**: Notes about the voucher group.

Operations Available:

- **View Details**: Inspect voucher details.
- **Print**: Generate a printable voucher list.
- **Download**: Export voucher details as a file.
- **Delete**: Remove a voucher group.



Voucher page – print or download

Using Vouchers in Captive Portal:

1. When creating a **Splash Page**, enable the **Voucher Login** option.
2. Assign the splash page to a **Captive Portal Policy**.
3. Apply the policy to a **Wi-Fi SSID**.
4. Users connecting to the SSID will be prompted to enter a valid voucher code for authentication.

Maintenance

Upgrade

The **Upgrade** section in the **GWN7062E(T) router** web UI allows users to update the router's firmware to the latest version. Firmware updates provide security patches, performance enhancements, and new features, ensuring the router remains up to date and functions optimally.

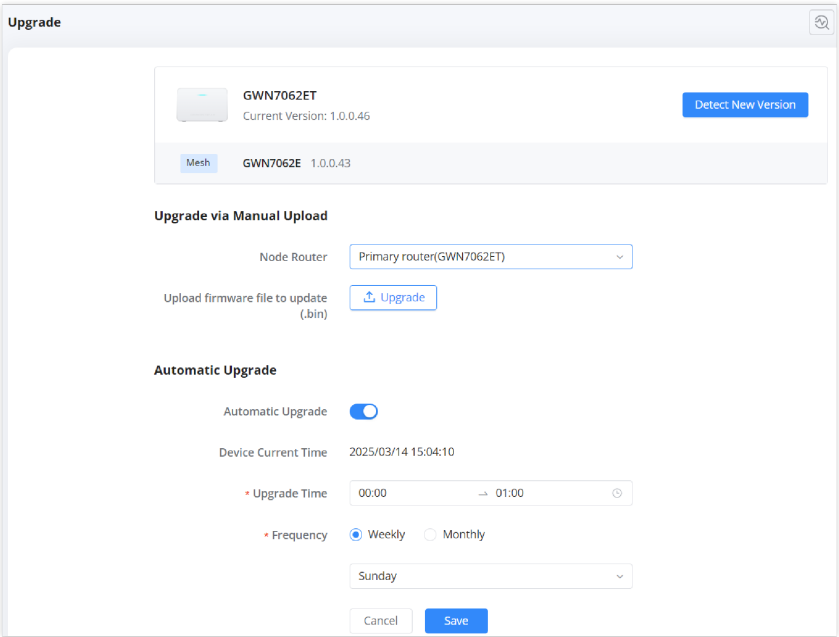
To access the **Upgrade page**:

1. Log in to the router's web UI.
2. Navigate to **Maintenance** → **Upgrade** in the left menu.
3. The upgrade section will display details about the current firmware version and update options.

Steps for Manual Upgrade:

1. **Select the Node Router**:
   - Choose either:
     - **Primary router (GWN7062ET)**
     - **Sub-router (GWN7062E)** (if part of a mesh network)
2. **Upload the Firmware File**:
   - Click **Upload** to select the firmware file.
   - Ensure the file is in `.bin` format.
3. **Click Upgrade** to start the firmware update process.

Note: Do not power off or disconnect the router during the update process.



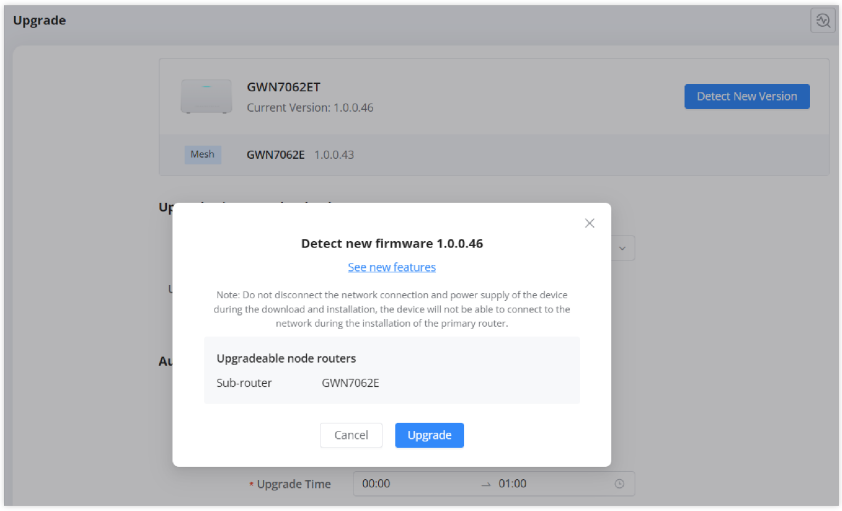
Upgrade page

Steps to Enable Automatic Upgrade:

1. **Toggle ON** the **Automatic Upgrade** option.
2. **Set Upgrade Time** – Define the time range for the update.
3. **Choose Frequency**:
   - **Weekly** – Select the day of the week (e.g., Sunday).
   - **Monthly** – Choose a specific day of the month.
4. **Click Save** to apply the settings.

Benefits of Automatic Upgrade:

- Ensures the router stays up to date without manual intervention.
- Reduces downtime by scheduling updates during non-peak hours.



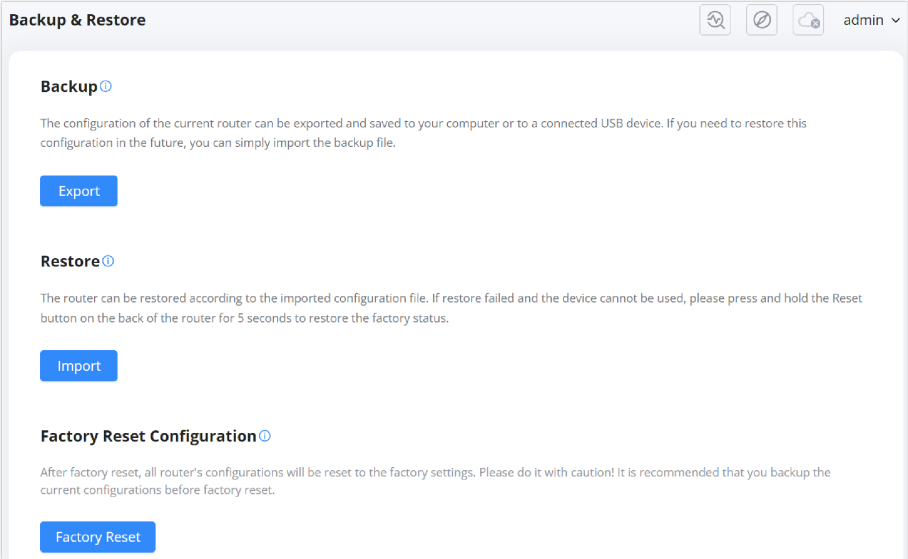
Upgrade – Detect New Firmware

Backup & Restore

The **Backup & Restore** section in the **GWN7062E(T) router** allows users to save, restore, and reset the router's configuration. This feature ensures that users can preserve their network settings, recover from misconfigurations, and restore factory defaults when necessary.

To access **Backup & Restore**:

1. Log in to the router's web UI.
2. Navigate to **Maintenance** → **Backup & Restore** in the left menu.
3. The page will display options to **Export, Import, or Factory Reset** the configuration.



Backup & Restore

4. The **Backup** function allows users to save the current router configuration to a local computer or a USB device.

Steps to Backup Configuration:

1. Click the **Export** button.
2. The router will generate a backup file (.bin) containing the current configuration.
3. Save the file to your computer or an external storage device.

Use Case:

- **Before making significant changes** to the router settings.
- **For disaster recovery**, allowing quick restoration of network settings.
- **To replicate configurations** across multiple routers.

2. The **Restore** function allows users to reload a previously saved configuration file.

Steps to Restore Configuration:

1. Click the **Import** button.
2. Select the previously saved backup file (.bin) from your computer.
3. The router will load the configuration and apply the settings.

Important Notes:

- Restoring a backup **overwrites** the existing configuration.
- If a restore fails and the router becomes unresponsive, **press and hold the physical reset button on the router for 5 seconds** to restore factory settings.

3. The **Factory Reset** function resets the router to its default settings, erasing all user configurations.

Steps to Perform a Factory Reset:

1. Click the **Factory Reset** button.
2. Confirm the action when prompted.
3. The router will reboot and revert to its original settings.

Alternative Reset Method:

- Press and **hold the reset button** on the back of the router for **5 seconds** until the LED indicator blinks.
- The router will reset and restart with factory defaults.

Caution:

- **All settings will be lost** after a factory reset.
- It is **highly recommended to perform a backup before resetting** the router.

Diagnostics

The **Diagnostics** section in the **GWN7062E(T) router** web UI provides essential troubleshooting tools to monitor system events, diagnose network issues, and capture logs. These tools help administrators identify potential problems, analyze network performance, and perform debugging tasks efficiently.

To access **Diagnostics**:

1. Log in to the router's web UI.
2. Navigate to **Maintenance** → **Diagnostics** in the left menu.
3. Select the relevant tab to perform diagnostic actions.

1. Log Monitoring

The **Log** tab records and displays system and network activity logs.

Features:

- **Time** – Timestamp of logged events.
- **Severity** – Indicates event type (Notice, Warning, Error).

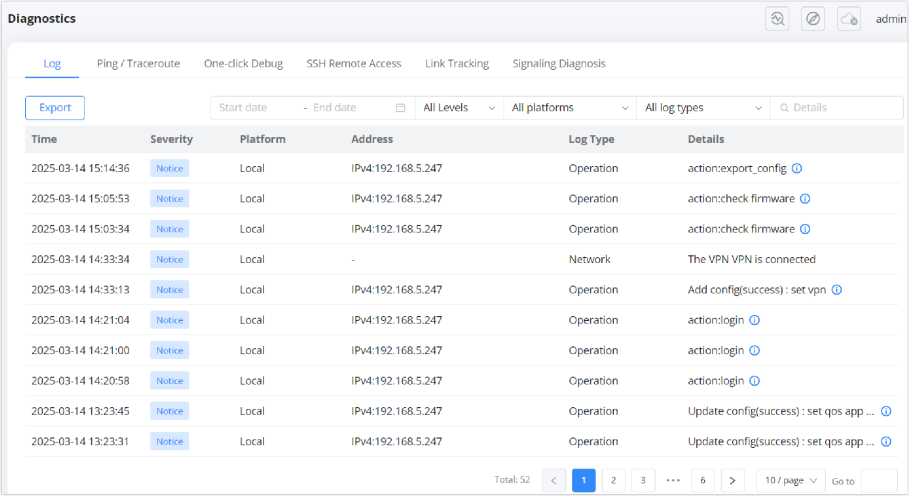
- **Platform** – Identifies whether the log event is local or network-related.
- **Address** – Shows the IP address involved in the event.
- **Log Type** – Categorizes log entries (Operation, Configuration, Security, etc.).
- **Details** – Provides additional information about the event.

Exporting Logs:

- Click **Export** to download logs as a CSV file for offline analysis.

Use Case:

- Monitor **configuration changes, remote access attempts, and security alerts**.
- Identify **network connectivity issues** and troubleshoot them effectively.



Diagnostics – log page

2. Ping / Traceroute

This tool helps verify network connectivity and diagnose latency or packet loss.

Steps to Use Ping / Traceroute:

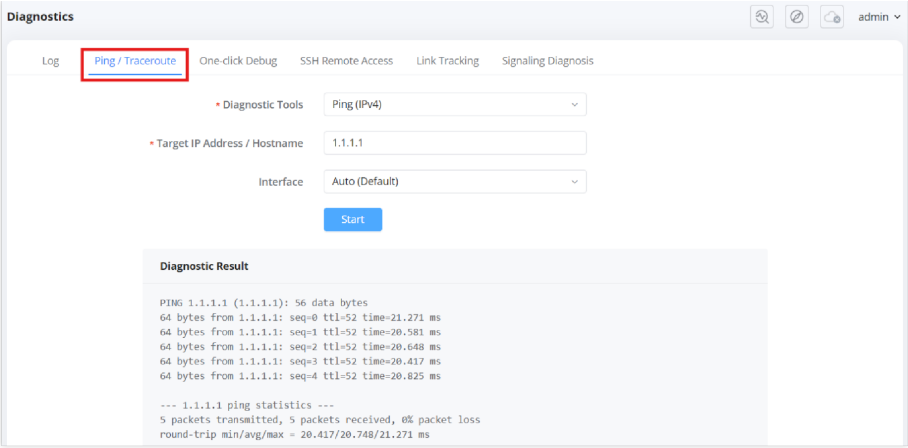
1. Select **Diagnostic Tools**:
   - **Ping (IPv4/IPv6)** – Checks if a device is reachable.
   - **Traceroute** – Traces the path packets take to a destination.
2. Enter **Target IP Address / Hostname**.
3. Select **Interface** (Auto by default).
4. Click **Start** to run the test.

Results Interpretation:

- **Low latency & no packet loss** → Connection is stable.
- **High latency or packet loss** → Possible network congestion or faulty routing.

Use Case:

- Verify **Internet connectivity** to external sites (e.g., 1.1.1.1).
- Diagnose **delays and packet loss** in internal or external network paths.



Diagnostics – Ping/Traceroute

3. One-click Debug

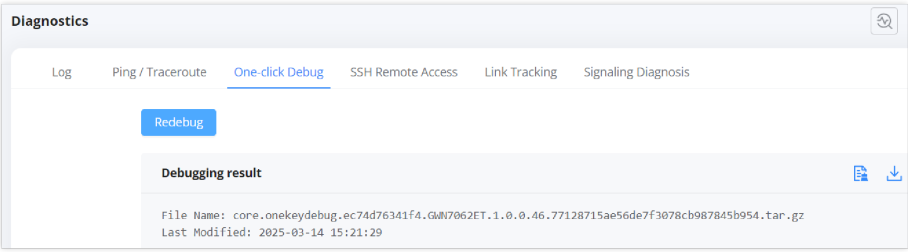
This feature automatically **collects system logs and diagnostic data** in a compressed file.

Steps to Generate Debug File:

1. Click **Redebug** to start data collection.
2. Once completed, a **debugging result file** appears.
3. Click the **download icon** to save the debug file.

Use Case:

- Share the debug file with **technical support** for advanced troubleshooting.
- Identify **firmware issues, network crashes, or system failures**.



Diagnostics – One-click Debug

4. SSH Remote Access

Allows **secure remote login** to the router for advanced debugging.

Features:

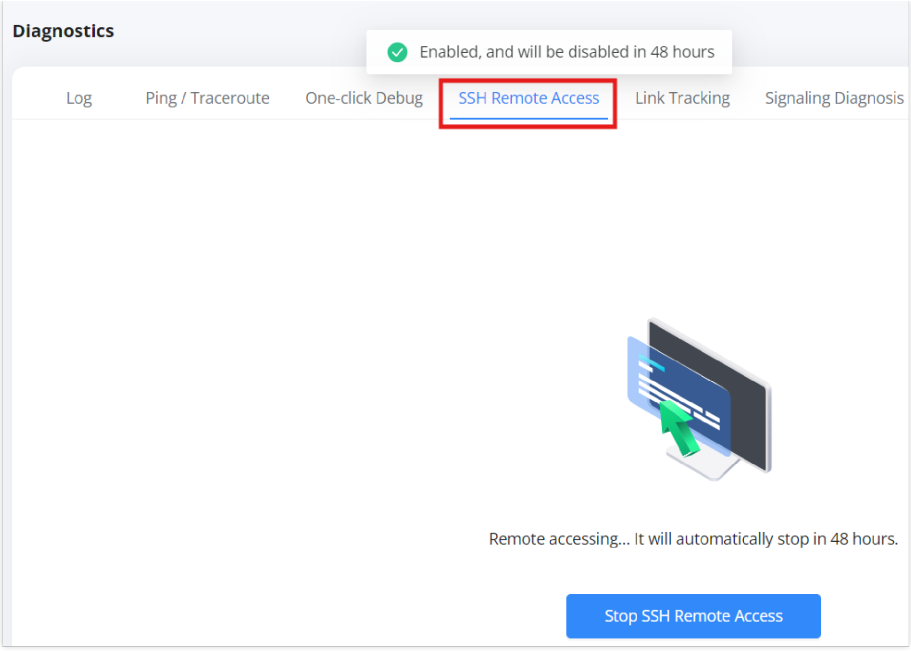
- Once enabled, **SSH access is granted for 48 hours**.
- Provides **command-line access** for deep diagnostics.

Steps to Enable SSH:

1. Click **Enable SSH Remote Access**.
2. Securely log in using an **SSH client** (e.g., PuTTY).
3. Click **Stop SSH Remote Access** when finished.

Use Case:

- Run **advanced commands** for deeper network analysis.
- Configure and troubleshoot issues directly from the **CLI**.



Diagnostics – SSH Remote Access

5. Link Tracking

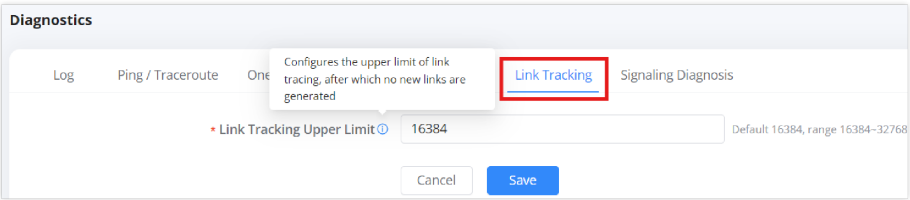
Monitors and controls **network connection limits**.

Configuration:

- **Link Tracking Upper Limit** – Adjusts the maximum number of tracked links.
- Default limit: **16384** (adjustable up to **32768**).

Use Case:

- Helps optimize **bandwidth monitoring**.
- Prevents excessive **logging overload**.



Diagnostics – Link Tracking

6. Signaling Diagnosis

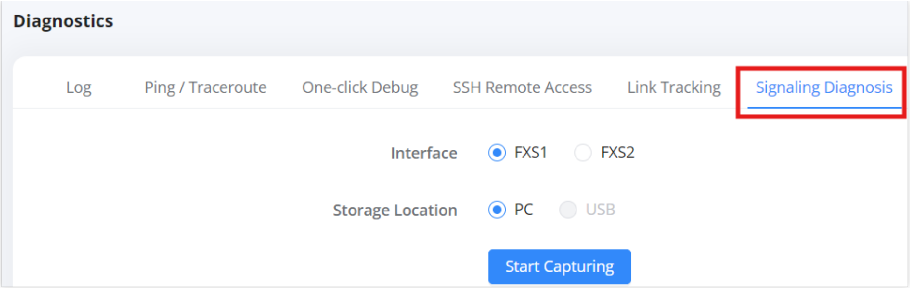
Captures **network traffic** for in-depth protocol analysis.

Steps to Start Capturing:

1. Select **Interface** (e.g., **FXS1, FXS2** for VoIP traffic).
2. Choose **Storage Location** (PC or USB).
3. Click **Start Capturing**.
4. The captured file can be saved in **PCAP format** and opened with tools like **Wireshark**.

Use Case:

- Analyze **VoIP signaling issues**.
- Investigate **packet-level network behavior**.



Diagnostics – Signaling Diagnosis

Intelligent Detection

The **Intelligent Detection** feature in the **GWN7062E(T) router** helps users diagnose and troubleshoot various network and system performance issues. This tool provides a comprehensive analysis of security, connectivity, internet failures, and mesh node connections, ensuring optimal router performance.

To access **Intelligent Detection**:

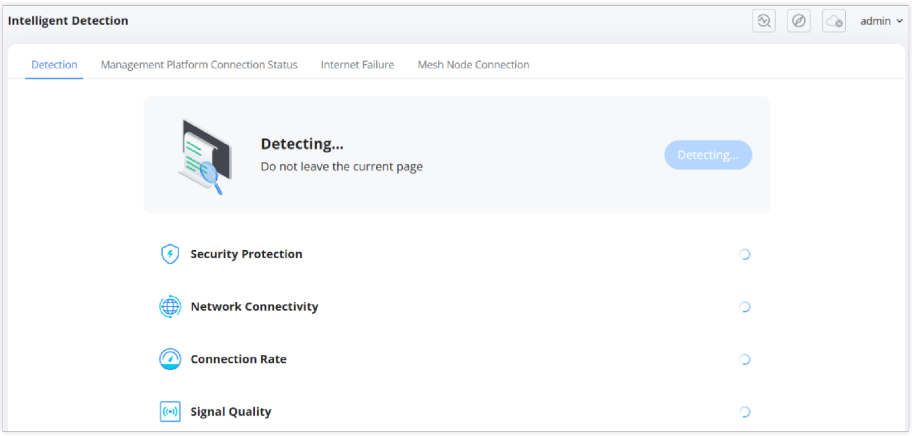
1. Log in to the router's web UI.
2. Navigate to **Maintenance → Intelligent Detection**.
3. Select the relevant tab to perform detection tests.

1. Detection Tab

The **Detection** tab provides a complete **network security and performance check**.

How to Run a Detection Test:

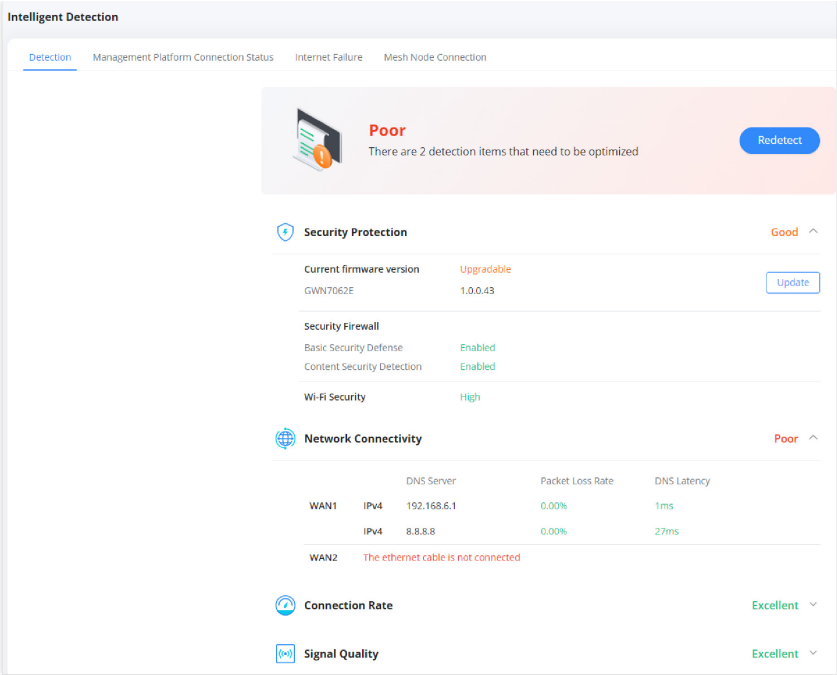
1. Click the **Detection** button.
2. The router runs diagnostics on the following areas:
   - **Security Protection** – Checks for firmware updates, firewall settings, and Wi-Fi security.
   - **Network Connectivity** – Analyzes DNS latency and packet loss.
   - **Connection Rate** – Monitors the status of network ports.
   - **Signal Quality** – Evaluates the Wi-Fi channel quality.
3. Once completed, the test results display a **rating** (e.g., **Poor, Good, Excellent**).
4. Click **Redetect** to run the test again.



Intelligent Detection page

Use Case:

- Quickly assess **network security and connectivity**.
- Detect issues such as **outdated firmware, firewall misconfigurations, or packet loss**.



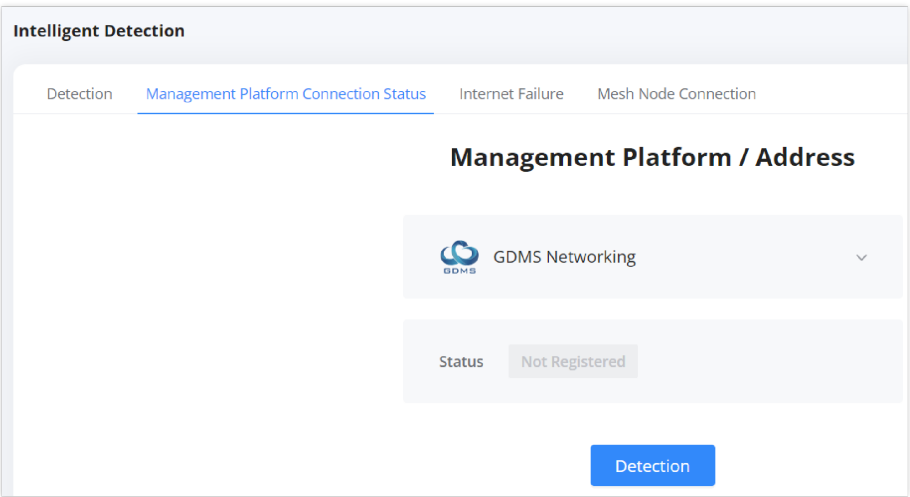
Intelligent Detection – Detection Tab

2. Management Platform Connection Status

This tab tests the router's connection with the **Grandstream Device Management System (GDMS)**.

How to Run a Connection Detection Test:

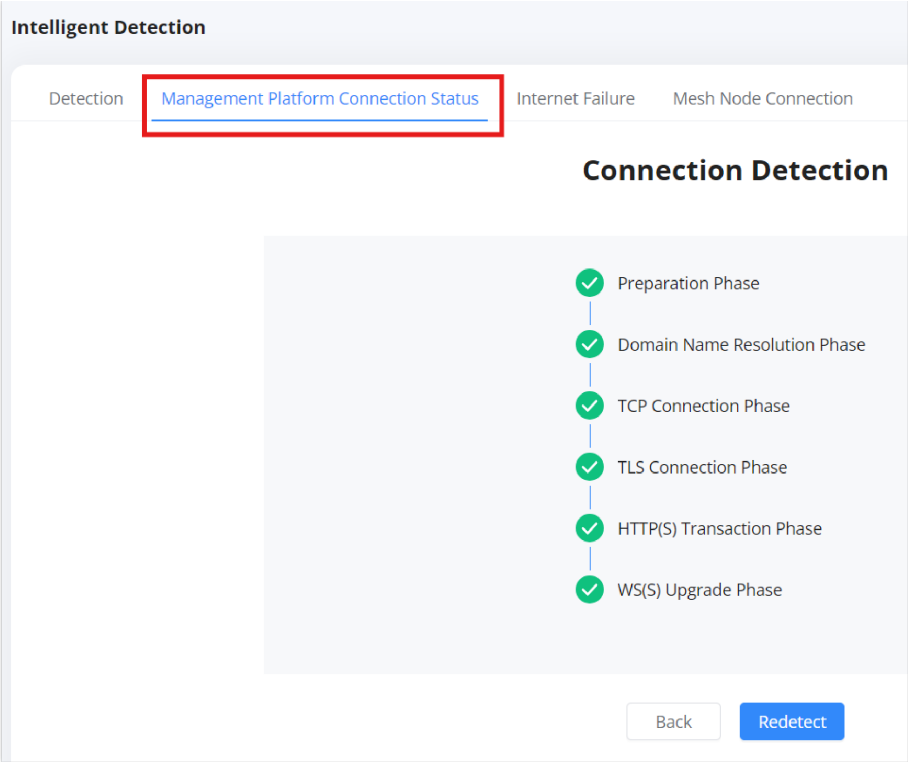
1. Click **Detection** to start the connection test.
2. The system verifies different **connection phases**:
   - **Preparation Phase**
   - **Domain Name Resolution Phase**
   - **TCP Connection Phase**
   - **TLS Connection Phase**
   - **HTTPS Transaction Phase**
   - **WebSocket Upgrade Phase**
3. If all phases are successful, the **connection is stable**.



Intelligent Detection – Management Platform Connection Status Tab

Use Case:

- Ensures the router can **connect to GDMS** for **remote management and monitoring**.
- Identifies issues preventing the router from establishing a **secure GDMS connection**.



Intelligent Detection – Management Platform Connection Status Tab

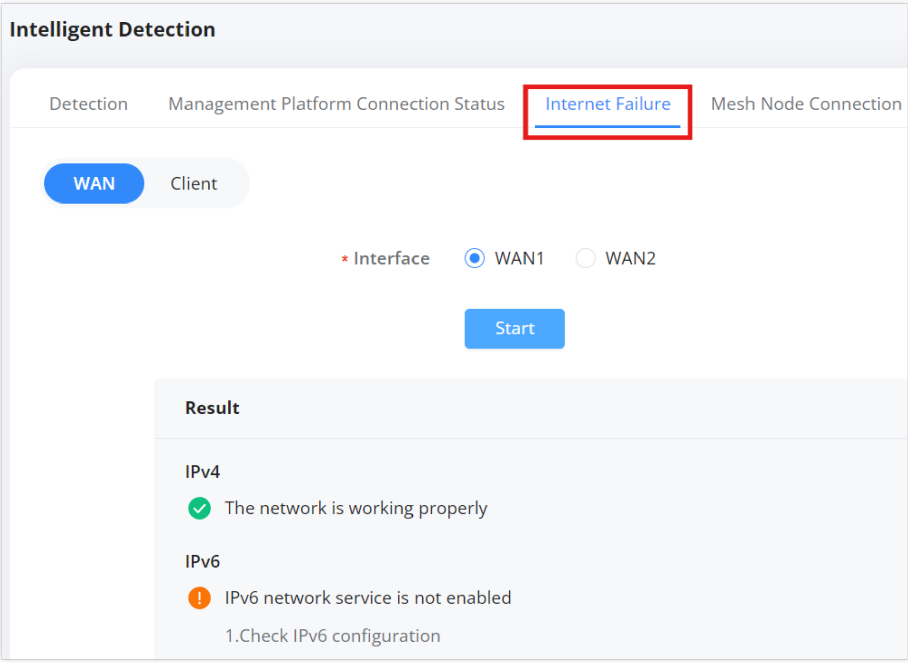
3. Internet Failure Detection

This tab diagnoses **network failures** for **WAN (Internet) and Client Devices**.

Running a WAN Connection Test:

1. Select **WAN** and choose the desired interface (**WAN1 / WAN2**).
2. Click **Start**.
3. The test checks for:
   - IPv4 connectivity.
   - IPv6 service availability.
   - DNS response times.

Example Issue: If IPv6 is disabled, the test will prompt the user to check IPv6 settings.



Intelligent Detection – Internet Failure tab

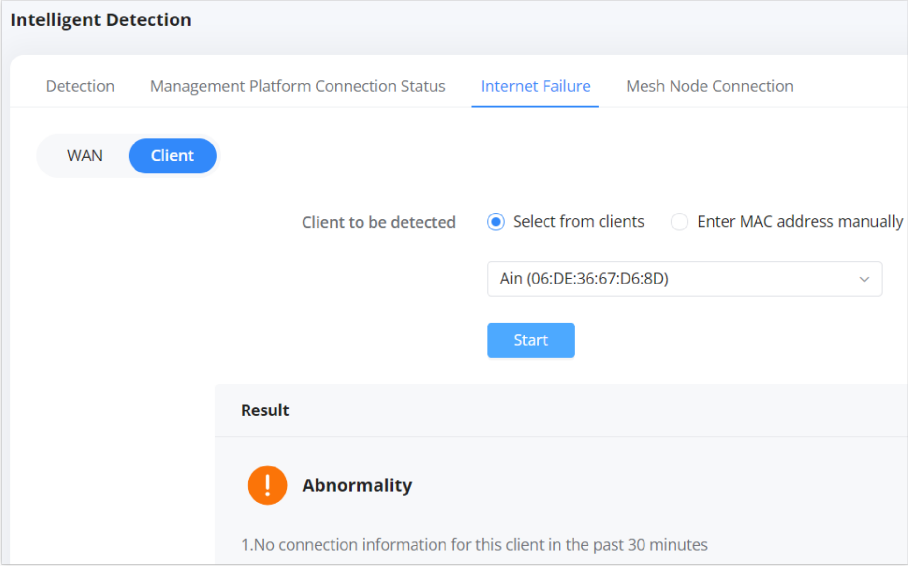
Running a Client Connection Test:

1. Select **Client** and choose a connected device from the list or enter a **MAC address manually**.
2. Click **Start**.
3. The system verifies:
   - If the client device has been active in the last **30 minutes**.
   - If the device is experiencing connectivity issues.

Example Issue: If a client has no connection logs, it may indicate a **disconnect or network problem**.

Use Case:

- Detects **Internet connectivity failures** in WAN/LAN.
- Troubleshoots **client device disconnections**.



Intelligent Detection – Internet Failure

4. Mesh Node Connection

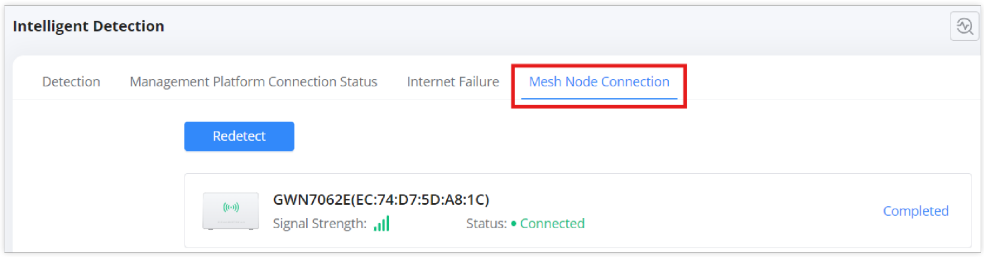
This tab checks the status of connected **mesh nodes** in a multi-router setup.

Running a Mesh Node Detection Test:

1. Click **Detect**.
2. The router scans for all connected **mesh nodes**.
3. Results display:
   - **Mesh node device name**.
   - **Signal strength**.
   - **Connection status (Connected/Disconnected)**.

Use Case:

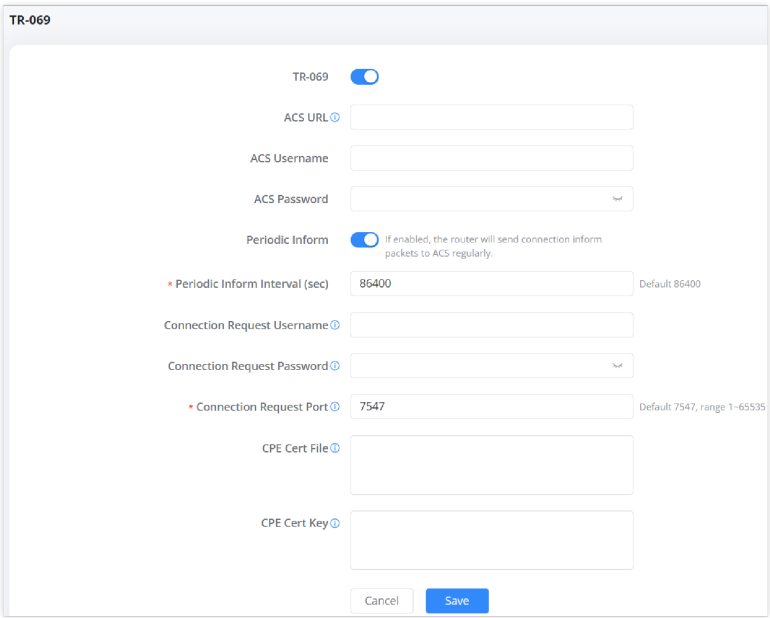
- Ensures **mesh nodes are properly connected**.
- Troubleshoots **mesh coverage issues**.



Intelligent Detection – Mesh Node Connection

TR-069

TR-069 (Technical Report 069) is a protocol for **remote management** of network devices, including routers. It allows **Auto-Configuration Servers (ACS)** to remotely configure, update firmware, monitor performance, and troubleshoot network devices without requiring manual intervention. This feature is commonly used by ISPs and IT administrators to manage a large number of routers remotely.



TR-069

TR-069 Configuration Options:

1. Enabling TR-069

- **TR-069 Toggle** – Enables or disables the TR-069 remote management feature.

2. Auto-Configuration Server (ACS) Settings

- **ACS URL** – The URL of the Auto-Configuration Server (ACS) that manages the router.
- **ACS Username & Password** – The credentials used by the ACS to authenticate and communicate with the router.

3. Periodic Inform

- **Periodic Inform Toggle** – When enabled, the router will periodically send status updates to the ACS.
- **Periodic Inform Interval (sec)** – Defines how frequently (in seconds) the router should send inform messages to the ACS. The default is **86400 seconds (24 hours)**.

4. Connection Request Settings

- **Connection Request Username & Password** – Credentials required for the ACS to initiate a request to the router.
- **Connection Request Port** – Defines the port used for ACS requests. The default is **7547** (configurable between **1-65535**).

5. Certificate Authentication

- **CPE Cert File** – Upload a certificate file to enable encrypted authentication between the router and ACS.
- **CPE Cert Key** – Upload a private key to establish a secure connection.

Use Cases for TR-069:

- **Remote Configuration** – Allows ISPs and administrators to configure settings remotely.
- **Firmware Management** – Enables automated firmware updates without user intervention.
- **Monitoring & Diagnostics** – Collects real-time router performance data for troubleshooting.
- **Security & Compliance** – Ensures routers follow security policies through automated management.

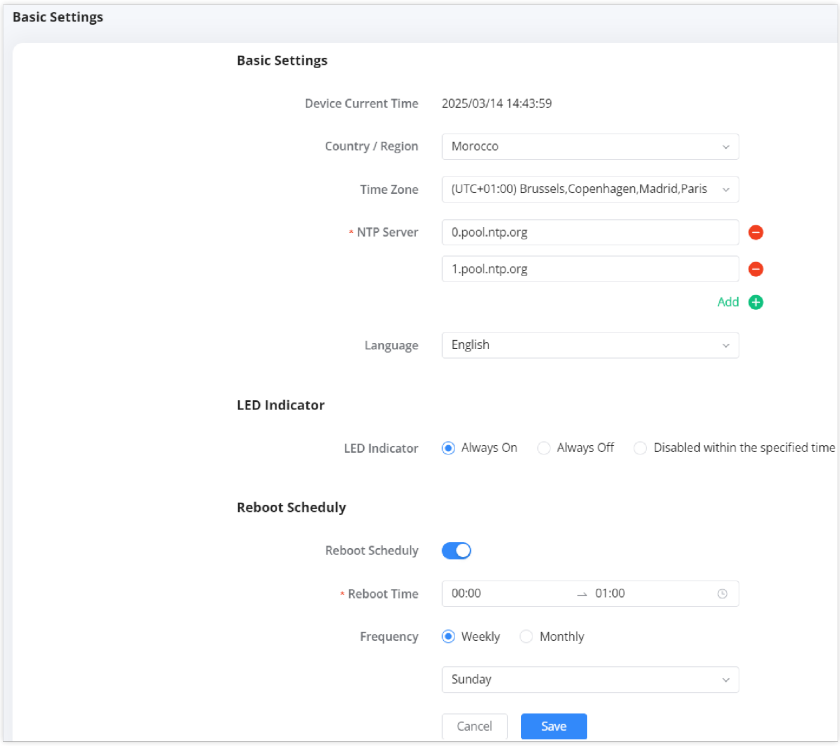
System

Basic Settings – System

The **Basic Settings** section in the GWN7062E(T) router web UI allows users to configure fundamental system settings such as time synchronization, language preferences, LED status, and automatic reboot scheduling. These settings help in ensuring accurate timekeeping, maintaining optimal device behavior, and improving overall network management.

To access the **Basic Settings**:

1. Log in to the router's web UI.
2. Navigate to **System** → **Basic Settings** in the left menu.
3. The page will display options to configure system settings as described below.



System – Basis Settings page

Basic Settings Options:

Device Current Time

- Displays the current system time of the router.
- This time is determined by the configured time zone and NTP server settings.

Country/Region

- Allows users to select the country or region where the router is deployed.
- This setting helps adjust time zone and regulatory compliance settings accordingly.

Time Zone

- Select the correct **UTC offset** from the dropdown menu.
- Ensures proper time synchronization for logs, scheduling, and other time-dependent services.

NTP Server

- The **Network Time Protocol (NTP) Server** synchronizes the router's time automatically.
- Users can specify one or more NTP servers (e.g., `0.pool.ntp.org`, `1.pool.ntp.org`).

- Clicking the **Add (+)** button allows additional NTP servers to be added.

Language

- Allows users to select the interface language.
- The default setting is **English**.

LED Indicator Settings

- **Always On** – The router's LED indicators remain active at all times.
- **Always Off** – The LED indicators are completely disabled.
- **Disabled within the specified time** – The LEDs will be turned off during a specified time period to reduce light pollution.

Reboot Schedule

This feature allows users to **automatically reboot** the router at a scheduled time, ensuring optimal performance by clearing temporary data and refreshing system processes.

- **Enable/Disable Toggle** – Users can enable or disable the scheduled reboot.
- **Reboot Time** – Defines the time frame for the scheduled reboot.
- **Frequency**:
  - **Weekly** – The router will reboot on a selected day of the week.
  - **Monthly** – The router will reboot on a specific day of the month.
- **Day Selection** – If **Weekly** is selected, users can choose the day (e.g., **Sunday**).

Access Management

The **Access Management** section of the GWN7062E(T) router allows users to configure authentication, user accounts, remote access control, and security policies to protect and manage administrative access. These settings enhance security by enforcing strong password policies, restricting unauthorized access, and enabling remote management through secure protocols.

To access **Access Management** settings:

1. Log in to the router's web UI.
2. Navigate to **System** → **Access Management** in the left menu.
3. Select the relevant tab to configure access settings.

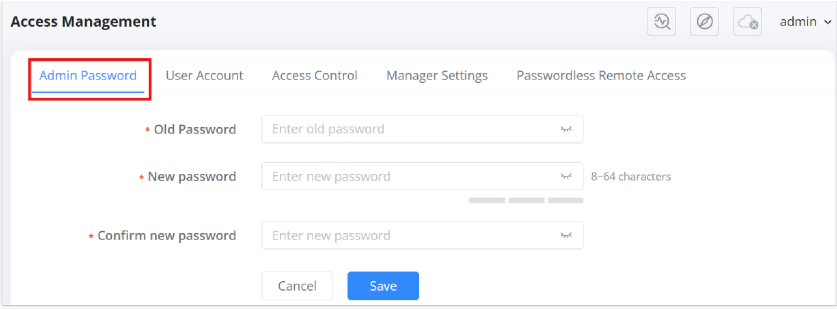
The **Admin Password** tab allows administrators to change the default password for security purposes.

Options:

- **Old Password** – Enter the current admin password.
- **New Password** – Set a new password (must be **8-64 characters** long).
- **Confirm New Password** – Re-enter the new password for confirmation.

Best Practices:

- Use a **strong password** with a mix of uppercase letters, numbers, and symbols.
- Change the default password **immediately after setup** for security.
- Regularly update passwords to reduce security risks.



Access management – Admin password

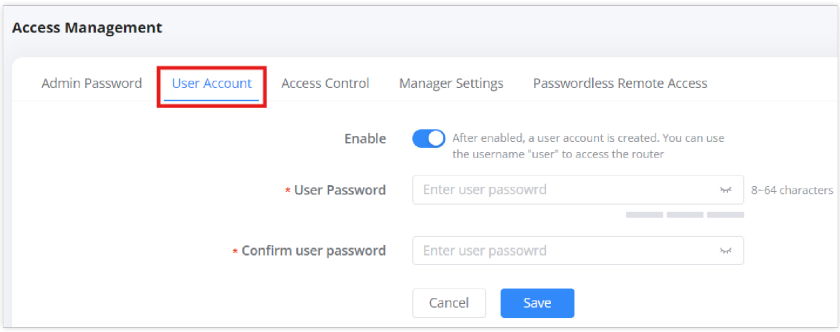
The **User Account** tab allows the creation of a secondary user account with limited access.

Options:

- **Enable** – Toggle to enable or disable the user account.
- **User Password** – Set a password for the secondary user.
- **Confirm User Password** – Re-enter the password to confirm.

Key Notes:

- Once enabled, the user can log in using the username **"user"**.
- This account has **restricted privileges** compared to the administrator.
- Useful for allowing **network monitoring** without granting full access.



Access management – User Account

The **Access Control** tab manages administrative access to the router from the LAN and WAN.

LAN Side Settings:

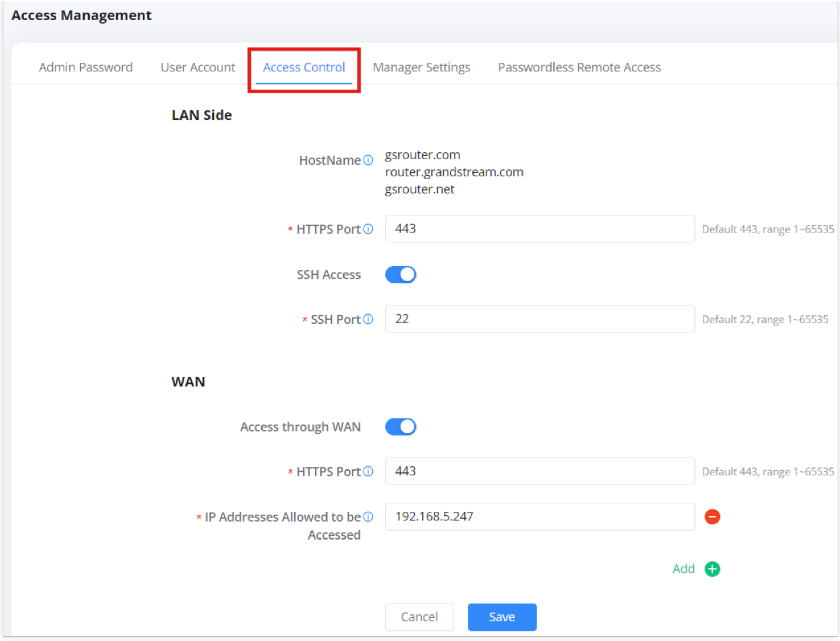
- **HostName** – Displays the router's local domain name.
- **HTTPS Port** – Default is **443** (Range: 1-65535).
- **SSH Access** – Toggle to enable or disable SSH access.
- **SSH Port** – Default is **22** (Range: 1-65535).

WAN Side Settings:

- **Access through WAN** – Toggle to enable remote access over the Internet.
- **HTTPS Port** – Specifies the port for remote HTTPS access.
- **IP Addresses Allowed to be Accessed** – Restrict remote access to specific IP addresses.

Security Recommendations:

- **Disable WAN access** if remote management is unnecessary.
- Change the **default SSH/HTTPS ports** to reduce attack risks.
- **Restrict remote access** to specific IPs whenever possible.

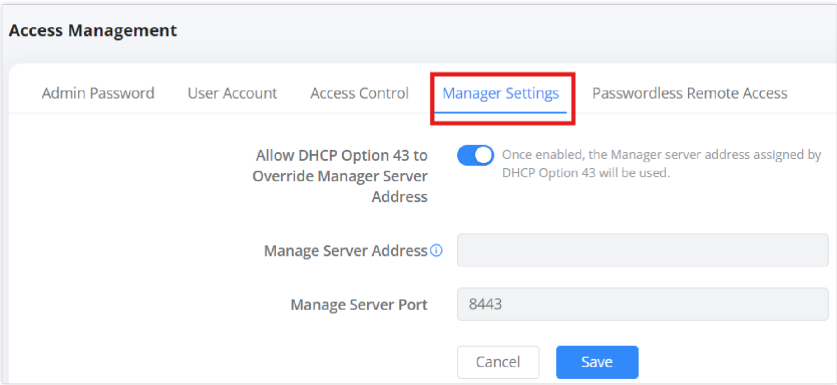


Access management – Access Control

This tab allows remote management through **GWN Manager**, Grandstream's on-premise network management platform.

Options:

- **Allow DHCP Option 43 to Override Manager Server Address** – When enabled, DHCP Option 43 can override the predefined GWN Manager address.
- **Manage Server Address** – Enter the IP or domain of the GWN Manager server.
- **Manage Server Port** – Default is **8443**.



Access management – Manager Settings

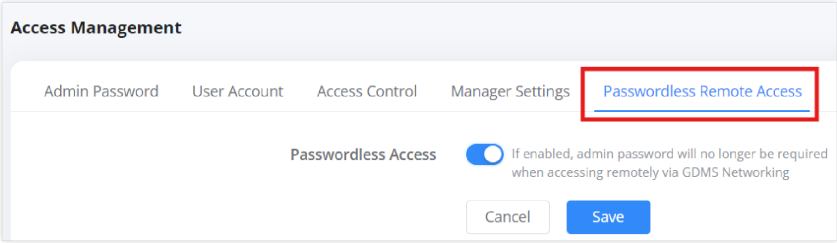
This feature allows **remote access without requiring a password** when using **GDMS Networking**, Grandstream's cloud management platform.

Options:

- **Passwordless Access Toggle** – Enable or disable passwordless login.

Security Considerations:

- **Enable this feature only if using GDMS Networking** for remote access.
- If security is a concern, it's best to **disable passwordless access** and require authentication.



CHANGE LOG

This section documents significant changes from previous versions of the GWN7062E(T) routers user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.1.10

- No major changes.

Firmware Version 1.0.1.7

- This is the initial release.
